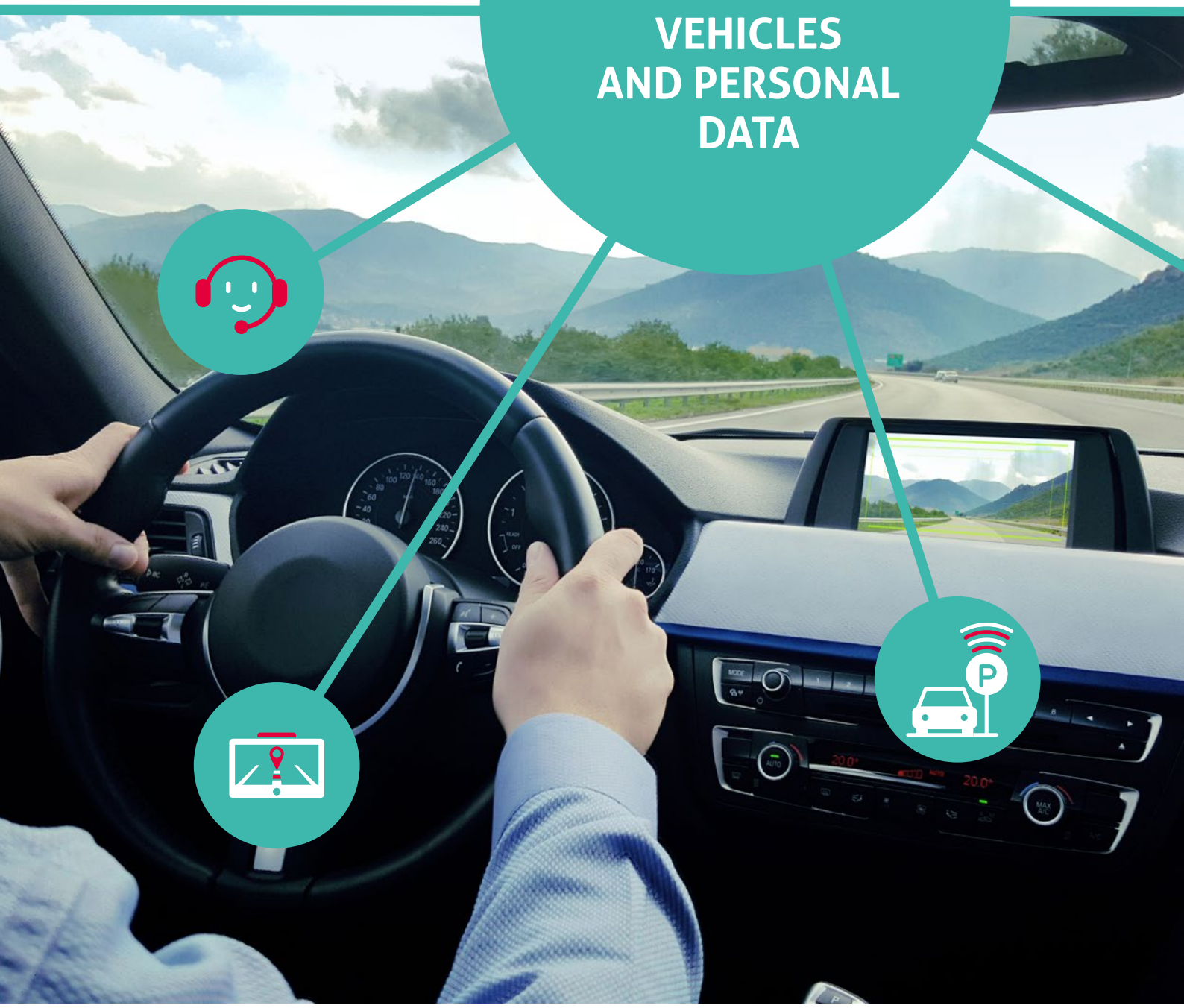
COMPLIANCE PACKAGE

CONNECTED VEHICLES AND PERSONAL DATA



CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

COMPLIANCE PACKAGE - INTRODUCTION

CONNECTED VEHICLES AND PERSONAL DATA

SUMMARY

INTRODUCTION

The CNIL (French Data Protection Authority) wishes to encourage innovation ecosystems and ensure the protection of car users' personal data. Accordingly, in March 2016, the CNIL created a working group on the "connected vehicles" compliance package.

The compliance package has been elaborated in consultation with stakeholders from the automobile sector, businesses in the insurance and telecoms sectors, as well as public authorities, in order to propose a sectorial reference framework, a toolbox for the responsible use of personal data.

The challenge is to incorporate the "protection of personal data" dimension from the product design phase, and to ensure that car users enjoy transparency and control in relation to their data. Such an approach helps to strengthen user confidence, and thus the long-term development of those technologies.

The guidelines that emerge from the compliance package constitute the CNIL's interpretation of the French Data Protection Act, as applied to connected vehicles. They reflect the analytical frameworks used by the CNIL to assess possible breaches of the law, and they constitute an element of legal security for data controllers.

They also enable the stakeholders to comply with the General Data Protection Regulation, applicable from 25 May 2018. The compliance package is intended to be extended to the European level to enable stakeholders to position themselves on a European, if not global market. It may constitute a European guideline, as set out in the General Data Protection Regulation.

The compliance package offers three working cases, which correspond to three scenarios encountered by professionals in the sector. For each type of processing, these guidelines specify: the intended purposes, the categories of data collected, the retention period of such data, the rights of data subjects, the security measures to be implemented, and the recipients of the information.

List of bodies consulted by the CNIL:

PUBLIC SECTOR

- French Environment and Energy Management Agency (“ADEME”)
- E-communication and Postal Regulation Authority (“ARCEP”)
- Directorate General for Enterprise (“DGE”)
- National Gendarmerie
- French Institute of Science and Technology for Transport, Development and Networks (“IFSTTAR”)
- Ministry for the Ecological and Solidarity Transition

PROFESSIONALS FROM THE AUTOMOBILE SECTOR

- Avis Car Rentals
- Committee of French Car Manufacturers (“CCFA”)
- National Council of Professions in the Automobile Sector (“CNPA”)
- International Chamber of Automobiles and Motorcycles (“CSIAM”)
- Drust
- Eliocity (Xee)
- Federation of Vehicle Equipment Industries (“FIEV”)
- Federation of Automobile Distribution Unions (“FSDA”)
- Michelin
- Nexyad
- PSA
- Renault

PROFESSIONALS IN THE INSURANCE SECTOR

- French Insurance Federation (“FFA”)

PROFESSIONALS IN THE TELECOMS SECTOR

- French Telecoms Federation (“FFT”)

PROFESSIONALS OF THE ELECTRICAL, ELECTRONIC, AND COMMUNICATIONS INDUSTRIES

- Federation of Electrical, Electronic and Communications Industries (“FIEEC”)

The scope of the compliance package

The compliance package applies to connected vehicles, *i.e.*, vehicles that communicate with the outside world (mobile applications, other vehicles, infrastructure, etc.).

The compliance package only covers the use of vehicles by customers for their personal needs and does not extend to the use of company vehicles by employees.

The scope of the compliance package is the processing of personal data collected *via* vehicle sensors, telematics boxes, or mobile applications, whether the data are processed inside the vehicles or exported to a centralised server.

The personal data concerned include all data associated or that can be associated with a natural person (driver, vehicle owner, passenger, etc.), especially via the vehicle serial number.

Thus, they may be directly identifying data, e.g. the driver's name, as well as indirectly identifying data, e.g. details of journeys made, the vehicle usage data (e.g. data relating to driving style or the distance covered), or the vehicle's technical data (e.g. data relating to the wear and tear on vehicle parts), which, by cross-referencing with other files, can be related to a natural person.

These guidelines are representative of the understanding, at this point in time, of the technologies and associated practices, and will be regularly reviewed. Thus, the compliance package is not prospective and is intended to specify the rules for services that already exist in the market. As an example, the compliance package does not cover intelligent transport systems ("ITS"), because the conditions for their possible roll-out have not yet been set out.

1. SCOPE OF THE FRENCH DATA PROTECTION ACT AND THE GENERAL DATA PROTECTION REGULATION (GDPR)

The French Data Protection Act of 6 January 1978, as amended, and the General Data Protection Regulation apply when processing involves personal data.

The notion of personal data is defined broadly by the French Data Protection Act. In this case, the term "personal data" shall cover all the vehicle data that, alone or in combination with others, can be linked to a natural person (driver, vehicle owner, passenger, etc.), especially *via* the vehicle serial number. To determine if a person has been identified or is identifiable, it is important to take into account all the means that are likely to be used by the data controller or by any other person.

The processing of personal data is subject to a certain number of legal obligations that are incumbent upon the data controller: providing information to data subjects in respect of the data processing, in certain circumstances obtaining their explicit consent, providing data subjects with a copy of their data, filing prior formalities with the CNIL, etc.

However, the French Data Protection Act does not apply when the data processed are anonymous, *i.e.*, when they cannot be directly or indirectly associated with a natural person. To determine the mechanism to put in place for obtaining anonymous data, the data controller shall consider the possibility of reidentifying natural persons based on the data obtained. Therefore, anonymisation mechanisms shall be defined on a case-by-case basis, especially based on the level of detail of the data.

