Data Privacy Compliance Report

Cloud Enhanced Vehicle Intelligent Sensor Sharing Project - CEVISS

Processing of personal data in the context of hazard detection, accident prevention and rescue support, according to the GDPR

Disclaimer:

This Data Privacy Compliance Report is provided for general information purposes only. It does not offer advice on which the recipients of the Data Privacy Compliance Report or any other person, company or third party should rely. Professional or specialist advice must be obtained before taking, or refraining from, any action based on information obtained from CEVT in this Data Privacy Compliance Report. CEVT makes no representations, warranties or guarantees, whether express or implied, that any information in this Data Privacy Compliance Report is accurate, complete or up to date.

Although CEVT has created the Data Privacy Compliance Report based on best knowledge of its colleagues and with the aim to provide with accurate and practical content, we recommend of getting professional or specialist advice on the topic.

Table of Contents

Executive Summary

Data privacy requirements and practices must be considered carefully when personal data are affected as part of certain technical solutions, especially in connected vehicles. Data privacy regulations globally, like the GDPR in the European Union should serve as enablers for implementation of new technologies which can – as in the current scope - contribute to road safety, enhance optimal usage of roads and support police or rescue operations when required.

One of the findings of this Data Privacy Compliance Report is that, data and personal data processing related to solutions connected to these special areas should be further regulated and harmonized on an EU-level or even beyond. In general, GDPR allows to use such innovative solutions in connected vehicles, but there are certain limitations for the personal data usage. These limitations come from uncertainties around interpretation of GDPR in these specific new innovative areas, but they also arise due to lack of harmonization of related regulations in the EU which shall be applied beside the GDPR for privacy (not necessarily data privacy).

It is also a question how these technical solutions and the related data usage would be perceived by the public and if it would be considered by people as an invasion to privacy.

Therefore, to eliminate data privacy related uncertainties, it is recommended to further investigate into the topic and identify potential regulatory measures which can be implemented on an EU-level (or beyond) and would require the usage of the solutions in vehicles which are mentioned in this Data Privacy Compliance Report.

In the current EU data privacy regulatory environment our view is that each person shall be given the freedom to choose, if they want to use these technical solutions related to road safety, road management and certain supports, or not. Even if people decide to opt-in, they shall have the possibility to change their view later.

Another aspect is that EU Member States might have national regulations or practices which would allow or block the usage of these type of solutions and that would need to be reviewed on a country-by-country level.

If specific regulatory requirements are implemented for these areas which are directly applicable in all EU Member States, it would support all parties, including manufacturers and authorities, and significantly limit potential connected compliance risks.

Introduction – CEVISS Project

Aim of the project

The aim of the CEVISS project is to identify a feasible solution to detect hazards on the road and support the drivers to either avoid the area or increase safety by providing information or intervene in driving, slow down the vehicles in the hazard area and increase distance between vehicles.

List of possible hazard types considered by the CEVISS Project:

- Wild animal in the road area
- Unprotected accident scene, ie. rescue service or the police are not present to secure the area
- Pedestrian on the road
- Hazardous object - unidentified or identified, obstructing street and driving
- Hazard lights turned on by other drivers

In order to provide the envisaged services to the drivers and other recipients, following background actions are performed:

- The next destination of the driver is predicted automatically based on historical driving data
- Actual location data of the vehicle, other data, images and video files are provided to Carmenta for distribution hazard warnings to other participants in the traffic and to support authorities, agencies, SOS Alarm, etc.
- A hazard zone is "created" by Carmenta, ie. a geofence area
- Carmenta calculates the vehicles proximity to the hazard zone
- Carmenta sends alert messages about the hazard zones to vehicles in the area

User value

Sharing of real time traffic situation data between OEMs through a central cloud will provide connected entities a more proactive and better traffic control.

Expectation of the driver (data subject) relating to personal data processing

“As a driver of a connected vehicle, when I am using connected services, I want to know that my personal data are protected.”

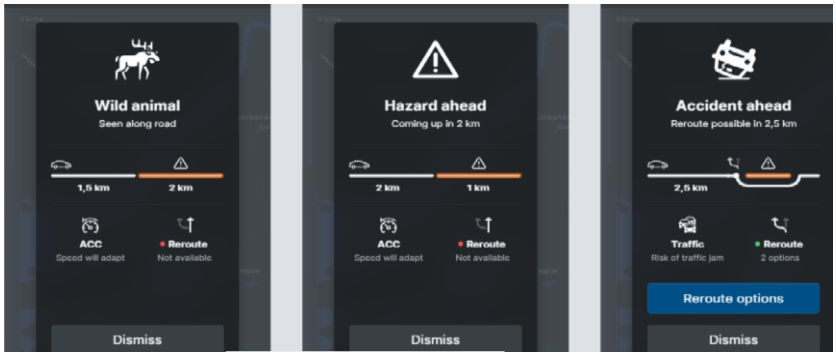
The following is a summary of a demonstration of the solution by the CEVISS project.

1. Sensor-detected Hazards
   - Large Animal
   - Pedestrian on highway
   - Accident Scene
   - Still-standing vehicle
2. Hazardous Location Warnings
   - Situation Analysis
   - Geofencing
   - Accident Scene Assessment
   - Standardized Messaging
3. Hazard Mitigation
   - Re-routing
   - Smart Speed Control

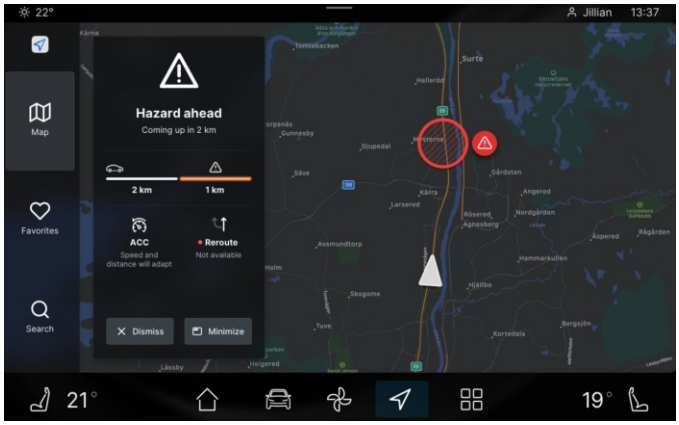
From the driver/user/data subject point of view

- My system displays my vehicle's location on navigation map
- My system displays a hazard location on the map and notifies me that it exists
- My system displays my most probable path/predicts my next destination (when I did not input where I am going)
- My system suggests an alternative route to avoid a hazard zone and shows me the alternative route, on the map
- My system continues to show my location, my new most probable path and the location of the hazard
- When I have moved away from the hazard, the hazard notification disappears from my navigation map
- If I did not reroute and I am still heading towards the hazard area, I see a warning that I am approaching the hazard area. In this case, it is assumed that the ACC is active and in use
- If I keep approaching the hazard area, my system informs me that an automatic cruise control function will activate, and my vehicle will slow down - tactile feedback on the steering wheel. If I want to stop the function, I need to de-activate the ACC
- As I am entering the geofenced hazard area, my vehicle slows down and increases distance from vehicle/objects in front of me
- I see on my navigation screen notifications that I am inside a hazard area and I should be careful
- I slowly cruise through the hazard zone
- As I exit the zone, my vehicle gradually increases speed, to revert back to the normal speed limit.

