OCTO

Smart Analytics for a Better Connected World

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

Octo Comments and Concerns

April 2020

octotelematics.com

OCTO Comments and Concerns: Local Processing of Personal Data

According to Guidelines processing and storing of personal data **inside the vehicle are mandatory**; the only exception is given by operational needs that, in any case, must be duly documented.

This approach is against IOT and the Commission Data Strategy also in terms of competition.

According to this approach, only OEM would process and store the data.

The boxes currently installed in the vehicle do not have the storage capacity and so they should be replaced with more expensive ones with a consequent increase of the costs for the consumers (see slide on Case Study).

OCTO Comments and Concerns: Definition of Personal Data

Not all the data collected in the vehicle can be considered personal.

Technical data concerning the vehicle movements as well as concerning the vehicle conditions, if not linked to an identified or indentifiable natural person, cannot be considered as personal data.

In addition, the Guidelines do not consider that some data are collected in order to provide a service, such insurance pay as you drive, thefts, e-calls like services.

In these cases the data collection is necessary to provide the service and cannot be denied when the person is in the car and after the execution of the relevant agreement.

The same applies for rental services where the owner must always be aware of the localisation of the car and the status.

As consequence, also data retention or data subjects rights exercise (such as request to delete all data collected) must take into consideration contractual obligations undertaken by the data controller and/or the data processor. For instance, upon data subject's request, the deletion of all data collected related to a telematics services should be limited to data eventually stored in the vehicle only.

Octo Comments and Concernes
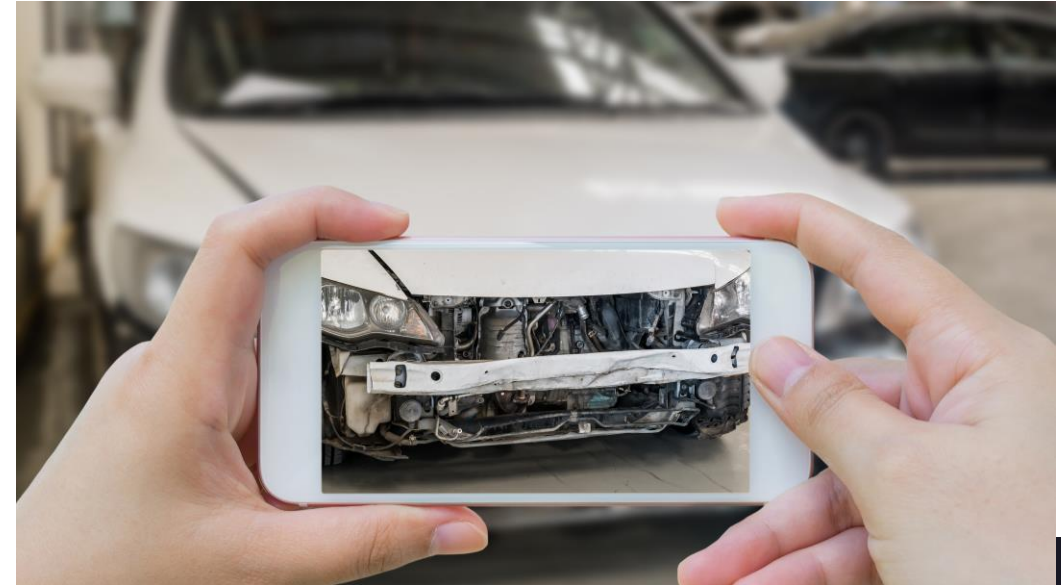
Par. 1.5.2 : Lack of control and asymmetry

Vehicle drivers and passengers may not always be adequately informed about the processing of data taking place in or through a connected vehicle

Vehicle drivers are fully informed when the contract is being signed. Passengers are only "guests" and they are "unknown". It's senseless to ask for the passenger's consent.

Other legal bases under GDPR must be considered as an alternative to consent and, in addition, the consent is not required at all from passenger since he/she cannot be identified and a different approach would bring a paradox implying data processing not necessary.

In accordance with European data strategy individuals should be effectively supported in enforcing their rights with regard to the use of the data they generate. Beyond data processing strictly necessary for contract execution and services provisions that cannot be changed upon data subject' request because this would imply impossibility to provide the data subject with the service that he/she has requested and paid, all data subjects must be in control of their data. This means that data subjects' level of awareness on data generated or that can be generated should increase and data subjects should be the primary decision makers on new opportunities arising from additional data processing directly proposed to them by providers.