Similarly, the French Data Protection Act does not apply in the case of processing performed in the course of purely personal activities (such as the processing described in scenario No. 1).

2. DEFINITION OF THE KEY NOTIONS OF THE FRENCH DATA PROTECTION ACT AND THE GENERAL DATA PROTECTION REGULATION

Processing of personal data shall mean any operation (collection, registration, storage, modification, extraction, consultation, use, communication, interconnection, destruction, etc.) that involves personal data.

Personal data shall mean any information relating to a natural person who is identified or identifiable, directly or indirectly, by reference to an identification number or to one or more pieces of information specific to that person. Thus, personal data include all data that, taken alone or in combination with others, can be linked to an identified or identifiable user, especially *via* the vehicle serial number or the vehicle licence plate number, whether by the data controller or by any other person. As an example, personal data include data relating to journeys made, the wear and tear on vehicle parts, the dates of technical controls, mileage, or driving style, to the extent that they can be linked to a natural person, especially *via* the vehicle serial number or the vehicle licence plate number, whether by the data controller or by any other person. Therefore, personal data are not just nominative data (surname and first name).

In the context of the compliance package, the following data categories are notably concerned:

- "client" data (surname, first name, address, telephone numbers, e-mail address, etc.);
- the vehicle serial number or any other unique identifier of the vehicle (e.g. the vehicle licence plate number);
- geolocation data;
- technical data relating to the state of the vehicle and its parts;
- the driver's biometric data;
- data relating to the use of the vehicle by the driver or the occupants (e.g. data relating to driving styles, mileage, life aboard the vehicle, etc.).

A **file** shall mean any structured and stable set of personal data that is accessible according to specific criteria. They may be computer files or paper files sorted, for example, alphabetically or chronologically.

Unless expressly designated by legislative or regulatory provisions, the **data controller** is the person who determines the purposes or means of processing. As an example, the designation of "data controller" shall apply to the service provider who processes vehicle data to send the driver traffic-information and eco-driving messages, as well as alerts regarding the functioning of the vehicle. The data controller shall comply with all the obligations imposed by the French Data Protection Act (especially regarding providing information to data subjects, obtaining the consent of data subjects, implementing adapted security measures, or filing prior formalities with the CNIL).

Pursuant to article 26 of the General Data Protection Regulation, several businesses can jointly determine the purposes and means of the processing and thus be considered as joint controllers. In this case, they have to clearly define their respective obligations, especially as regards the exercising of the rights of data subjects and the provision of information to data subjects.

The **data processor** is any person who processes personal data for and on behalf of the data controller. The data processor collects and processes data on instruction from the data controller, without using those data for its own account.

Article 28 of the General Data Protection Regulation reinforces data processors' obligations. Thus, in addition to the obligation to implement appropriate technical and organisational measures in order to guarantee a security level that is adapted to risk, data processors shall:

- not be able to subcontract to a third party without the specific written agreement of the data controller, and shall inform the data controller of all modifications concerning their own subcontractors, in order to enable the data controller to object to such modifications;
- ensure that all persons whom they authorise to process personal data are covered by a confidentiality requirement;
- use appropriate technical and organisational measures to assist the data controller in complying with its data protection obligations;
- subject to the data controller's choice, delete data or return them to the data controller at the end of the contract;
- provide the data controller with all the information needed to show that the data processors are compliant with data protection regulations;
- inform the data controller if they consider that the processing breaches the General Data Protection Regulation; and
- keep an up-to-date register of all categories of processing activities carried out for and on behalf of the data controller.

The **data subject** is the natural person to whom the data covered by the processing relate. In the context of the present pack, it can, in particular, be the driver (main or occasional), the passenger, or the owner of the vehicle.

The **recipient** is any person authorised to receive personal data, other than the data subject, the data controller, the data processor, and the persons who, by reason of their functions, are in charge of processing data. As an example, it can be a commercial partner of the service provider.

The recipient collects and processes data on its own account. Therefore, the recipient shall comply with all the obligations imposed by the French Data Protection Act (especially providing information to data subjects, obtaining the consent of data subjects, implementing adapted security measures, or filing prior formalities with the CNIL).

Clarification: As part of a particular mission or in exercising a right of communication, authorities that are legally entitled to ask a data controller to send them the personal data are not recipients. As an example, authorised third parties are officers of the criminal investigation police, the police, and the gendarmerie, when they request personal data as part of a preliminary investigation, investigations of flagrancy, or a rogatory commission, under the conditions of the Code of Criminal Procedure.

Finally, **pseudonymisation** is a technique that consists of replacing directly-identifying personal data by a non-signifying pseudonym. For example, that can be done by hashing, using a secret-key hash algorithm. Data pseudonymisation improves the protection of the confidentiality of personal data by reducing the risks of misuse. Pseudonymisation is reversible, unlike anonymisation (cf. opinion No. 05 / 2014 on "*anonymisation techniques*" of the Article 29 Working Party dated 10 April 2014). Anonymous data are not subject to the French Data Protection Act. However, that is not the case for pseudonymised data, which remain personal data.

3. KEY PRINCIPLES TO BE RESPECTED WITH REGARD TO THE FRENCH DATA PROTECTION ACT AND THE GENERAL DATA PROTECTION REGULATION

The processing of personal data shall comply with the French Data Protection Act. Any person wishing to process personal data is subject to a number of legal obligations.

THE PRINCIPLE OF INFORMATIONAL SELF-DETERMINATION

(article 1 of the French Data Protection Act)

Article 1 of the French Data Protection Act provides that information technology shall be at the service of every citizen, and it shall not harm human identity, human rights, privacy, individual freedoms, or public liberties.

In addition, pursuant to article 1, section 2, any person has the right to determine the use made of their personal data.

That right to informational self-determination expresses the individual's necessary control over their data during the entire processing period.

CLARIFICATION

Specifically, that control includes, in particular:

- configurations by default that protect privacy;
- the option for users to easily modify those configurations, during the entire processing period, especially for the purpose of activating or deactivating services based on consent or on the performance of a contract (e.g. commercial offers personalised on the basis of geolocation or breakdown assistance);
- where appropriate, the option for users to adjust the level of detail of the data collected to the level of service requested, e.g. by accessing a map without being geolocated if they do not wish to be guided; and
- the option for users to access those data easily.

THE OBLIGATION TO HAVE A LEGAL BASIS FOR THE PROCESSING IMPLEMENTED

(article 7 of the French Data Protection Act, and article 6 of the General Data Protection Regulation)

Processing of personal data shall have received the consent of the data subject, or shall satisfy one of the following conditions:

1 - compliance with a legal obligation that is incumbent upon the data controller;
2 - protection of the data subject's life;
3 - carrying out a public-service mission entrusted to the data controller or the data recipient;

4 - the performance of a contract to which the data subject is a party, or of pre-contractual measures taken at the request of the data subject;

5 - the pursuit of the data controller's or the data recipient's legitimate interest, provided that it is not incompatible with the interests or the fundamental rights and liberties of the data subject.

What changes with the GDPR

When consent constitutes the legal basis for processing, article 7 of the General Data Protection Regulation specifies that consent shall be specific, *i.e.*, it shall be clearly distinguished form other questions, in a form that is understandable and easily accessible and set out in clear and simple terms. Moreover, data subjects have the right to withdraw their consent at any time, and are expressly informed of that right. Finally, the data controller shall be able to show that the data subjects have given their consent to the processing of their personal data.

THE OBLIGATION THAT DATA BE PROCESSED FAIRLY AND LAWFULLY

(article 6-1° of the French Data Protection Act, and article 5-1° a/ of the General Data Protection Regulation)

All processing of personal data shall be done under conditions that ensure transparency with regard to the data subjects, and it shall not be implemented without the knowledge of the data subjects.

As a minimum, that obligation involves providing information to data subjects in accordance with article 32 of the French Data Protection Act, and, in some cases, obtaining their consent.

THE OBLIGATION THAT DATA BE OBTAINED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

(article 6-2° of the French Data Protection Act, and article 5-1° b/ of the General Data Protection Regulation)

Personal data can only be collected and processed for a specific, explicit, and legitimate use. Therefore, the objectives pursued by the data controller shall be defined beforehand in a clear, explicit, and exhaustive manner.

Any use of personal data for an objective that is incompatible with the primary purpose of processing is a misuse that is subject to administrative or criminal sanctions.

For example, *a mechanic cannot sell the vehicle's technical data to insurers to enable them to infer the driving profiles of their policyholders.*

THE OBLIGATION OF DATA ADEQUACY

(article 6-3° of the French Data Protection Act, and article 5-1° c/ of the General Data Protection Regulation)

Data processing shall only involve information that is relevant, adequate, and not excessive with regard to the purpose of the file, *i.e.,* its objective. In that regard, the General Data Protection Regulation refers to the principle of "*data minimisation*".

For example, *a data controller shall not continuously process the precise and detailed location of the vehicle for a purpose involving technical maintenance or model optimisation.*

THE LIMITED DATA RETENTION

(article 6-5° of the French Data Protection Act, and article 5-1° e/ of the General Data Protection Regulation)

Personal data cannot be stored indefinitely in a file.

The data controller shall determine a specific retention period based on the purpose of each processing operation.

For example, *a data controller cannot retain, for an unlimited period, the technical details of vehicles (identified in particular by means of the serial number) for the purpose of product improvement, unless the data are anonymised.*

However, legislative or regulatory provisions may require a data controller to retain data beyond the period during which they are stored in an active database.