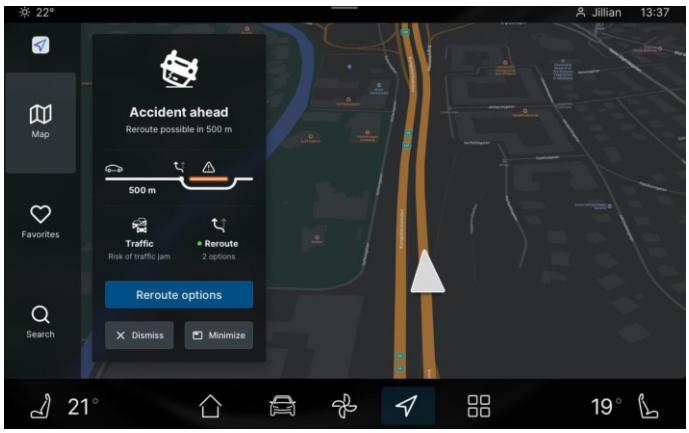
The warning is displayed in the vehicle (examples, final solution might differ)



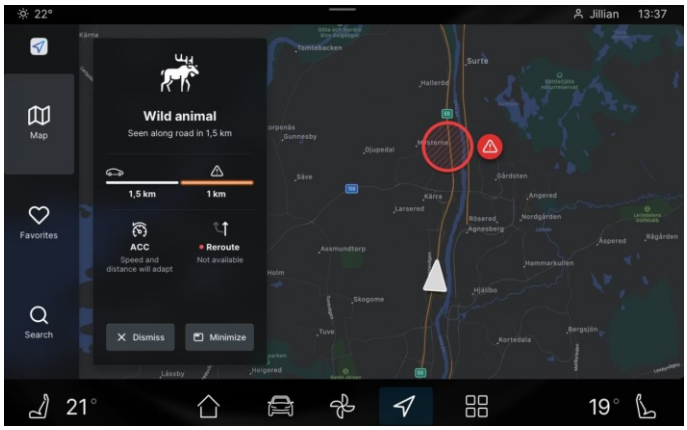
Example hazard warning



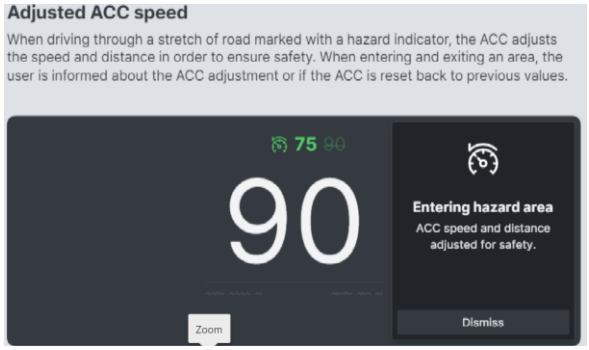
Example accident warning



Example wild animal warning



Information about slowing done the vehicle in the geofenced area



Scope of the Data Privacy Compliance Report

The Compliance Report **primarily focuses** on data privacy requirements according to ***REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*** – **"GDPR"**

As the GDPR is directly applicable in all EU Member States, the Compliance Report provides a general overview about requirements in all these markets relating to data privacy. However, local EU Member State privacy laws and local guidelines which might contain deviations from the GDPR, have not been considered in the Compliance Report.

The Compliance Report also considers the **opinions of the European Data Protection Board** ("EDPB"), which contributes to the consistent application of data protection rules throughout the EU.

The ePrivacy Directive (2002/58/EC, as revised by 2009/136/EC), sets a specific standard for all actors that wish to store or access information stored in the terminal equipment of a subscriber or user in the European Economic Area (EEA). If most of the "ePrivacy" directive provisions (art. 6, art. 9, etc.) only applies to providers of publicly available electronic communication services and providers of public communication networks, art. 5(3) ePrivacy directive is a general provision. It does not only apply to electronic communication services but also to every entity that places on or reads information from a terminal equipment without regard to the nature of the data being stored or accessed. The connected vehicle and every device connected to it shall be considered as a "terminal equipment" (just like a computer, a smartphone or a smart TV) and provisions of art. 5(3) ePrivacy directive must apply where relevant. Therefore, the ePrivacy Directive is in scope as well.

Although the Compliance Report is to summarize EU data privacy requirements based on the GDPR and to provide guidelines and recommendations for further considerations by OEMs and governing bodies, it also considers **ongoing EU regulatory developments** and other EU projects which have been identified as potentially relevant, as they include personal data processing in their scopes in a similar context.

Therefore, the **draft e-Privacy Regulation** is also considered, which would replace the ePrivacy Directive when it is finalized, published and it comes into force.

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 is a similar safety related solution – "**eCall Regulation**". From personal data processing perspective there are similarities and therefore it is considered by the Compliance Report.

The Cooperative Intelligent Transport Systems ("C-ITS") Platform is an initiative of the Directorate for Transport and Mobility of the European Union. The C-ITS Directive contains provisions relating to the Platform and the Article 29 Working Party issued an opinion about the personal data processing in that context. Therefore, it is considered by the Compliance Report.

Potential specific provisions relating to camera surveillance systems in Sweden have been reviewed on a high level and commented in the Compliance Report to create a proof of concept in one EU Member State. In that sense, the **Camera Surveillance Act (2018:1200) ("the CSA")** was reviewed from the perspective of potential restrictions. However, as the camera surveillance related regulations are not harmonized in the EU, further investigation is required to identify potential restrictions, licensing requirements, application, etc. Even the Swedish legislation was reviewed only on a high level, as this type of requirements were not in scope from the beginning of the project, but it was brought up during the project as a potential regulatory challenge.

Out of scope of the Compliance Report:

EU Member State privacy laws and national guidelines are out of scope of the Compliance Report. These laws and guidelines might contain additional requirements to the GDPR and therefore should be further investigated for specific markets. However, it is unlikely that EU Member State privacy laws and national guidelines would contain significant differences to GDPR requirements relating to the subject.

Furthermore, other local EU Member State laws, regulations, guidelines are out of scope of the Compliance Report. These laws, regulations, guidelines might have relevance in privacy considerations, but these laws are typically not data privacy related and therefore out of scope of the data privacy investigation.