Par. 1.5.4 : Excessive data collections

The approach of the EDPB is confusing about collection of data (see par. 54 and 55). Octo agrees only with par. 55 which must stay.

Par. 2.1.1: Geolocation data

The geolocation is not very risky depending on the scope of the service rendered. It is not correct that gyroscope may substitute geolocalitation. They are complementary. For instance, in case of crash or assistance, it is necessary to have both. The data collection cannot be stopped by the driver when it is the legal basis of the contract, such as pay as you drive insurance or rental services.

OCTO

EDPB recommends:	
the vehicle's usage data should be processed directly in telematics boxes	Not applicable for the the following reasons: Computation power is generally available in a Data Center and is not possible to implement the same capability in local. Predictive scoring algorithms or other more sophisticated algorithm for crash reconstruction cannot be calculated in the telematics box (due to the limited resources in the box). The cost of the box must be kept as lowest as possible to guarantee the sustainability of the service provided: the cost of the technology must guarantee the access for all the market. Sector has to work for safety and flex price with not-discriminatory access.

EDPB recommends:

if a telematics service provider (TSP) collects the data on behalf of the controller (the insurance company) there is no need to know the identity of the driver (such as names, licence plates, etc.) of the policy holders.

in addition the TSP must provide only scores and not raw data.

moreover, if only mileage is necessary for the performance of the insurance, location shall not be collected (109)

Information and rights of data subjects 3.1.1.4

Personal data can be split only in case the TSP is only involved in the score calculation.

This is not valid when Usage Based Insurance includes the following services:

- assistance in case of crash and first notice of loss which requires to know customer references (personal contact, licence plate, make and model of vehicle) as necessary to provide the service

- customer care for managing the policy lifecycle linked to telematics option (for example the installation of the box, the RMA in case of fault, the substitution in case of change of vehicle),

- assistance in case of breakdown, crash detection and assistance private e-call service. For private e-call services TSP is required to manage the first aid assistance on behalf of the Insurance

- website/App provided by TSP to the insurer. This requires for the fulfilment all the customer data.

- location is necessary to calculate the mileage and must be kept and stored in case of customer complaints against the Insurance Company or the Rental.

TSP must have full access data and right of data retention as third independent party vs Insurance and insurer.

This autonomous independency is recognized as legal proof in case of judgement. (ex. Italy Insurance Codex, art. 145 bis).

EDPB states that:

usage data can be classified as raw data and aggregated data. As stated above, if possible, data controllers or processors should not process raw 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. (3.1.1.3)

Information and rights of data subjects (111 – 112)

Keeping raw data is necessary to provide evidence of services correctly performed. Customers often ask on which basis the scoring has been calculated.

Raw data are intended to be the Data directly provided by the source without any prior calculation.

For same application it may be possible to consider raw data storage to re-process the aggregated data and check the validity for the contract purpose.

After that period, they can be anonymized or deleted.

Data Collected (3.2,2)

The European E-call define the minimun set of data as the one necessary as minimum to identify the "event of need".

Indeed, the crash detection which really is based on algorithms calculating the ROC Curve to minimize the false positive and negative and reduce the society costs and save human lifes, require more than the miminum data.

The data subject is informed about the services at the contract signature.

Security measures already in place:

access to the systems by TSP personnel takes place through nominal accounts and with authorization profiles based on the principle of "least privilege"; each data access is tracked and securely recorded in the Log Management System.

The certification in place guaranting higth security level are ISO27001, ISO27017, ISO27018 and ISO9001.

OCTO Smart Mobility Solution - Main Components To Empower the Connected Vehicles Business

OCTO

Octo solution simplify the process of leveraging OEM data from the connected-car opening the way to new business models and diagnostics solutions.

SMART MOBILITY

1	2	3	4	5	6	7	8	9
Keyless Renting and Sharing	**Anti-theft (SVR)**	**Damage Detection and reconstruction**	**Fuel and mileage Consumption**	**Diagnostic and Maintenance**	**Driving monitoring**	**Tracking and Geofence**	**Predictive Maintenance /Residual Value**	**Peace of mind and Loyalty**