In that case, data can be stored in an archive database for the period required to comply with the obligation in question, in compliance with the conditions specified by the CNIL's discussion on the conditions of electronic archiving (cf. discussion no. 2005-213 of 11 October 2005); in such a case, reference is made to intermediate archiving.

THE OBLIGATION OF DATA SECURITY

(article 34 of the French Data Protection Act, and article 5-1° f/ of the General Data Protection Regulation)

The data controller is bound by a security obligation and shall notably take measures to guarantee the confidentiality of the collected data, and avoid their disclosure to unauthorised third parties.

In the context of connected vehicles, the need for data confidentiality and security shall apply to data collected and processed within the vehicle as well as to data transmitted away from the vehicle. Therefore, general security measures shall be taken, involving in particular:

- encrypting communication channels (e.g. by adding a security module of the "*Hardware Security Module*" type), and correctly configuring the communication channels (e.g. by renewing and securing keys);
- subjecting access to the information system that processes the data to a reliable authentication of the user;
- authenticating the various devices taking part in communication (onboard calculators, sensors, servers, users, third parties, etc.);
- the implementation of a robust and secured process for updating equipment;
- effective partitioning of the various domains and subdomains taking part in processing (the vehicle's vital functions, communication functions, etc.) linked to implementing filtering measures; and
- in the case of password-based authentication, application of the Commission's recommendations of 22 June 2017 (cf. discussion no. 2017-190 of 22 June 2017);
- detecting an intrusion into the information system, and the option to function in downgraded mode in case of attack.

Security measures shall be adapted to the risks posed by the processing. Accordingly, taking account of the fact that local data processing (scenario No. 1 "IN → IN") presents fewer risks from a security point of view than data processing outside the vehicle (scenarios Nos. 2 and 3), security requirements could then be streamlined when the data are processed within the vehicle.

However, whatever their location, the sensitivity of certain data (e.g. data likely to reveal criminal offences) imposes an additional level of requirement in matters of security, due to the consequences that the dissemination of those data could have for privacy.

Finally, security measures shall be regularly reviewed and updated relative to the state of the art and the risks bearing down on processing, particularly with regard to the severity of potential impacts on the privacy of data subjects (that seriousness being assessed with regard to the nature of the data processed) and of their likelihood. Therefore, the capacity to update security measures over time is also a challenge, especially with regard to the number of vehicles concerned and the longevity of this type of product.

What changes with the GDPR

Pursuant to article 33 of the General Data Protection Regulation, in the event of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data controller shall be responsible for notifying the CNIL of the breach as soon as possible, and, if possible, no later than 72 hours of having become aware of it. Pursuant to article 34 of the General Data Protection Regulation, the data controller shall also be responsible for giving notification thereof to the data subjects, if the breach is likely to result in a high risk to their rights and freedoms.

INFORMATION OF DATA SUBJECTS

(article 32 of the French Data Protection Act, and articles 12, 13, and 14 of the General Data Protection Regulation)

Any natural person whose personal data is collected shall be informed beforehand.

More particularly, data subjects shall be informed of:

- the identity of the data controller or of the latter's representative;
- the purposes of the processing;
- the compulsory or optional nature of responses;
- the possible consequences of not answering;
- the recipients or categories of recipients of the data;
- the existence of rights in their favour (the right to challenge, the right of access to data concerning them, and the right to rectify), as well as the contact details of the department where those rights can be exercised;
- the storage period of the categories of data processed, or, if that is not possible, the criteria used to determine that period; and
- where appropriate, data transfers to countries that are not Member States of the European Union (recipients' host countries, nature of data transferred, purpose of transfer, recipient category, and protection level offered by the third country / countries).

What changes with the GDPR

The General Data Protection Regulation reinforces the requirement to inform data subjects, and stipulates that, in addition to existing requirements, data subjects shall be given the following information in clear, simple, and easily-accessible terms:

- the contact details of the data protection officer;
- the legal basis justifying the legitimacy of the processing;
- explicit reference to the legitimate interests pursued by the data controller when those interests constitute the legal basis for processing;
- the right to request erasure of personal data or restriction of processing concerning the data subject;
- the right to data portability;
- the right to withdraw one's consent at any time;
- the right to lodge a complaint with the CNIL;
- information on the question of knowing if the requirement to provide personal data is of a regulatory or contractual character, or if it affects the signing of a contract, and if the data subject is required to provide personal data, as well as the possible consequences of not providing those data;
- the existence of automated decision-making, including profiling that produces legal effects concerning the data subject or similarly significantly affects the data subject, and, at least in like cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Furthermore, pursuant to the General Data Protection Regulation, when data have not been collected directly by the data controller, the service provider shall, in addition to the information mentioned above, also indicate the source from which the personal data originate, and, if applicable, whether those data came from publicly accessible sources. That information shall be provided within a reasonable period after obtaining the data, and no later than the first of the following dates: (i) one month after the data are obtained, having regard to the specific circumstances in which the personal data are processed, (ii) upon first communication with the data subject, or (iii) if those data are transmitted to a third party, before the transmission of the data.

The information can be provided together with standardised icons, in order to provide, in relation to the planned processing, a good overview that is easily visible, understandable, and clearly legible.

CLARIFICATION

The information provided to the data subjects may be provided in layers, *i.e.*, by separating two levels of information: on the one hand, first-level information, which are the most important for the data subjects, and, on the other hand, information that presumably are of interest at a later stage. The essential first-level information includes, in addition to the identity of the data controller, the purpose of the processing, as well as any additional information that is needed to guarantee fair processing of information relative to the data subjects (cf. opinion No. 10 / 2004 of the Article 29 Working Party on *"more harmonised information provisions"* dated 25 November 2004).

The Commission recommends that the data subjects be informed by:

- concise and easily-understandable clauses in the contract of sale of the vehicle and / or in the contract for the provision of services; and
- by using distinct documents (e.g. the vehicle's maintenance record book or manual) or the on-board computer; and
- using standardised icons in vehicles. The Commission strongly encourages the implementation of those icons to inform the data subjects in a clear, summarised, and easily-understandable manner of the processing of their data. In addition, the Commission emphasises the importance of standardising those icons, so that the user finds the same symbols regardless of the make or model of the vehicle.

THE DATA SUBJECTS' RIGHTS

(articles 38, 39, and 40 of the French Data Protection Act, and articles 15 to 21 of the General Data Protection Regulation)

The data subject has the following rights:

- **the right to object to the processing on legitimate grounds:** individuals have the right to object to the use of their data on legitimate grounds, unless such processing is the result of a legal requirement. In this case, the data controller shall, without delay, notify the objection to any other data controller to whom said personal data have been sent;

- **the right to object that is not subject to legitimate grounds:** individuals have the right, regardless of reasons, to challenge the use of their personal data for purposes of canvassing, in particular for commercial ends. Data subjects shall be able to object before the final validation of their responses;
- **the right of access:** individuals with proof of their identity can obtain a copy of their personal data and access any available information on the origin of those data, as well as information enabling them to understand and challenge the logic involved in the automated processing, in the case of a decision based thereon and producing legal effects in relation to the data subject;
- **the right of rectification:** individuals with proof of their identity can ask the data controller to rectify personal data concerning them that are inaccurate, incomplete, equivocal, or out of date, or the collection, use, disclosure or retention is prohibited. When the data have been passed on to a third party, the data collector who rectified them shall also immediately inform the recipient, who shall in turn modify their processing.

What changes with the GDPR

In addition to the rights mentioned above, the General Data Protection Regulation introduces three new rights, *i.e.,* the right to be forgotten, the right to portability, and the right to restriction of the processing.

THE RIGHT TO BE FORGOTTEN

(article 17 of the General Data Protection Regulation)

Individuals can request the erasure of their personal data by the data controller when:

- the data are no longer necessary with regard to the purposes for which they were collected;
- the data subjects withdraw their consent (when that consent constituted the legal basis for the processing), and processing has no other legal basis;
- the data subjects object to a processing based on the performance of a task carried out in the public interest or on legitimate interests, for reasons relating to their particular situation, and there is no overriding legitimate grounds for the processing;
- the data subjects object to the processing of their data for direct marketing purposes;
- the data were unlawfully processed;
- applicable legislation requires the erasure of those data;
- the data were collected in relation to the information society services and concern a child.

When the data controller has made the data public and is required to erase them, they shall take reasonable measures with regard to the technology available and to implementation costs, to inform third parties that the data subject has requested the erasure of any links to, or copy or replication of those personal data.

The right to be forgotten does not apply if data storage is needed to exercise the right of freedom of expression, the personal data have to be erased for compliance with a legal obligation or for the performance of a task carried out in the public interest, in the field of public health, or for archiving purposes in the public interest, scientific or historical research purposes, for statistical purposes, or for the establishment, exercise, or defence of legal claims.

THE RIGHT TO DATA PORTABILITY

(article 20 of the General Data Protection Regulation)

The right to data portability enables individuals to receive personal data concerning them, in a structured, commonly-used, machine-readable format. Thereafter, the data subject can transmit those data to another data controller, or, if that is technically possible, ask for the data controller to send the personal data to the new data controller. The data controller cannot refuse the implementation of the right, which is exercised free of charge, pursuant to article 12.5 of the General Data Protection Regulation.