Personal data

According to the GDPR, personal data is:

"Any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, and identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Many data associated with vehicles could be considered personal data to the extent that it is possible to link it to one or more identifiable individuals. This includes technical data concerning the vehicle's movements as well concerning the vehicle's condition.

In the CEVISS project, data are collected from within and outside of the vehicle. That means that individuals can potentially be directly or indirectly identified within the vehicle and outside of the vehicle as well, depending on the selected two use cases.

Special categories of personal data

"Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

Special attention to geolocation data

The EDPB's opinion is that geolocation data **may warrant special attention** given their sensitivity and/or potential impact on the rights and interests of data subjects. Therefore, collecting geolocation data should happen when absolutely necessary for the purpose of personal data processing.

Collecting geolocation data is also subject to compliance with the following principles:

− adequate configuration of the frequency of access to, and of the level of detail of, geolocation data collected relative to the purpose of processing,

− providing accurate information on the purpose of processing,

− when the processing is based on consent, obtaining valid (free, specific and informed) consent that is distinct from the general conditions of sale or use (for example on the onboard computer),

− 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,

− the option to deactivate geolocation at any time,

− defining a limited storage period.

Controllers/Processors

The Controller is primarily responsible for personal data processing. Identification of the Controller(s) in the processing activity and for each purpose of personal data processing is essential.

If Processors are involved, the Controller takes responsibility for selecting only such processors which can provide sufficient guarantees to implement appropriate technical and organizational measures that personal data processing will meet the GDPR requirements and which can ensure the protection of the rights of data subjects.

Controllers and Processors shall draw up a contract specifying legal obligations of each party. All parties are responsible for the data they process.

Data recipients

The recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. As an example, a commercial partner of the service provider that receives from the service provider personal data generated from the vehicle is a recipient of personal data. Whether they act as a new data controller or as a data processor, they shall comply with all the obligations imposed by the GDPR.

However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing. As an example, law enforcement authorities are authorized third parties when they request personal data as part of an investigation in accordance with European Union or Member State law.

Controllers

According to the GDPR, Controller is:

"A natural or legal person, public authority, agency or other body which, **alone or jointly with others, determines the purposes and means of the processing of personal data**."

Controllers are primarily responsible for the personal data processing, to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR

In the context of destination prediction, predictive re-routing, hazard avoidance, accident mitigation and accident support, Controllers can potentially include:

- OEMs,
- Cloud service providers,
- Developers,
- Service partners,
- Authorities,
- Agencies,
- Government bodies,
- SOS Alarm,
- Emergency responders,
- Rescue services,
- Private or public organizations that play a role in handling of incidents,
- Police,
- and other parties which determine the purposes and means of the processing of personal data.

Two or more controllers 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 providing information to the data subjects, depending on, if personal data have been obtained from the data subject or from another source.

Processors

According to the GDPR, Processor is:

*"A natural or legal person, public authority, agency or other body which processes personal data **on behalf of the controller**."*

The data processor collects and processes data on instruction from the data controller, without using those data for its own account.

The Processor shall process personal data only on documented instructions from the Controller(s), shall ensure that only authorized persons have access to personal data and shall fulfill other obligations according to the GDPR, like guarantee a security level which is adapted to the risk level of personal data processing, respond to data subject requests, etc..

In the context of destination prediction, predictive re-routing, hazard avoidance, accident mitigation and accident support, Processors can potentially include:

- Cloud service providers,
- Developers,
- Other service providers,
- Agencies,
- SOS Alarm,
- Emergency responders,
- Private or public organizations that play a role in handling of incidents,
- Rescue services,
- and other parties which process personal data on behalf of the Controllers.

Identification of Processors is essential to determine responsibilities properly, have relevant data processing agreements in place and to be able to inform data subjects in a correct way.

Law enforcement authorities, eg. police

Data collected by connected vehicles may be processed by law enforcement authorities to detect speeding or other infractions if and when specific conditions are fulfilled. In this case, such data will be considered as relating to criminal convictions and offences under the conditions laid down by GDPR (Art. 10) and any applicable national legislation.

Controllers may provide the law enforcement authorities with such data if the specific conditions for such processing are fulfilled.

The EDPB's opinion is that processing of personal data for the purpose of fulfilling requests made by law enforcement authorities does not constitute a specified, explicit and legitimate purpose within the meaning of Art. 5(1)(b) GDPR – purpose limitation.

When law enforcement authorities are authorized by law, they could be third parties receiving of personal data. In this case Controllers would be entitled to provide them with any data at their disposal subject to compliance with the relevant legal framework in each EU Member State – Art 6 (1)(c) GDPR.

Principles of data privacy

All principles relating to processing of personal data shall be considered according to GDPR. We would point out two from these principles.

Data minimization

One of the GDPR personal data processing principles is data minimization, which requires that personal data shall be:

Adequate – sufficient to properly fulfil the stated purpose,

Relevant – has a rational link to the stated purpose,

Limited to what is necessary in relation to the purpose for which it is processed.

To ensure adequate personal data processing, the purpose of processing shall be carefully identified.

Data protection by design and by default

The controller(s) shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

The CEVISS Project has been continuously informed from the beginning of the project about privacy by design and by default requirements and the principle was followed during designing of the solution.

How long can/shall the personal data be retained?

The retention periods of the processed personal data by all Controllers and Processors involved should be clearly identified and indicated to the data subjects.

In the context of data processing taking place for the performance of a contract, it is important to distinguish between two types of data before defining their respective retention periods:

− **Commercial and transactional data**: 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 for potential litigation purposes. Thereafter, at the end of the statutory limitation periods, the data shall be deleted or anonymized;

− **Usage data**: usage data can be classified as raw data and aggregated data. If it is necessary, raw data should be kept only as long as they are required to elaborate the aggregated data and to check the validity of that aggregation process. Aggregated data should be kept as long as it is necessary for the provision of the service or otherwise requested by a Union or Member state law.

A) DESTINATION PREDICTION

ACCIDENT ASSESSMENT, HAZARD IDENTIFICATION AND WARNINGS TO VEHICLES, MOBILITY SUPPORT – PREDICTIVE RE-ROUTING (NAVIGATION ADVICE), SLOWDOWN OF VEHICLES (ADAPTIVE CRUZE CONTROL FUNCTIONALITY), RESCUE MISSION SUPPORT WITH DATA (NO IMAGES OR VIDEO FILES)

From the data subject perspective:

"As a driver of a connected vehicle, when I am using connected services, I want to know that my personal data are protected."

"As a driver of a connected vehicle, if I receive hazard notifications from the CEVISS system, I want my navigation system to give me rerouting suggestions to avoid those hazards."

"As a driver of a connected vehicle, when I am approaching the location of hazard alerts from the CEVISS system, I want my set speed limit to automatically decrease, and the set distance from vehicle in front to increase, until I am out of the hazard area."