The presence of data relating to third parties (who are often part of the entourage of the data subject, e.g. a contact book) in the data requested as part of portability cannot by itself justify a rejection of the portability request.

However, the exercise of that right is subject to conditions.

Firstly, it can only apply to data contained in automated processing, which excludes data contained in so-called "paper" files.

Secondly, and most important, the right only applies to personal data processed on the basis of the consent of the data subject or of the performance of a contract signed by the data subject (e.g. data produced by providing a geolocation service at the driver's request). Thus, personal data processed on the sole basis of the data controller's legitimate interest cannot be subject to a portability request. As an example, technical data collected only for model optimisation by car manufacturers are not part of data that can be ported.

The guidelines of the Article 29 Working Party on "*the right to portability*" of 5 April 2017 specified the personal data covered by the right to data portability. It applies to personal data provided by the data subjects *i.e.*, transmitted to the data controller, for example by using a form (name, e-mail address, and telephone number), or by using the vehicle navigation system (the destinations to which one wishes to be guided). It also applies to personal data generated by the driver's activity (journey history, data relating to driving style, etc.).

Conversely, the right to portability does not apply to technical configurations not provided by the user (e.g. engine or injection mapping, etc.) or to data inferred by the data controller on the basis of data provided by the data subject (e.g. score relating to driving style, eco-driving score, etc.). Indeed, such data are not provided by the data subject, but created by the data controller.

As regards the transmission of personal data to another data controller, the right to portability shall not circumvent the application of sectorial regulations. Hence, the right to data portability does not render inapplicable the European regulation of 20 June 2017, as amended, whereby the transmission of information regarding the repair and maintenance of vehicles to independent operators is not necessarily free of charge and can be subject to the payment of "*reasonable and proportionate fees*".

THE RIGHT TO RESTRICTION OF PROCESSING

(article 18 of the General Data Protection Regulation)

The data subject also has the right to obtain from the controller the restriction of the processing when:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise, or defence of legal claims;
- the data subject has objected to processing based on the performance of a task carried out in the public interest or on legitimate interests, for reasons relating to their particular situation, pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing is thus restricted, such personal data shall, with the exception of storage, only be processed with the consent of the data subject, or for the establishment, exercise, or defence of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest.

Finally, article 11 of the General Data Protection Regulation provides that the data controller is not required to obtain additional information in order to identify the data subject for the sole purpose of complying with the General Data Protection Regulation. Hence, in view of data minimisation and the respect for privacy, service providers are not required to collect passengers' personal data only to enable them to exercise their rights.

DATA PROTECTION BY DESIGN AND DATA PROTECTION BY DEFAULT

(article 25 of the General Data Protection Regulation)

Article 25, section 1, of the General Data Protection Regulation requires the controller to implement data-protection principles from the product setting-up and design stage *("privacy by design")*.

In addition, article 25, section 2, of the General Data Protection Regulation provides that the controller implements appropriate technical and organisational measures to guarantee that, by default, only personal data which are necessary for each specific purpose of the processing are processed *("privacy by default")*.

Personal-data processing implemented after 25 May 2018 shall comply with those two principles.

PRIOR FORMALITIES

The processing of personal data requires the filing of a formality with the CNIL before it is implemented, unless it is specifically exempt therefrom.

The formalities to be completed (declaration, authorisation request, or request for an opinion) depend on the purpose of the processing operation and the nature of the data collected.

All formalities can be completed on line on the CNIL's website. In case of doubt over the formalities to be accomplished or over your obligations, you can make enquiries with the CNIL's departments.

NB : If an acknowledgement of receipt is received in relation to a formality completed with the CNIL, it does not exonerate the data controller from the substantive obligations set out in the French Data Protection Act.

What changes with the GDPR

With the General Data Protection Regulation, the declarative regime will be eliminated. Nevertheless, the processing of personal-data *via* connected vehicles is likely to result in a high risk to the rights and freedoms of individuals. In such a case, prior to the processing, the controller shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, analyse the risks incurred, and document their compliance in accordance with the principle of "*accountability*".

The right questions to ask prior to the processing of personal data:

1 - Is the processing legitimate, in light of my missions and the rights of the individuals?

2 - What is the purpose of this processing?

3 - How can this purpose be explained so that it is easily understood by everyone?

4 - What data do I need to attain this purpose?

5 - Can the same purpose be attained by processing less data?

6 - Until when will those data be of use to me (deadline, duration, legal obligations, or statute of limitation)?

7 - How to inform the data subjects in a clear and simple manner?

8 - How shall I guarantee the rights of the data subjects (especially the right of access, the right to object, and the right to rectify)?

9 - Have I given users complete control over their data (activating / deactivating functionalities at any time)?

10 - Have I carried out an impact assessment to define adequate security measures (technical and organisational)?

11 - Have I taken technical measures to patch rapidly security vulnerabilities?

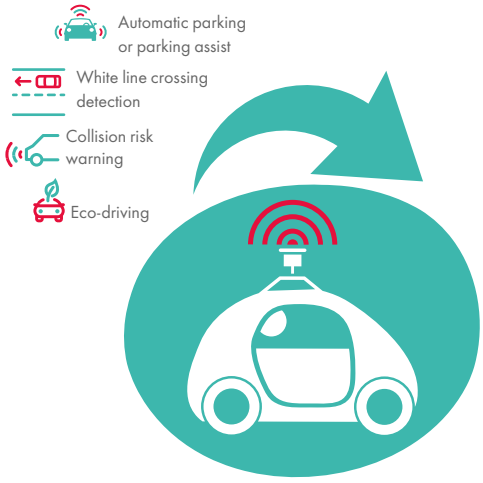
12 - What formality shall be accomplished with the CNIL?

SCENARIO N°1
IN → IN

THE VEHICLE'S DATA ARE NOT TRANSMITTED TO THE SERVICE PROVIDER.

SCOPE

In this scenario, the data collected in the vehicle remain under the user's sole control and are not transmitted to the service provider. In particular, this scenario applies in the following two cases:



1 **Purely "IN → IN" applications:** several products or solutions communicate with each other within the vehicle, without transferring data to the outside.

Example : *an eco-driving solution that processes data in the vehicle in order to display eco-driving advice in real time on the onboard computer.*

2 **Applications that involve a transfer of data from the vehicle, without such data being transmitted to the service provider. This is the case of applications for which personal data:**

- remain confined to communication networks under the user's full control (e.g. Wi-Fi, Bluetooth, or other local network); or
- circulate on telecommunication networks that are open to the public (e.g. ADSL, fibre, and GSM).

The fact that the data are transmitted on networks managed by electronic communications operators does not pose any difficulties insofar as these operators have stringent obligations as to what they can do with such traffic data. This is however only valid if the operator in question acts as the provider of the electronic communication service. Conversely, if the operator wishes to provide another service, the applicable recommendations are those of Scenarios No.2 and No.3.

Example : *a smartphone application that communicates directly with the vehicle via the onboard computer, when the vehicle's data are not transmitted to the application provider, and, conversely, when the smartphone data are not transmitted to the manufacturer.*

ANALYSIS OF THE PERSONAL DATA PROCESSING IN LIGHT OF THE FRENCH DATA PROTECTION ACT AND THE GENERAL DATA PROTECTION REGULATION

Pursuant to article 2, section 1 of the French Data Protection Act and to article 2 2° c/ of the General Data Protection Regulation, processing carried out for the performance of purely personal activities is not subject to data protection regulations.

Therefore, the French Data Protection Act does not apply to the use cases covered by this scenario, provided that the personal data are not transmitted to the service provider and that users retain full control over their data.

Users' control over their data notably involves:

- that personal data are not transmitted to the service provider;
- the deactivation (as a default setting) of the local storage of data relating to the localisation of the vehicle and relating to offences, except for real-time data-processing;
- the possibility to deactivate the functionalities at any time, except for functionalities that are strictly needed for the vehicle to function;
- in the absence of real-time processing, the option to easily access and delete usage-data (e.g. using a button inside the vehicle and / or using one's smartphone and / or using the onboard computer);
- informing users regarding data that are likely to be stored locally, as well as the data-deletion options.

CLARIFICATION

Regarding the deactivation by default, it does not exclude the option to predefine profiles that can be user-activated and for which data-collection would take place by default, so that users do not have to configure their preferences each time the vehicle is started.

Clarification : the scenario does not apply when the vehicle is provided to employees by their employer and the employer requires them to use functionalities such as eco-driving or biometric authentication. In such cases, the domestic-use exception does not apply, even if data remain stored in the vehicle.

When possible having regard to the purpose, real-time data-processing shall be preferred (e.g. eco-driving advice that does not require a data history).

SCENARIO N°1 - « IN → IN » :

The vehicle's data are not transmitted to the service provider

PURPOSES OF THE PROCESSING (NON-EXHAUSTIVE LIST)

- **Purpose 1: improving the driving experience and onboard life *("infotainment"):*** users benefit from functionalities aimed at improving their driving experience (e.g. automatic seat adjustment to the driver's height).

- **Purpose 2: improving driving from a "road safety" perspective and preventive maintenance:** users receive messages to improve their driving (e.g. audible signal or vibration of the steering wheel if overtaking a car without indicating, straying over white lines, or speeding), or to give an alert as to the state of the vehicle (e.g. an alert on the wear and tear affecting brake pads).

- **Purpose 3: automated driving assistance:** the user benefits from automated driving-assistance functions (e.g. adaptive cruise control, automatic parking, and automatic emergency braking).

- **Purpose 4: unlocking, starting, and activating certain vehicle commands using the driver's biometric data:** if users want to unlock or start their vehicle using their biometric data (e.g. their fingerprint), use voice recognition to activate certain of the vehicle's commands, or be alerted in cases of falling asleep at the wheel (e.g. by means of pressure points activated by the driver's back on the front seat).

LEGAL BASIS

This scenario involves users having full control over their data.

In the context of this scenario, the Commission considers that control over biometric data necessarily involves, on the one hand, the existence of a non-biometric alternative (e.g. using a physical key or a code) without additional constraint, and, on the other hand, storing and comparing the biometric template in encrypted form only on a local basis, with biometric data not being processed by an external reading / comparison terminal.

DATA COLLECTED

Given that the French Data Protection Act, and especially article 9 thereof, does not apply to processing performed in the course of purely personal activities, this scenario enables the processing of data relating to criminal offences, subject to such data being processed without being transmitted to the service provider.

Given the nature of such data, it is recommended that they be processed in real time and without storage, including on a local basis.

RETENTION PERIOD

The user shall at all times be able to delete all usage data stored locally in the vehicle, except for data needed for the proper functioning of the vehicle.

By default, data are stored for a period necessary for the provision of service. For example, the data needed to put together an eco-driving indicator are stored for the time needed to calculate the eco-driving index. The eco-driving index can be stored for as long as the user does not sell the vehicle or does not choose to delete the data.

The CNIL recommends that usage data stored on second-hand vehicles should be systematically deleted before those vehicles are put up for sale. Similarly, data shall be deleted before a vehicle is sent for scrapping.

RECIPIENTS

The user has sole access to the data.

INFORMING PEOPLE, AND PEOPLE'S ENTITLEMENTS

To allow users to exercise effective control over their data, they shall be informed of data that is likely to be processed locally, the purpose of the processing, and the option to, at all times, deactivate data collection and delete the data concerned.

SECURITY

The CNIL recommends that all useful precautions be taken that guarantee the security and confidentiality of personal data.

More specifically, the Commission recommends:

- authenticating data-receiving devices;
- making access to data subject to reliable user authentication (for password authentication, applying the Commission's recommendations of 22 June 2017, electronic certificate, etc.).

The measures thus put in place shall be adapted to the level of data sensitivity and to devices' control capacity. Thus, for processing data that relate to criminal offences, the Commission recommends that strong security measures be put in place, such as:

- data encryption using state-of-the-art algorithms, by the user in person, e.g. by means of a secret held by the latter;
- regularly renewing encryption keys;
- protecting encryption keys from being accidentally revealed;
- protection against being read by unauthorised persons;
- physical protection against those data being modified by a third party.

In the case of biometric data, in addition to the measures above, it is important to ensure that the biometric authentication solution is sufficiently reliable, in particular by checking that:

- the adjustment of the biometric solution used (e.g. the rate of false positives and false negatives) is adapted to the security level of the required access control;
- the biometric solution used is based on a sensor that is resistant to attacks that are deemed trivial in the state of the art (such as, at the current time, the use of a flat-printed print for fingerprint recognition);
- the number of authentication attempts is limited;
- only the biometric template is stored on the device, in an encrypted form using a cryptographic algorithm and key management that comply with the state of the art; and
- the raw data used to make up the biometric template and for user authentication are processed in real time without being stored locally (e.g. sound recordings in the case of a voice-recognition system).

If communication between the vehicle and the smartphone is done *via* telecommunication networks, the Commission recommends that the communication channel be encrypted using a state-of-the-art algorithm.

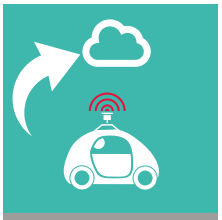
PRIOR FORMALITIES

Since processing has been implemented for the performance of solely personal activities, there are no formalities to be completed with the CNIL.

CLARIFICATION

Scenario No. 1 offers the following advantages:

- it gives users a good level of control over their data, which is a factor of trust and acceptability of the products;
- it enables the processing of data (notably data relating to criminal offences and biometric data) which otherwise would be subject to the strict rules provided in scenarios Nos. 2 and 3;
- it presents fewer risks of piracy and involves little latency, which makes it particularly suited to automated driving-assistance functions;
- for certain data, it involves streamlined security measures as compared to scenarios Nos. 2 and 3;
- its implementation does not involve any prior formality with the CNIL.



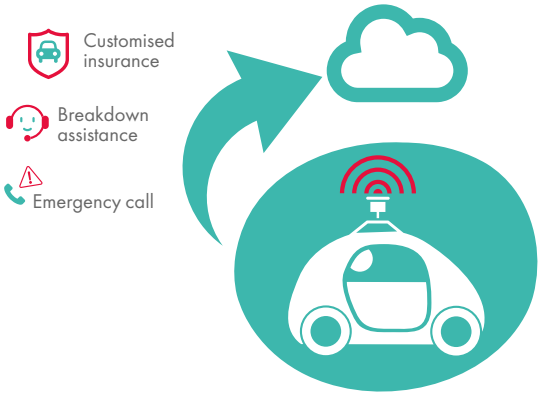
SCENARIO N°2
IN → OUT

THE VEHICLE'S DATA ARE TRANSMITTED TO THE SERVICE PROVIDER WITHOUT AUTOMATIC ACTION BEING TRIGGERED IN THE VEHICLE.

SCOPE

This scenario covers cases in which the data collected are transmitted to the service provider, for example in order to provide an added-value service to the user or to improve the products.

It concerns the case in which a service functions remotely, but does not trigger an automatic action in the vehicle (unlike scenario No. 3).



ANALYSIS OF THE PROCESSING OF PERSONAL DATA IN LIGHT OF THE FRENCH DATA PROTECTION ACT AND THE GENERAL DATA PROTECTION REGULATION

Any person who wishes to process personal data shall comply with a certain number of legal obligations.

PURPOSES OF THE PROCESSING (NON-EXHAUSTIVE LIST)

- **Purpose 1: model optimisation and product improvement:** a service provider compiles statistics on the vehicle's functioning parameters or on the wear and tear affecting the vehicle's parts, based on the usage data of the data subject.
- **Purpose 2: accidentology studies:** data subjects voluntarily agree to take part in accidentology studies aimed at better understanding the causes of road accidents.
- **Purpose 3: commercial use of the vehicle's data:** data subjects contract with a service provider in order to obtain added-value services relating to their vehicle (e.g. a "*Pay As You Drive*" insurance contract or breakdown assistance).
- **Purpose 4: "*e-Call*":** in the event of a serious accident in European Union territory, the vehicle automatically triggers an "*eCall*" to 112, the EU-wide emergency number.
- **Purpose 5:** fighting theft: data subjects wish, in case of theft, to find their vehicle thanks to geolocation. Using location data is limited to the strict needs of the investigation and to the case assessment by the competent legal authorities.

SCENARIO N°2 - « IN → OUT » :

The vehicle's data are transmitted to the service provider without automatic action being triggered in the vehicle

LEGAL BASIS

- **For purpose 1** (model optimisation and product improvement), if the data used for the processing are anonymised, they are no longer personal data, so they can be used freely. Anonymisation involves the irreversible deletion of the link between usage data and the vehicle's serial number, making it impossible for the data subjects to be re-identified. Failing anonymisation, legitimate interest can constitute a legal basis for compiling statistics, subject to data being pseudonymised (e.g. by using an irreversible hash algorithm with a secret key that shall be regularly renewed, or by using asymmetric encryption) and minimised (e.g. data being "physically" collected only during technical checks, not on a remote and continuous basis).

- **For purpose 2** (accidentology studies), the legal basis for processing is the consent of the data subject.

- **For purpose 3** (commercial use of the vehicle's data): the legal basis for processing is the performance of a contract to which the data subject is a party. That legal basis is materialised by the data subject signing the contract with a service provider for a specific service. If the service provider is the car manufacturer, the contract of provision of service shall be separate from the contract of sale of the vehicle. The sale of the vehicle cannot be made subject to signing the service contract and to accepting that the car manufacturer collects vehicle's data.

CLARIFICATION

If the service provider is the car manufacturer, the contract of provision of service shall be separate from the contract of sale of the vehicle. The sale of the vehicle cannot be made subject to signing the service contract and to accepting that the car manufacturer collects vehicle's data.

- **For purpose 4** (*"eCall"*): with effect from April 2018, the legal basis for processing shall be compliance with a legal obligation (i.e., regulation EU 2015 / 758 of 29 April 2015 concerning type-approval requirements for the deployment of the *"eCall"* in-vehicle system based on the 112 service, and amending Directive 2007 / 46 / EC).

- **For purpose 5** (fighting theft): the legal basis for processing is the consent of the vehicle's owner, or, if applicable, the performance of a contract.

Consent shall be an expression of the free, specific, and informed will of the person whose data are being processed (e.g. ticking a box that is not pre-ticked, or configuring the onboard computer to activate a function in the vehicle). Freedom to give consent involves the option of withdrawing consent at any time, of which the data subject shall be expressly informed. Withdrawal of consent shall lead to the processing being stopped. The data shall then be deleted from the active database, or anonymised, or archived.