The aim is to provide information to the driver and alternative route to avoid the hazard, by either using the pre-set destination or predict the driver's driving destination.

For destination prediction, the history of the driver's trips have to be stored. That means that previous locations and timestamps have to be collected. The intention is not to apply a deep-learning approach.

Storage location: The destination prediction data are stored **in the car**. The destination prediction data will not be exported from the car and stored in the cloud. The destination prediction data will only be stored in the car.

If pre-routing is not possible or declined by the driver, intervention is necessary to slow down the vehicle in the hazardous area (geofenced area).

There are two alternatives for re-routing:

1) Driver uses the vehicle's navigation system

When the vehicle starts moving, it is checked, if the driver has entered a route in the navigation system.

If the driver has entered a route in the navigation system, this route is stored in the car, and then sent to the OEM for further distribution to Carmenta.

The message to Carmenta does not contain information from which the vehicle or the driver would be directly or indirectly identifiable.

Carmenta identifies any active hazards along the route.

If a hazard is identified along the route, Carmenta creates a geofenced area and sends a message of that geofenced area back to the OEM, containing the specification of the category of the hazard.

The OEM sends a message to the vehicle with the geofenced area and the category of the hazard.

An alternative route is calculated in the vehicle and type of hazard is displayed in the vehicle to inform the driver.

2) Driver does not use the vehicle's navigation system

If the driver has not entered a route into the navigation system, the OEM applies a model for predicting destination.

The model is trained on the history of routes.

The model predicts where the driver is going - Most Probable Path, MPP.

The model is trained, stored and runs in the car, with data that is also stored in the car. This data consists of historic trips that the car took, the date and time those trips occurred and the driver's ID/number belonging to car key to identify the driver. (This information is gathered from the car key).

The OEM vehicle's MPP is sent to Carmenta, who then identifies, if there is a hazard along that route.

If there is a hazard along the route, Carmenta creates a geofenced area and sends the message of geofenced area to the OEM, containing the specification about type of the hazard.

The OEM sends a message to the vehicle with the geofenced area and the category of the hazard.

A second alternative route is calculated in the vehicle and type of hazard is displayed in the vehicle to inform the driver.

If there is no hazard along the route, Carmenta sends a message to the OEM that the MPP can be used.

The OEM sends a message to the vehicle that the MPP can be used.

The MPP prediction model requires that the specific vehicle was driven at least once before through the predicted destination. The more times the vehicle has completed that route, the more accurate the prediction will be. This means that the model improves as it gets more information from the historic routes. Therefore, long-term storage of the driven routes is necessary.

Other possible solutions considered

1. Continuously send location data of CEVT vehicles to Carmenta, and Carmenta could do the calculation of MPP.

This option was not selected, as we would be exposing the location of our vehicles constantly, which is an unnecessary transfer of personal data.

2. Deploy the prediction model in the CEVT cloud and continuously send location data of CEVT vehicles.

This would create more security risks, than the chosen solution of storing the prediction model in the vehicle. **Therefore, this option was not selected.**

Purposes of personal data processing

Personal data is transferred from the vehicle to the OEM's cloud. Personal data is **anonymized** when further transferred from the OEM's cloud to Carmenta and used for another purpose (Purpose 2), i.e. personally identifiable information is removed from data sets, so the data subject whom the data describe remain anonymous.

Data subject is **notified about personal data processing** through responses from the service provider and data subject **directly benefits** from allowing personal data processing through the provided services.

Purpose 1
To provide a service to the data subject which
- Improves safety of the data subject and other individuals in the same vehicle,
- Optimizes road usage for the data subject,
- Reduces fuel and energy usage relating to the vehicle.

Purpose 2
To provide hazard warnings to other participants in the traffic and to authorities, agencies, SOS Alarm, etc., which drives to:
- Intervention with increased efficiency,
- Optimal usage of assets of rescue services,
- Improved road safety,
- More optimized traffic,
- Greater transport efficiency, optimal use of road, traffic and travel data,
- Fewer negative environmental impact,
- Support for economic development.

Note! The CEVISS Project considered seriously the purposes for which personal data should be processed and to avoid any interference with the data subject privacy according to the GDPR and the ePrivacy Directive. Therefore, **the purposes are very specific and transparent**.

Note! There is **no other purpose** of personal data processing at the Controllers or Processors and **no further personal data processing** by the Controllers or Processors.

Personal data set

Usage data

1) Following personal data are processed **within the vehicle** to be able to provide the services to the data subject (Purpose 1):
   - Location data
   - Historical location data

Note! Processing only these two types of personal data would not allow to provide the services. Further personal data processing is also necessary, which is from the vehicle to the OEM's cloud.

2) Following personal data are transferred **from the vehicle to the OEM's cloud**:
   - Message identifier
   - Identification of the vehicle
   - Time stamp
   - Location of the vehicle
   - Direction of the vehicle
   - Recent location of the vehicle

Commercial and transactional data

Commercial and transactional data are used to identify the data subject when collecting consent or signing a contract about providing the specific services for the data subject:

- Data subject's identifying information,
- Transaction related data,
- Data relating to means of payment,
- etc.

Automated decision making

The GDPR **specifically addresses profiling and automated individual decision-making, including profiling**. Profiling and automated decision-making can pose significant risks for individuals' rights and freedoms which require appropriate safeguards.

Furthermore, automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

Therefore, it is important to consider, if

1. Automated decision making or profiling would take place in the situations which are subject of the Compliance Report,
2. Special categories of personal data would be processed.

Would automated decision-making take place?

Solely automated decision-making is the ability to make decisions by technological means without human involvement. Automated decisions can be based on any type of data, for example data observed about the individuals, such as location data collected via an application.

In case of route prediction, location data will be collected of an individual, and predictions made based on previous routes.

Conclusion: **YES**, solely automated decision-making would take place in case of route prediction.

Would special categories of personal data be processed?

The GDPR definition explicitly states what are special categories of personal data (Art 9).

Geolocation data is not mentioned explicitly in the GDPR definition about special categories of personal data.

Conclusion: **NO**, special categories of personal data are not be processed in case of route prediction.

Note!

Although special categories of personal data are not processed by definition, the EDPB's opinion is that geolocation data **may warrant special attention** given their sensitivity and/or potential impact on the rights and interests of data subjects. That sensitivity of location data was considered by the CEVISS project from the beginning and the solution developed accordingly.

Exclusion of profiling

According to the GDPR definition, profiling is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular **to analyse or predict aspects** concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, **location or movements.**
Based on the GDPR, profiling is automated processing of personal data for evaluating personal aspects, in particular to analyse or make **predictions about individuals**. The use of the word 'evaluating' suggests that profiling involves some form of assessment or judgement about a person.

Broadly speaking, profiling means gathering information about an individual (or group of individuals) and evaluating their characteristics or behaviour patterns in order to place them into a certain category or group, in particular to analyse and/or make predictions about, for example, their:

- ability to perform a task;
- interests; or
- likely behavior.