In addition, pursuant to article 1 of the French Data Protection Act, data subjects shall be able to decide upon and to control the use made of their personal data.

That control includes in particular:

- configurations by default that protect privacy;
- the option for users to easily modify those configurations, during the entire processing, especially for the purpose of activating or deactivating services based on consent or on the performance of a contract (e.g. commercial offers personalised on the basis of geolocation or breakdown assistance);
- where appropriate, the option for users to adjust the level of detail of the data collected to the level of service requested, e.g. by accessing a map without being geolocated if they do not wish to be guided; and
- the option for users to access those data easily.

CLARIFICATION

geolocation data are particularly revealing of the life habits of the data subjects. The journeys carried out are very characteristic in that they enable to infer the place of work and of residence to be deduced, as well as the driver's centres of interest (leisure, and, possibly, religion through the place of worship, or sexual orientation through the places visited).

Accordingly, the service provider shall be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purpose of processing. In particular, when the processing consists in detecting the vehicle's movement, the gyroscope is sufficient to fulfil that function, without there being a need to collect location data.

In general and except in the case of legal obligation, collecting geolocation data is subject to compliance with the following principles:

- obtaining specific consent that is distinct from the general conditions of sale or use, e.g. on the onboard computer;
- adequate configuration of the detail of geolocation relative to the purpose of processing (for example, a weather application should not be able to access the vehicle's geolocation every second, even with the consent of the data subject);
- the option to deactivate geolocation at any time;
- activating geolocation only when the user launches a functionality that requires the vehicle's location to be known, and not by default and continuously when the car is started;
- informing the user that geolocation has been activated, in particular by using icons (e.g. an arrow that moves across the screen);
- providing accurate information on the purpose of processing (e.g. is geolocation history stored? If so, what is its purpose?);
- defining a limited storage period.

These rules do not apply to geolocating employees' vehicles, for which the CNIL has published specific rules under simplified regulation NS-51 (cf. deliberation no. 2015-65 of 4 June 2015 on adopting a simplified regulation on the automated processing of personal data implemented by public or private bodies and intended to geolocate vehicles used by their employees).

DATA COLLECTED

The data control shall only collect personal data that are strictly necessary for the processing. In the case of a contract for the provision of services, the only data that can be collected are those that are essential for the provision of service.

Concerning data relating to criminal offences:

- **For purpose 1** (model optimisation and product improvement) **and 3** (commercial use of the vehicle's data): except in the case of specific legal provision, data that are likely to reveal criminal offences shall not be processed by legal persons who do not administer a public service, except to defend their rights in court. However, that data can be processed locally, directly in the vehicle, in accordance with scenario No. 1, in order to give the user control over that particularly sensitive data and limit as much as possible the consequences on privacy.

- **For purpose 2** (accidentology studies): scientific research linked to accidentology justifies the collection of the instantaneous speed, including by legal persons who do not administer a public service in the strict sense. In general, the CNIL deems it relevant to store only recordings of the 45 seconds before the reference event or sequence, and of the 15 seconds after the reference event or sequence.

Clarification: the Commission considers instantaneous speed not to be offence-related data by nature, in that it is not sufficient on its own to establish a criminal offence. Indeed, to deduce from the instantaneous speed that an offence has been committed, it is necessary to combine the instantaneous speed and the vehicle's location as speed limits vary according to the type of roads (city centre, national road, motorway, etc.). However, instantaneous speed is offence-related data by destination, *i.e.*, it may come under article 9 of the French Data Protection Act, because of the purpose for which it is collected. In the specific case of scientific research in the field of accidentology, the Commission considers that instantaneous speed is not offence-related data by destination, which justifies the collection of instantaneous speed by legal persons who do not administer a public service in the strict sense.

Concerning location data:

- **For purpose 1** (model optimisation and product improvement), processing an accurate and detailed geolocation appears excessive under article 6-3° of the French Data Protection Act.

- **For purposes 3** (commercial use of the vehicle's data) **and 8** (fighting theft), location data cannot be collected continuously but only when the client activates the service. For example, for breakdown assistance, location data can only be passed on from the time when the client requests an intervention. Similarly, for purpose 5 (fighting theft), location data can only be transmitted as of the declaration of theft, and cannot be collected continuously the rest of the time.

RETENTION PERIOD

- **For purpose 1** (model optimisation and product improvement): in case of pseudonymisation, the French Data Protection Act continues to apply, and the data cannot be retained for an unlimited period. In that case, a storage period of 3 years seems proportionate given the purpose of the processing. It is reminded that accurate and detailed geolocation is expressly excluded from the scope of data that can be processed for purpose 1. Once anonymised, usage data can be retained for an unlimited period.

- **For purpose 2** (accidentology studies): it is important to distinguish between two types of data:
  - **Data relating to participants and vehicles:** those data can be retained for the duration of the study.
  - **Technical data from vehicles:** the CNIL recommends that those data be retained for no more than 5 years from the end date of the study. At the end of that period, the data shall be deleted or anonymised.

- **For purpose 3** (commercial use of the vehicle's data), requiring the signing of a contract for the provision of service, it is important to distinguish between two types of data:
  - **Commercial data** (the person's identity, transaction-related data, data relating to means of payment, etc.): those data can be retained in an active database for the full duration of the contract. At the end of the contract, they can be archived physically (on a separate medium: CD-ROM, etc.) or logically (by authorisation management) to prevent possible litigation. Thereafter, at the end of the statutory limitation periods, the data shall be deleted or anonymised.
  - **Usage data:** those data shall be stored for a limited period in detailed form, then they shall be aggregated for the remaining duration of the contract.

- **For purpose 4** *("eCall")*: EU regulation 2015 / 758 of 29 April 2015 stipulates that data shall not be retained for longer than is needed for processing emergency situations. Those data shall be completely deleted when they are no longer needed for that purpose. Furthermore, in the internal memory of the "*eCall*" system, data shall be automatically and constantly deleted. Only the vehicle's last three positions can be stored, insofar as it is strictly necessary to specify the current position of the vehicle and the direction of travel at the time of the event.

- **For purpose 5** (fighting theft): location data can only be retained for the period during which the case is assessed by the competent legal authorities, or until the end of a procedure to dispel doubt that does not end with confirmation of the theft of the vehicle.

RECIPIENTS AND DATA PROCESSORS

In principle, only the data controller and the data subject have access to the data. However, the data controller can transmit personal data to a data processor or to a commercial partner (recipient).

- **Transmitting data to a data processor:** the service provider can freely transmit personal data to the data processor selected to play a part in providing the service to the data subject, it being specified that the data processor shall not use those data for its own account. In that case, the service provider, acting as data controller, is responsible for the conditions under which data is processed by the data processor.

- **Transmitting data to a commercial partner:**
  - **If the data transmitted are anonymous data:** the service provider can freely transmit such data to a commercial partner. In that case, neither the service provider nor the commercial partner have obligations under the French Data Protection Act, which does not apply to anonymous data;
  - **If the data transmitted are personal data:** in view of the possible sensitivity of the vehicle-usage data (journeys made, driving style, etc.), the CNIL recommends that the data subject's consent be systematically obtained before their data are transmitted to a commercial partner (e.g. by ticking a box that is not pre-ticked, or, where technically possible, by using a physical or logical device that the person can access from the vehicle). The commercial partner in turn becomes the data controller for the data that it receives, and is subject to all the provisions of the French Data Protection Act.

- **For purpose 3** (commercial use of the vehicle's data): the CNIL recommends that, as far as possible, the vehicle's usage data should be processed directly in telematics boxes, so that the service provider only accesses the results data (e.g. a score), not detailed raw data.

- **For purpose 5** (fighting theft): in the event of a theft declaration, location data can be passed on the (i) approved officers of the remote-surveillance platform, and (ii) to the legally-approved authorities.

INFORMATION OF DATA SUBJECTS

Prior to the processing of personal data, the data subject shall be informed of the identity of the data controller, the purpose of processing, the data recipients, the period for which data will be stored, and the person's rights under the French Data Protection Act.

- **For purpose 1** (model optimisation and product improvement), 3 (commercial use of the vehicle's data) and 5 (combating): that information can be provided when the contract is signed.

- **For purpose 2** (accidentology studies), in the case of collecting offence-related data, the data subjects shall be specifically informed of the data collection. That information can be given on signing the form to agree to take part in the accidentology study.

- **For purpose 4** *("eCall")*, EU regulation 2015 / 758 of 29 April 2015 stipulates that, in user manuals, manufacturers shall provide clear and complete information on data processing done using the "*eCall*" system.

  That information includes:
  - reference to the legal basis for processing;
  - the fact that the "*eCall*" is activated by default;
  - the conditions under which data are processed by the "*eCall*" system;
  - the specific aim of "*eCall*" processing, which is limited to emergency situations;

- the types of data collected and processed, as well as the recipients of those data;
- the period for storing data in the "*eCall*" system;
- the fact that the vehicle is not under constant surveillance;
- the conditions for the data subjects to exercise their rights, as well as the competent contact department for processing access requests;
- any additional information needed in relation to traceability, surveillance, and processing personal data in relation to providing an "*eCall*" handled by third-party services and / or other added-value services, that being subject to the explicit agreement of the owner and being compliant with directive 95 / 46 / EC. Particular attention is paid to the fact that differences can exist between data-processing using the onboard "*eCall*" system based on the number 112, and the onboard "*eCall*" systems handled by third-party services or other added-value services.