The purpose of profiling is to classify individuals based on known characteristics.

In case of route prediction, classification of individuals would not take place, evaluation the individuals characteristics or behavior patterns in order to place them into a certain category or group would not happen.

Therefore, automated data processing in this case **would not lead to profiling**.

Data minimization – applied carefully

Personal data shall be **Adequate**, **Relevant,** and **Limited to what is necessary** in relation to the purpose for which it is processed.

Purposes of data processing have been carefully identified by the CEVISS project, therefore personal data shall be considered adequate. The personal data which are processed are absolutely relevant to the purposes and all the personal data are necessary to provide the services to the data subject, which means that no more personal data is processed than necessary.

The personal data processing for destination prediction purposes is a **hybrid type of personal data processing**, when data are processed within the vehicle (without disclosing them to controllers or processors) and outside of the vehicle, when personal data are transferred to the OEM's cloud.

This hybrid type of personal data processing is encouraged by the EDPB as it ensures that principles of data minimization are satisfied by design.

Legal basis

The legal basis of a hybrid type of personal data processing require careful consideration, also considering that location data are processed which are of sensitive nature and that solely automated decision taking is implemented for route prediction (see in later specific section).

Generally, the GDPR is applicable, but additionally to the GDPR, the ePrivacy Directive sets a specific standard in case data (any sort, including personal data) is stored in or accessed from the "terminal equipment" of an individual (subscriber or user).

Terminal equipment is an (a) "equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network; (b) satellite earth station equipment".

According to the definition of the terminal equipment, the connected vehicle and every device connected to it shall be considered as a "terminal equipment" (similarly to a computer, a smartphone or a smart TV) and provisions of the ePrivacy Directive must apply.

Consent

According to the EDPB's opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, art. 5(3) ePrivacy directive provides that, as a rule, prior consent is required for the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user. To the extent that the information stored in the end-user's device constitutes personal data, art. 5(3) ePrivacy Directive shall take precedence over art. 6 GDPR with regards to the activity of storing or gaining access to this information.

Any processing operations of personal data following the primary processing operations, including processing personal data obtained by accessing information in the terminal equipment, must additionally have a legal basis under art. 6 GDPR in order to be lawful.

The controller has to inform the data subject about all the purposes of the processing – including any processing following the aforementioned operations – when seeking consent for the storing or gaining of access to information pursuant to art. 5(3) ePrivacy Directive, the consent should also cover such processing operations. Consent will likely constitute the legal basis both for the storing and gaining of access to information already stored and the processing of personal data following the primary processing operations.

The notion of consent in the ePrivacy Directive remains the notion of consent in the GDPR and must meet all the requirements of the consent as provided by art. 4(11) and 7 GDPR.

(Art. 5(3) ePrivacy Directive provides two exemptions from the requirement of informed consent. These exemptions **are <u>not applicable</u>** relating to data and personal data processing in relation to the identified scenarios in the CEVISS project. The exemptions are mentioned here for the sake of completeness and to demonstrate that they were considered in the Compliance Report.

The exemption allows the storing of information or the gaining of access to information that is already stored in the terminal equipment to be exempted from the requirement of informed consent, if it satisfy one of the following criteria:

• Exemption 1: for the sole purpose of carrying out the transmission of a communication over an electronic communications network;

• Exemption 2: when it is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

In these two cases, the processing of personal data including personal data obtained by accessing information in the terminal equipment is based on one of the legal basis as provided by art. 6 GDPR.

None of the exemptions provided by those provisions can apply in this context: the processing is not for the sole purpose of carrying out the transmission of a communication over an electronic communications network nor does it relate to an information society service explicitly requested by the subscriber or user.)

Prior consent of the data subject should be collected according to art. 6 GDPR. Prior consent should be collected for each purpose separately.

Such prior consents must be provided on a specific form, through which the data subject agrees to use the service and have his or her personal data processed for that purposes (separate for Purpose 1 and Purpose 2).

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). Such consent must be provided separately, for specific purposes, may not be bundled with the contract to buy or lease a new car and the consent must be as easily withdrawn as it is given. Withdrawal of consent shall lead to the processing being stopped. The personal data shall then be deleted from where it is stored, or anonymised.

Contract

Initial consent would not allow further personal data processing (Purpose 2), as consent must be informed and specific to be valid.

Therefore, **next to collecting consent from the data subject**, **a contract shall be concluded**.

As regards the processing of personal data following the storage or access to the end-user's terminal equipment, the personal data processing according to Purpose 2 can rely on art. 6(1)(b) GDPR, provided it is possible to establish both that

- the processing takes place in the context of a valid contract with the data subject and
- the processing is necessary in order that the particular contract with the data subject can be performed.

Compliance with a legal obligation – Law enforcement authorities

The EDPB's opinion is that processing of personal data for the purpose of fulfilling requests made by law enforcement authorities **does not constitute a specified, explicit and legitimate purpose within the meaning of art. 5(1)(b) GDPR – purpose limitation**.

When law enforcement authorities are authorized by law, they could be third parties receiving of personal data.

In this case Controllers would be entitled to provide them with any data at their disposal subject to compliance with the relevant legal framework in each EU Member State – Art 6 (1)c.

Compliance with a legal obligation – General

In case the general EU legal framework or EU Member State law would make it obligatory to provide the services and process personal data for the Purpose 1 and Purpose 2, it could

- **replace the consent requirement** and
- **replace the requirement of signing a specific contract** with the data subject.

In that case personal data processing could take place according to GDPR art 6(1)c, to comply with relevant legal obligation.

However, the **consent requirement according to the ePrivacy Directive** or the later ePrivacy Regulation (after finalized, published and it is in force) **might still be valid**. That action would make personal data processing and providing the service more secure.

Until it is a legal obligation in all EU Member States, **collecting consents from data subjects and conclude a specific contract is required** to be able to provide the services.

If **single EU Member States** implement laws which make mandatory the related personal data processing, **collecting consents from data subjects and conclude a specific contract would not be required on these EU Member States.**

Special data subject rights relating to automated processing

The data subject shall have the right **not to be subject to a decision based solely on automated processing**, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

This right of the data subject shall not apply if the decision:

(a) is necessary for entering into, or **performance of, a contract between the data subject and a data controller**;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is **based on the data subject's explicit consent**.

To provide the services in the scenarios of the CEVISS Project, the data subject shall provide his/her explicit consent and sign a contract relating to the services. The data subject has to be aware that re-routing decisions will take place solely on automated processing of personal data.

Therefore, this special data subject right does not apply. It would similarly not apply, if the solely automated decision making would be authorized by Union or EU Member State law. Such a requirement would be optimal to be implemented on an EU level (not in each EU Member State), similarly to the e-call requirement. Considering similar ongoing EU projects, like the C-ITS, it is likely that the European regulatory framework will be improved in this way soon.

Information to data subjects

Where personal data relating to a data subject are collected from the data subject, the Controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the specific purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on legitimate interest, the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of safeguards and the means by which to obtain a copy of them or where they have been made available;

(g) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(h) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(i) where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(j) the right to lodge a complaint with a supervisory authority;

(k) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(l) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;

Further, the data subject shall be informed about:

1. That the in-vehicle system is activated by default, or not
2. How to deactivate the in-vehicle system
3. The data processing that the in-vehicle system performs
4. The types of data collected and processed
5. The fact that there is or there is no constant tracking of the vehicle
6. Any necessary additional information regarding traceability, tracking and processing of personal data relating to added value services.

Where the Controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the Controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information,

Users should be able to control how their data are collected and processed in the vehicle. Therefore, information regarding personal data processing must be provided in the data subject's language (in user manual, settings, etc.);

The information directed 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 and a description of the data subject's rights, as well as any additional information on the processing which has the most impact on the data subject and processing which could surprise them.

The EDPB recommends that, in the context of connected vehicles, the data subject to be made aware of all the recipients in the first layer of information.

As stated in the EDPB/WP29 guidelines on transparency, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers cannot provide

the names of the recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients.

The data subjects may be informed by concise and easily understandable clauses in the contract of sale of the vehicle, in the contract for the provision of services, and/or in any written medium, by using distinct documents (e.g., the vehicle's user manual or maintenance record book) or the onboard computer.

Camera surveillance related specific provisions in Sweden

There are no laws in Sweden strictly prohibiting fixed installation of cameras in a vehicle.

However, Sweden has a relatively new camera surveillance legislation with limited case law. This means it cannot be ruled out that the cameras used in the CEVISS scenarios could fall within the scope of the CSA (The Camera Surveillance Act (2018:1200) ("the CSA").

Fully integrated cameras in vehicles that are used for e.g. parking assistance purposes, which are turned on automatically when the car is started or when backing the car, will usually fall within the scope of the CSA.

In the event the use of built-in cameras should be considered camera surveillance and therefore be subject to the CSA, such use will most likely not require a permit, as the monitoring would be carried out for the safety of traffic in order to improve the visibility of the driver or user.

B) VIDEO/PHOTO FEED

RESCUE MISSION SUPPORT WITH IMAGES AND VIDEO FILES

From the data subject perspective:

"As a driver of a connected vehicle, when I am using connected services, I want to know that my personal data are protected."

"As a driver of a connected vehicle, I want to support the rescue mission with data and, images and video files about hazards on the way of my vehicle."

"As a data subject participating in the traffic and involved in an accident, I want efficient support and rescue from the rescue services."

"As a data subject participating in the traffic and not involved in an accident, but close to an accident, I want my personal data protected and not processed by any company, agency, insurer, law enforcement authorities (eg. police), except when data processing is required by EU regulation or EU Member State law."

The aim is to provide images and video files to SOS Alarm and the rescue services, additionally to other data and information.

Rescue services can optimize their rescue operations based on additional information on pictures or from video files. An example for such kind of additional information is the license plate of a vehicle which is involved in an accident and the type of the engine which the vehicle is equipped with. If the rescue operation can identify before arriving to the accident scene based on the license plate what is the type of the engine the vehicle is equipped with (eg. electric engine), the preparation for the rescue mission can be more effective.

The challenge from personal data processing purposes is, that images and video files are recorded by the vehicle automatically and continuously and from outside of the vehicle.

In these cases, personal data of the driver in the vehicle and personal data of other data subjects outside of the vehicle are processed.

Another challenge is that the personal data processing takes place at all parties who got access to the images and video files, ie. the number of Controllers and Processors can be more than just 1-2 and that makes coordination and control of personal data processing more difficult – but not impossible. It requires strong control by the Controllers.

Purpose of personal data processing

The purpose of personal data processing is to

- Support the Rescue Services/SOS Alarm in their operation with images and video files about accidents to increase efficiency of rescue activities and,
- Support other participants in the traffic to avoid hazards and accidents with information about accidents and hazards.

Personal data set

Following personal data are transferred **from the vehicle to the OEM's cloud:**

- Message identifier
- Identification of the vehicle
- Time stamp
- Location of the vehicle
- Direction of the vehicle
- Images from outside of the vehicle or/and
- Video file from outside of the vehicle

Following personal data and data which have sensitive nature from data privacy point of view are transferred **from the OEM's cloud** and **to the Carmenta cloud** and further **to the Rescue Services/SOS Alarm**.

- Time stamp
- Location of the vehicle
- Direction of the vehicle
- Images from outside of the vehicle or/and
- Video file from outside of the vehicle

Data subjects could be identified directly or indirectly based on Images and video files from outside of the vehicle.

Data minimization – applied carefully

Personal data shall be **Adequate**, **Relevant,** and **Limited to what is necessary** in relation to the purpose for which it is processed.

Purposes of data processing have been carefully identified by the CEVISS project, therefore personal data shall be considered adequate. The personal data which are processed are absolutely relevant to the purposes and all the personal data are necessary to provide the services to the data subject, which means that no more personal data is processed than necessary.

Legal basis 1 – driver/user

The legal basis of a hybrid type of personal data processing require careful consideration, also considering that location data are processed which are of sensitive nature.

Generally, the GDPR is applicable, but additionally to the GDPR, the ePrivacy Directive sets a specific standard in case data (any sort, including personal data) is stored in or accessed from the "terminal equipment" of an individual.

According to the definition of the terminal equipment, the connected vehicle and every device connected to it shall be considered as a "terminal equipment" (similarly to a computer, a smartphone or a smart TV) and provisions of the ePrivacy Directive must apply.

Consent

According to the EDPB's opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, art. 5(3) ePrivacy directive provides that, as a rule, prior consent is required for the storing of information, or the gaining of access to information already stored, in the terminal equipment of a

subscriber or user. To the extent that the information stored in the end-user's device constitutes personal data, art. 5(3) ePrivacy Directive shall take precedence over art. 6 GDPR with regards to the activity of storing or gaining access to this information.

Any processing operations of personal data following the primary processing operations, including processing personal data obtained by accessing information in the terminal equipment, must additionally have a legal basis under art. 6 GDPR in order to be lawful.

The controller has to inform the data subject about all the purposes of the processing – including any processing following the aforementioned operations – when seeking consent for the storing or gaining of access to information pursuant to art. 5(3) ePrivacy Directive, the consent should also cover such processing operations. Consent will likely constitute the legal basis both for the storing and gaining of access to information already stored and the processing of personal data following the primary processing operations.

The notion of consent in the ePrivacy Directive remains the notion of consent in the GDPR and must meet all the requirements of the consent as provided by art. 4(11) and 7 GDPR.