Regulation EU 2015 / 758 of 29 April 2015 stipulates that before the system is used, the information shall be provided in an owner's manual separate from those relating to the "*eCall*" systems handled by third-party services.

Furthermore, pursuant to the General Data Protection Regulation, the service provider shall also provide the data subjects with the following information, in clear, simple, and easily-accessible terms:

- the contact details of the data protection officer;
- the explicit mention of the legitimate interests pursued by the controller, when such legitimate interests constitute the legal basis for processing;
- the right to request erasure of personal data or restriction of processing concerning the data subject;
- the right to data portability;
- the right to withdraw one's consent at any time;
- the right to lodge a complaint with the CNIL;
- information on the question of knowing if the requirement to provide personal data is of a regulatory or contractual character, or if it affects the signing of a contract, and if the data subject is required to provide personal data, as well as the possible consequences of not providing those data;
- the existence of automated decision-making, including profiling that produces legal effects concerning the data subject or similarly significantly affects the data subject, and, at least in like cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Furthermore, pursuant to the General Data Protection Regulation, when data have not been collected directly by the data controller, the service provider shall, in addition to the information mentioned above, also indicate the source from which the personal data originate, and, if applicable, whether those data came from publicly accessible sources. That information shall be provided within a reasonable period after obtaining the data, and no later than the first of the following dates: (i) one month after the data are obtained, having regard to the specific circumstances in which the personal data are processed, (ii) upon first communication with the data subject, or (iii) if those data are transmitted to a third party, before the transmission of the data.

The information can be provided together with standardised icons, in order to provide, in relation to the planned processing, a good overview that is easily visible, understandable, and clearly legible.

Clarification: the information provided to the data subjects may be provided in layers, i.e., by separating two levels of information: on the one hand, first-level information, which are the most important for the data subjects, and, on the other hand, information that presumably are of interest at a later stage. The essential first-level information includes, in addition to the identity of the data controller, the purpose of the processing, as well as any additional information that is needed to guarantee fair processing of information relative to the data subjects (cf. opinion No. 10 / 2004 of the Article 29 Working Party on *"more harmonised information provisions"* dated 25 November 2004).

The Commission recommends that the data subjects be informed by:

- concise and easily-understandable clauses in the contract of sale of the vehicle and / or in the contract for the provision of services; and
- by using distinct documents (e.g. the vehicle's maintenance record book or manual) or the on-board computer; and
- using standardised icons in vehicles. The Commission strongly encourages the implementation of those icons to inform the data subjects in a clear, summarised, and easily-understandable manner of the processing of their data. In addition, the Commission emphasises the importance of standardising those icons, so that the user finds the same symbols regardless of the make or model of the vehicle.

THE DATA SUBJECTS' RIGHTS

Data subjects are entitled to exercise the right of access, the right to object, and the right to correct their data. The service provider shall allow the data subjects to exercise their right of access in the most effective way possible, knowing that the right of access covers all the personal data held by the service provider.

- **For purpose 1** (model optimisation and product improvement), when the legal basis for the processing is the legitimate interest of the data controller, pursuant to article 21 of the General Data Protection Regulation, data subjects also have the right to challenge the processing at any time for reasons relating to their particular situation. In that case, the data controller shall stop processing the personal data of the data subject, unless it is possible to prove the existence of overriding legitimate grounds for the processing that take precedence over the rights and freedoms of the data subject, or for establishing, exercising, or defending legal claims.

In addition to the rights mentioned above, the General Data Protection Regulation introduces three new rights, *i.e.,* the right to be forgotten, the right to portability, and the right to restriction of processing (cf. the introduction of the pack).

SECURITY

The service provider shall be able to put in place measures that guarantee the security and confidentiality of processed data, and to take all useful precautions to prevent control being taken by an unauthorised person, in particular by:

- encrypting the communication channels by means of a state-of-the-art algorithm;
- putting in place an encryption-key management system that is unique to each vehicle, not to each model;
- encrypting data in the database by means of state-of-the-art algorithms;
- protecting encryptions keys from any accidental disclosure;
- authenticating data-receiving devices;
- ensuring data integrity (e.g. by hashing);
- make access to personal data subject to reliable user authentication (password, electronic certificate, etc.);
- applying the Commission's recommendations of 22 June 2017, in the case of password-based authentication (cf. deliberation No. 2017-190).

Concerning more specifically car manufacturers, the Commission recommends the implementation of the following security measures:

- partitioning the vehicle's vital functions from those always connected to the internet (e.g. *"infotainment");*
- implementing technical measures that enable to rapidly patch security vulnerabilities;
- for the vehicle's vital functions, give priority as much as possible to using secure frequencies that are specifically dedicated to transport;
- setting up an alarm system in case of attack, with the possibility of operating in downgraded mode;
- storing a log history going back six months, in order to enable the origin of the attack to be understood.

The measures put in place shall be adapted to the level of data sensitivity. Thus, if instantaneous speed is collected as part of accidentology studies, the Commission recommends putting in place strong security measures, such as:

- implementing pseudonymisation measures (e.g. secret-key hashing of data like the surname / first name of the data subject and the serial number); and
- storing data relating to instantaneous speed and to geolocation in separate databases (e.g. using a state-of-the-art encryption mechanism with distinct keys and approval mechanisms); or
- deleting geolocation data as soon as the reference event or sequence is qualified (e.g. the type of road, day / night), and the storage of directly-identifying data in a separate database that can only be accessed by a small number of people.

- **For purpose 1** (model optimisation and product improvement), anonymisation measures or, as a minimum, pseudonymisation measures shall be put in place.

- **As regards purpose 4** *("eCall")*, EU regulation 2015 / 758 of 29 April 2015 stipulates the requirement to incorporate into the *"eCall"* system technologies that strengthen the protection of privacy, in order to offer users the appropriate level of protection of privacy, as well as the guarantees needed to prevent surveillance and abusive uses. In addition, manufacturers shall ensure that the *"eCall"* system based on the number 112, as well as any other system providing an *"eCall"* that is handled by third-party services or an added-value service, are so designed that it is impossible for personal data to be exchanged between those systems.

As regards measures to be put in place in infrastructures that are outside the vehicle, the service provider shall carry out a study of the risks engendered by processing, in order to determine and implement the measures needed to protect people's privacy. The CNIL provides a method of that type on its web site (https://www.cnil.fr/fr/PIA-privacy-impact-assessment), but other equivalent methods can be used.

Finally, the service provider shall develop products and services by incorporating, from the outset, the problem of personal data *("privacy by design")*. At the very least, the product or service shall limit the vehicle's data output to that which is strictly necessary for the provision of service, and give priority to decisions taken locally over those taken outside the vehicle. The service provider shall also prioritise data anonymisation as early as possible in the collection chain. In the case of anonymised data, it is restated that the French Data Protection Act no longer applies, so the data can be stored and exchanged in an unlimited manner.

PRIOR FORMALITIES

The data controller shall file a normal declaration with the CNIL, except if processing criminal offence-related data, in which case the CNIL's prior authorisation is necessary.

The CNIL considers that the processing of personal data collected via connected vehicles may present risks in terms of privacy within the meaning of the General Data Protection Regulation. Accordingly, in such a case, the service provider shall carry out an impact assessment and analyse the risks incurred, in order to implement measures that enable those risks to be limited.

In addition, pursuant to article 33 of the General Data Protection Regulation, in the event of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data controller shall be responsible for notifying the CNIL of the breach as soon as possible, and, if possible, no later than 72 hours of having become aware of it. Pursuant to article 34 of the General Data Protection Regulation, the data controller shall also be responsible for giving notification thereof to the data subjects, if the breach is likely to result in a high risk to their rights and freedoms.

CLARIFICATION

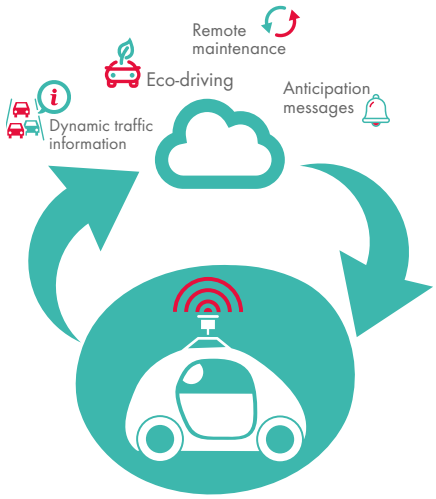
In particular, that scenario is intended to be used when processing personal data requires calculating power that cannot be mobilised locally in the vehicle, or when processing personal data is not in itself sufficient for the provision of service, and requires the service provider to carry out further analysis.

SCENARIO N°3
IN → OUT → IN

THE VEHICLE'S DATA ARE TRANSMITTED TO THE SERVICE PROVIDER TO REMOTELY TRIGGER AN AUTOMATIC ACTION IN THE VEHICLE.

SCOPE

The scenario covers cases in which the data collected are passed on to the service provider to remotely trigger an automatic action in the vehicle.



ANALYSIS OF THE PROCESSING OF PERSONAL DATA IN LIGHT OF THE FRENCH DATA PROTECTION ACT AND THE GENERAL DATA PROTECTION REGULATION

Any person who wishes to process personal data shall comply with a certain number of legal obligations.

PURPOSES OF THE PROCESSING (NON-EXHAUSTIVE LIST)

- **Purpose 1: remote maintenance:** data subjects enter into a contract with a service provider in order to receive messages or alerts relating to the vehicle's functioning (e.g. an alert on the state of brake wear, or a reminder of the technical-inspection date), or remotely receive technical updates in the vehicle.
- **Purpose 2: improving the driving experience:** data subjects wish to benefit from services in order to improve their driving experience (e.g. dynamic traffic information with a new route being sent after an incident along the road, early-warning messages, or eco-driving alerts).

LEGAL BASIS

- **For purposes 1 (remote maintenance) and 2 (improving the driving experience),** the legal basis for processing is the performance of the contract that the data subject chose to sign.

Pursuant to article 1 of the French Data Protection Act, data subjects shall be able to decide upon and to control the use that is made of their personal data. That control includes, in particular:

- configurations by default that protect privacy;
- the option for users to easily change those configurations, during the entire processing, especially for the purpose of deactivating services based on consent or on the performance of a contract (e.g. dynamic traffic information);
- where appropriate, the option for users to adjust the level of detail of the data collected to the level of service requested, e.g. by accessing a map without being geolocated if they do not wish to be guided; and
- the option for users to access those data easily.

SCENARIO N°3 - « IN → OUT → IN » :

The vehicle's data are transmitted to the service provider to remotely trigger an automatic action in the vehicle

DATA COLLECTED

The data control shall only collect personal data that are strictly necessary for the processing. In the case of a contract for the provision of service, the only data that can be collected are those that are essential for the provision of service.

As an example, accurate and detailed geolocation cannot be processed for purpose 1 (remote maintenance).

As part of this scenario, and except for specific legal provisions, data that are likely to reveal criminal offences cannot be processed by legal persons who do not administer a public service, except to defend their rights in court. However, those data can be processed locally, directly in the vehicle, in accordance with scenario No. 1, so as to give the user control over that particularly sensitive data and limit as much as possible the risks of impact on privacy.

RETENTION PERIOD

It is important to distinguish between two types of data:

- **Commercial data (the person's identity, transaction-related data, data relating to means of payment, etc.):** those data can be retained in an active database for the full duration of the contract. At the end of the contract, they can be archived physically (on a separate media: CD-ROM, etc.) or logically (by authorisation management) to prevent possible litigation. Thereafter, at the end of the statutory limitation periods, the data shall be deleted or anonymised.
- **Usage data:** those data shall be retained for a limited period in detailed form, then they shall be aggregated for the remaining duration of the contract. However, for purpose 1 (remote maintenance), data relating to interventions on the vehicle can be retained for the life of the vehicle.

RECIPIENTS AND DATA PROCESSORS

In principle, only the service provider and the data subject can have access to the data. However, the data controller can transmit personal data to the data processor selected to play a part in providing the service to the data subject, it being specified that the data processor shall not use those data for its own account. In that case, the service provider, acting as data controller, is responsible for the conditions under which data is processed by the data processor.

INFORMATION OF DATA SUBJECTS

Prior to the processing of personal data, the data subject shall be informed of the identity of the data controller, the purpose of processing, the data recipients, the period for which data will be stored, and the person's rights under the French Data Protection Act. That information can be provided when the data subject signs a contract for the provision of service.

Furthermore, pursuant to the General Data Protection Regulation, the service provider shall also provide the data subjects with the following information, in clear, simple, and easily-accessible terms:

- the contact details of the data protection officer;
- the explicit mention of the legitimate interests pursued by the controller, when such legitimate interests constitute the legal basis for processing;
- the right to request erasure of personal data or restriction of processing concerning the data subject;
- the right to data portability;
- the right to withdraw one's consent at any time;
- the right to lodge a complaint with the CNIL;
- information on the question of knowing if the requirement to provide personal data is of a regulatory or contractual character, or if it affects the signing of a contract, and if the data subject is required to provide personal data, as well as the possible consequences of not providing those data;
- the existence of automated decision-making, including profiling that produces legal effects concerning the data subject or similarly significantly affects the data subject, and, at least in such cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Furthermore, when data have not been collected directly by the data controller, the service provider shall, in addition to the information mentioned above, also indicate the source from which the personal data originate, and, if applicable, whether those data came from publicly accessible

sources. That information shall be provided within a reasonable period after obtaining the data, and no later than the first of the following dates: (i) one month after the data are obtained, having regard to the specific circumstances in which the personal data are processed, (ii) upon first communication with the data subject, or (iii) if those data are transmitted to a third party, before the transmission of the data.

> **Clarification :** the information provided to the data subjects may be provided in layers, i.e., by separating two levels of information: on the one hand, first-level information, which is the most important for the data subjects, and, on the other hand, information that presumably is of interest at a later stage. The essential first-level information includes, in addition to the identity of the data controller, the purpose of the processing, as well as any additional information that is needed to guarantee fair processing of information relative to the data subjects (cf. opinion No. 10 / 2004 of the Article 29 Working Party on "*more harmonised information provisions*" dated 25 November 2004).

The Commission recommends that the data subjects be informed by:

- concise and easily-understandable clauses in the contract of sale of the vehicle and / or in the contract for the provision of services; and
- by using distinct documents (e.g. the vehicle's maintenance record book or manual) or the on-board computer; and
- using standardised icons in vehicles. The Commission strongly encourages the implementation of those icons to inform the data subjects in a clear, summarised, and easily-understandable manner of the processing of their data. In addition, the Commission emphasises the importance of standardising those icons, so that the user finds the same symbols regardless of the make or model of the vehicle.

THE DATA SUBJECTS' RIGHTS

Data subjects are entitled to exercise the right of access, the right to object, and the right to correct their data. The service provider shall allow the data subjects to exercise their right of access in the most effective way possible, knowing that the right of access covers all the personal data held by the service provider.

In addition to the rights mentioned above, the General Data Protection Regulation introduces three new rights, *i.e.*, the right to be forgotten, the right to portability, and the right to restriction of processing (cf. the introduction of the pack).

SECURITY

The service provider shall be able to put in place measures that guarantee the security and confidentiality of processed data, and to take all useful precautions to prevent control being taken by an unauthorised person, in particular by:

- encrypting the communication channels by means of a state-of-the-art algorithm;
- putting in place an encryption-key management system that is unique to each vehicle, not to each model;
- encrypting data in the database by means of state-of-the-art algorithms;
- protecting encryptions keys from any accidental disclosure;
- authenticating data-receiving devices;
- making access to personal data subject to reliable user authentication (password, electronic certificate, etc.);
- authenticating devices that issue actions aimed at the vehicle;
- applying the Commission's recommendations of 22 June 2017, in the case of password-based authentication (cf. deliberation No. 2017-190).

SCENARIO N°3 - « IN → OUT → IN » :

The vehicle's data are transmitted to the service provider to remotely trigger an automatic action in the vehicle

Concerning more specifically car manufacturers, the Commission recommends the implementation of the following security measures:

- partitioning the vehicle's vital functions from those always connected to the internet (e.g. *"infotainment");*
- implementing technical measures that enable to rapidly patch security vulnerabilities;
- for the vehicle's vital functions, give priority as much as possible to using secure frequencies that are specifically dedicated to transport;
- setting up an alarm system in case of attack, with the possibility of operating in downgraded mode;
- storing a log history going back six months, in order to enable the origin of the attack to be understood.

The measures put in place shall be adapted to the level of data sensitivity and to the control capacity of the devices.

As regards measures to be put in place in infrastructures that are outside the vehicle, the service provider shall carry out a study of the risks engendered by processing, in order to determine and implement the measures needed to protect people's privacy. The CNIL provides a method of that type on its web site (https://www.cnil.fr/fr/PIA-privacy-impact-assessment), but other equivalent methods can be used.

Finally, the service provider shall develop products and services by incorporating, from the outset, the problem of personal data *("privacy by design")*. At the very least, the product or service shall limit the vehicle's data output to that which is strictly necessary for the provision of service, and give priority to decisions taken locally over those taken outside the vehicle. The service provider shall also prioritise data anonymisation as early as possible in the collection chain. It is restated that in the case of anonymised data, the French Data Protection Act no longer applies, so the data can be stored and exchanged in an unlimited manner.

PRIOR FORMALITIES

The data controller shall file a normal declaration with the CNIL. This declaration shall be filed on the CNIL's web site (https://www.cnil.fr/).

The CNIL considers that the processing of personal data collected *via* connected vehicles may present risks in terms of privacy within the meaning of the General Data Protection Regulation. Accordingly, in such a case, the service provider shall carry out an impact assessment and analyse the risks incurred, in order to implement measures that enable those risks to be limited.

In addition, pursuant to article 33 of the General Data Protection Regulation, in the event of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data controller shall be responsible for notifying the CNIL of the breach as soon as possible, and, if possible, no later than 72 hours after having become aware of it. Pursuant to article 34 of the General Data Protection Regulation, the data controller shall also be responsible for giving notification thereof to the data subjects, if the breach is likely to result in a high risk to their rights and freedoms.

CLARIFICATION

In particular, that scenario is intended to be used when processing personal data requires calculating power that cannot be mobilised locally in the vehicle, or when the provision of service requires additional data that are external to the vehicle.