Prior consent of the data subject should be collected according to art. 6 GDPR.

Such prior consents must be provided on a specific form, through which the data subject agrees to use the service and have his or her personal data processed for that purposes.

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). Such consent must be provided separately, for specific purposes, may not be bundled with the contract to buy or lease a new car and the consent must be as easily withdrawn as it is given. Withdrawal of consent shall lead to the processing being stopped. The personal data shall then be deleted from where it is stored, or anonymised.

Compliance with a legal obligation – General

In case the general EU legal framework or EU Member State law would make it obligatory to provide the services and process personal data, it could **replace the consent requirement.**

In that case personal data processing could take place according to GDPR art 6(1)c, to comply with relevant legal obligation.

However, the **consent requirement according to the ePrivacy Directive** or the later ePrivacy Regulation (after finalized, published and it is in force) **might still be valid**. That action would make personal data processing and providing the service more secure.

Until it is a legal obligation in all EU Member States, **collecting consents from data subjects is required** to be able to provide the services.

If **single EU Member States** implement laws which make mandatory the related personal data processing, **collecting consents from data subjects would not be required in these EU Member States.**

Legal basis 2 – data subjects on images or in video files

Processing of personal data of data subjects outside of the car can be based on

- the legitimate interest of the controller or a third party (Art 6 (1) (f) GDPR) or
- the necessity of protecting the vital interest of the data subject or of another natural person (Art 6 (1) (d) GDPR) – in case of accidents.

Data revealing criminal offenses or other infractions

Processing of **personal data relating to criminal convictions and offences or related security measures** shall be carried out

- **only under the control of official authority or**
- **when the processing is authorized by Union or Member State law** providing appropriate safeguards for the rights and freedoms of data subjects.

For example, speeding, red lights or other infractions data would be considered as relate to criminal convictions according to GDPR.

The EDPB emphasizes that external processing of data revealing criminal offences or other infractions is forbidden. Thus, according to the sensitivity of the data, strong security measures must be put in place in order to offer protection against the illegitimate access, modification and deletion of those data.

For demonstration purposes, that following is not considered for example offence related data according to the EDPB: instantaneous speed collected in the context of a study is not offence related data by destination (ie, it is not being collected for the purpose of investigating or prosecuting an offence), which justifies the collection by legal persons who are not public authorities in the strict sense. However, that opinion relates to studies and there can be other incidents which could be considered as offence related data, eg. signal violations, like driving through a red light.

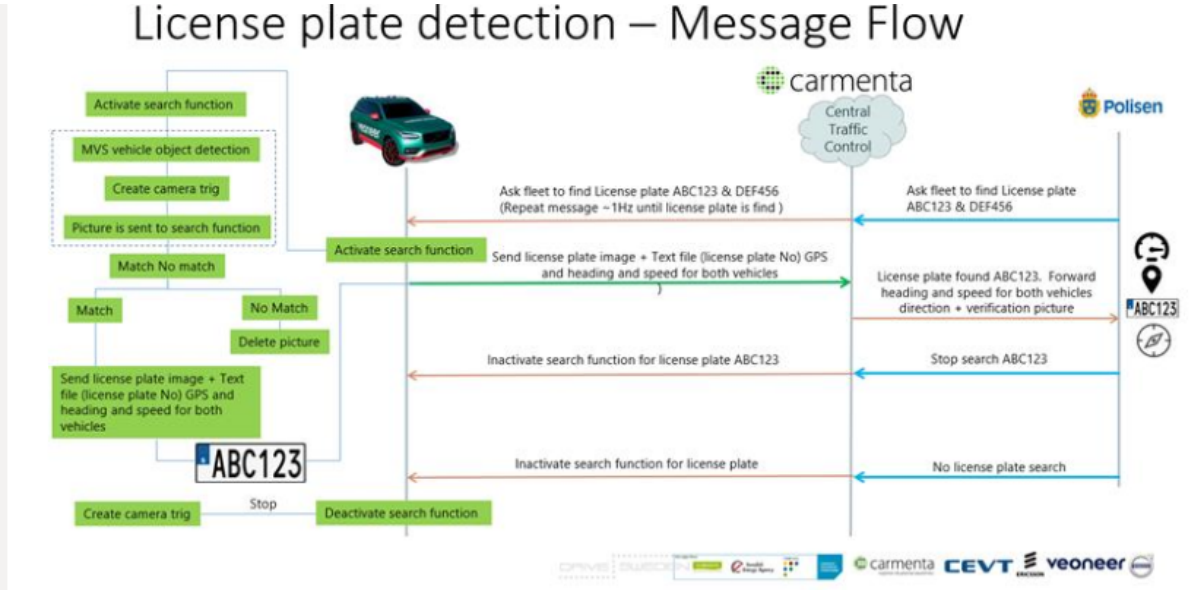
Note! Relating to the C-ITS, the EDPB's opinion is that using data for non-specified other purposes than road safety, accident prevention could constitute a criminal offence.

Camera surveillance related specific provisions in Sweden

Fully integrated cameras in vehicles that are used for e.g. parking assistance purposes, which are turned on automatically when the car is started or when backing the car, will usually fall within the scope of the CSA.

In the event the use of built-in cameras should be considered camera surveillance and therefore be subject to the CSA, such use could require a permit, if the purpose of the camera usage is not connected to improve the visibility of the driver or user.

C) LICENSE PLATE DETECTION



Purpose of personal data processing

Personal data is processed to identify individual license plates on the road and support Police in their searching activities and capture the car with the specific license plate on it.

Personal data sets

There is a personal data processing of

1. The user/driver of the vehicle which have identified the specific license plate through its sensors and cameras and ("DRIVER 1"),

2. The user/driver/owner of the car which has the specific license plate on it. The potential data subject or data subjects are identified based on the specific license plate; therefore, it can be other data subjects as well, who's data is subject to the data processing activity. ("DRIVER 2)

Legal basis

The legal basis according to the GDPR could be of personal data processing for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Art. 6 (1) e.)

Current situation in Sweden

Camera surveillance is becoming more common in several places. Cameras help in creating safer environment and in criminal investigations.

Police is already receiving information through cameras placed out at specific areas where vehicles and license plates can be identified. In these cases, Police uses fixed cameras which are operated directly by the Police.

However, Police can also collaborate with housing companies and civil society and in these cases the cameras are not operated directly by the Police.

Police can also use drones which are equipped by cameras. However, even if the drones are operated directly by the Police, identification of individuals while operating drones is allowed in very specific cases.

Further special rules apply, if data are used in relation to security related regulations, eg. in connection with espionage, sabotage, terrorist crimes and other special crimes.

Data revealing criminal offenses or other infractions

Processing of **personal data relating to criminal convictions and offences or related security measures** shall be carried out

- **only under the control of official authority or**
- **when the processing is authorized by Union or Member State law** providing appropriate safeguards for the rights and freedoms of data subjects.

For example, speeding, red lights or other infractions data would be considered as relate to criminal convictions according to GDPR.

The EDPB's opinion is that processing of personal data for the purpose of fulfilling requests made by law enforcement authorities **does not constitute a specified, explicit and legitimate purpose within the meaning of art. 5(1)(b) GDPR – purpose limitation**.

When law enforcement authorities are authorized by law, they could be third parties receiving of personal data.

In this case Controllers would be entitled to provide them with any data at their disposal subject to compliance with the relevant legal framework in each EU Member State – Art 6 (1)c.

Obtaining the EDPB's opinion on this specific solution could significantly reduce related data privacy compliance risks.

Camera surveillance related specific provisions in Sweden

Fully integrated cameras in vehicles that are used for e.g. parking assistance purposes, which are turned on automatically when the car is started or when backing the car, will usually fall within the scope of the CSA.

In the event the use of built-in cameras should be considered camera surveillance and therefore be subject to the CSA, such use could require a permit, if the purpose of the camera usage is not connected to improve the visibility of the driver or user.

It requires further investigations who can be the holder of such CSA permit in case of vehicles and how the collaboration with the Police could be authorized.

Other considerations relating to A), B) and C)

Security

Controllers/Processors/Receivers shall put in place measures that guarantee the security and confidentiality of processed data and take all useful precautions to prevent control being taken by an unauthorized person.

The security measures put in place shall be adapted to the level of data sensitivity.

The following measures can be considered:

− 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;

− when stored remotely, encrypting data by means of state-of-the-art algorithms;

− regularly renewing encryption keys;

− protecting encryptions keys from any disclosure;

− authenticating data-receiving devices;

− ensuring data integrity (e.g., by hashing);

− making access to personal data subject to reliable user authentication techniques (password, electronic certificate, etc.);

− deleting geolocation data as soon as the reference event or sequence is qualified.

Concerning more specifically vehicle manufacturers, the EDPB recommends the implementation of the following security measures:

− partitioning the vehicle's vital functions from those always relying on telecommunication capacities (e.g., "infotainment");

− implementing technical measures that enable vehicle manufacturers to rapidly patch security vulnerabilities during the entire lifespan of the vehicle;

− for the vehicle's vital functions, give priority as much as possible to using secure frequencies that are specifically dedicated to transportation;

− setting up an alarm system in case of attack on the vehicle's systems, with the possibility of operating in downgraded mode;

− storing a log history of any access to the vehicle's information system, e.g. going back six months as a maximum period, in order to enable the origin of any potential attack to be understood and periodically carry out a review of the logged information to detect possible anomalies.

Risks

Following potential risks or risk areas have been identified:

- Excessive data collection compared to what is necessary to achieve the purposes
- Unauthorized usage
- Loose of data

- Attack with negative motivation
- Reidentification of the data subject (data minimization could support to solve)
- Risk of tracking
- Third parties
- Data transfer to third countries
- No solution to withdraw consent at any time
- Driver/data subject is not fully aware of the scope of processing and how data are processed (lack of transparency)
- Information asymmetri between senders and receivers, Unrestricted number of receivers → Sender does not know the receivers (potential solution: rebalanced asymmetri with a higher level of control on personal data
- Fake alarms

Data subject rights

Controllers should facilitate data subjects' control over their data during the entire personal data processing period, through the implementation of specific tools providing an effective way to exercise their rights, in particular their right of access, rectification, erasure, their right to restrict the processing and, depending on the legal basis of the processing, their right to data portability and their right to object.

Recommendations

General recommendations

- Solutions and services should be optional for the data subjects.
- Users should be able to control how their data are collected and processed in the vehicle.
- The EDPB recommends, that only data strictly necessary for the vehicle functioning are processed by default. Data subjects should have the possibility to activate or deactivate the data processing for each other purpose and controller/processor and have the possibility to delete the data concerned.;
- Data should be transmitted to limited number of third parties;
- Data should be retained only for as long as is necessary for the provision of the service or otherwise required by Union or EU member state law;
- Data subjects should be able to delete permanently any personal data before the vehicles are put up for sale;
- Data subjects should, where feasible, have a direct access to the data generated by these applications.

- While it may not always be possible to resort to local data processing for every use-case, "hybrid processing" can often be put in place – in-car and outside of the car;

- Provide the data subjects a privacy policy, which demonstrates that data protection principles are followed and personal data are processed in a secure way;

- Standardized icons could be used in addition to the information necessary (art 13 and 14 GDPR) in order to reduce the need for vast amounts of written information to be presented to the data subject. If possible, standardized icons, that the data subjects understand the icon, irrespectively of brands or models of vehicles. Eg. when geolocation data is collected;

- Anonymization of personal data when a function or service can be achieved with anonymized data. If combined (anonymized and non-anonymized), it should be treated as personal data;

- No centralized database of the exchanged messages which contain personal data by any of the Controllers/Processors.

Anonymization

Data which leave the vehicle should be anonymized before transmitting them, if possible. Principles of personal data processing do not apply to anonymized data. Anonymization may be a good strategy to mitigate the risks relating to personal data processing.

Pseudonymization

"The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

Pseudonymization can help to mitigate risks, it improves the protection of personal data. Pseudonymization means replacing directly identifying personal data by a non-signifying pseudonym, for example by using a secret key algorithm. However, pseudonymization is reversible and data which are processed this way are considered personal data according to the GDPR.

Data Protection Impact Assessment

If data processing is likely to result in a high risk to the rights and freedoms of individuals, like processing personal data outside of the vehicle, Controllers are required to perform a data protection impact assessment ("DPIA") to identify and mitigate risks.

Even in the cases where a DPIA would not be formally required by the GDPR relating to personal data processing via connected vehicles, the EDPB recommends conducting a DPIA as best practice as early as possible in the design phase.

Conducting DPIAs by Controllers as next actions for all three areas mentioned in this Data Privacy Compliance Report (A), B) and C)) could demonstrate that personal data processing would not result in high risk according to Art 35 of the GDPR. However, the outcome of DPIAs cannot be predicted based on the available information.

Controllers and Processors can demonstrate by conducting DPIAs that they have sufficiently identified and mitigated data privacy related risks.

In case a DPIA would indicate that the personal data processing would result in a high risk, the supervisory authority shall be consulted prior to personal data processing and prior authorization might be necessary.

References

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

"ePrivacy" Directive (2002/58/EC, as revised by 2009/136/EC),

Regarding the notion of "terminal equipment", the definition is given by directive 2008/63/CE. Art. 1

EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications

EDPBs opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR

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

Camera Surveillance Act (2018:1200)

Aricle 29 Data Protection Working Party: Opinion 03/2017 on processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)

Date: **05 November 2020**

Version: **V1.0 05112020 GaborMolnar**