# Motor Insurance Technical POC and Implementation Architecture Guidance

**Draft Working Document & Request for Comment**

**Version 1.0**

December 2021

**Authors**

Neil Walker, BA Hons.
Martin Dennehy, BSc.
Gunnar Andersson, M.Sc.
Fouad Husseini, FCII, BEng.



*This paper is subject to, and should be interpreted in light of, important disclaimers which appear at the end of this paper. Please carefully review those disclaimers, use the information at your own risk, and do not rely on this paper for making any decisions.*

# CONTENTS

# 1. INTRODUCTION

## 1.1. Introduction To Proof Of Concept Approaches

The Open Insurance Initiative (OPIN) has partnered and collaborated with COVESA (formally the GENIVI Automotive Alliance) on the alignment of the Open Insurance API and data standards with the Vehicle Signal Specification (VSS), to further enhance and augment the adoption of a standard which encourages shared business and system models in the insurance and mobility markets.

The first version of the alignment will be published in the OPIN website and the group will be inviting both OEMs and insurance organisations to explore and conduct proof of concept and elaboration of the API and data standard.

To undertake this work the standard will be published with supporting papers to ensure POC tasks can sufficiently adopt the standards effectively.

There are a number of use case scenarios that have been elaborated and agreed upon which are also published to allow organisations to explore which use cases to adopt and prove the standard and model.

The purpose for the alignment and the published standard is:

- Innovate and encourage experimentation
- Release readable standards that are technology agnostic and easily adoptable
- Factor in innovative services and technological advances to improve data exchanges

The specification and standards will support you in understanding naming conventions, data elements, service functions and vehicle signal data and functions.

## 1.2. How To Access And Deploy Sample Source Code

The latest version of the API contract and data schema is published in GitHub and is licensed under the MPL 2.0 license.

This version is under continuous review by both OPIN and COVESA and future updates will be published by the group with release notes to support changes.

Change requests and feedback are always welcome and a change log for future updates will also be published in Github.

# 2. OVERVIEW OF THE SPECIFICATION

The following section provides the overview and definition of the Data Entities and API interfaces available from both the OPIN standard and the VSS standard, the alignment and the adoption of the specification technically.

OPIN has taken a Domain Driven Design (DDD) approach to elaborating the Insurance domains, some of which are in place for future development, e.g. Pet Insurance. This paper will reference such domains but will focus specifically on the Motor domain and the Vehicle subdomain which will now embed details of signals relevant from the COVESA VSS standard.

## 2.1. Open Insurance Domain model

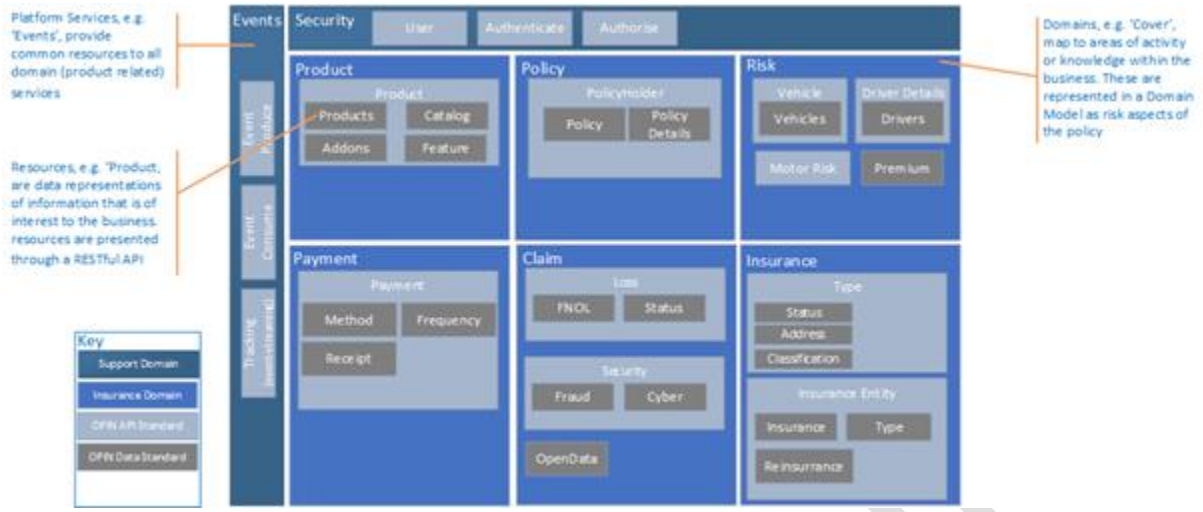
A Domain model is a conceptual model that describes the data (Data Standard) and behaviour (API standard), of the domain (insurance) in one model. The Domain model provides the context to the standard and the areas of relationship across both the Data Standard and API Standard.

The Domain model helps by providing additional context on the full standard but also clarifies areas of dependency, referential integrity and in areas applicable, a business process if required to adopt in a logical sequential preferred manner where necessary. A domain model reflecting the Data Schema domain boundary is illustrated below and shows the API standard and the Data standard reflected together in one model.

The Domain will iterate and evolve as a domain extends or becomes adopted, other domains may be considered in addition, or also be applicable and reusable in new or consolidated scenarios.

The domain model has 6 insurance domains and 2 supporting domains. The Insurance domain is bounded by its context of an API standard and a Data standard, these are:

- Product domain
- Policy domain
- Cover domain
- Payment domain
- Claim domain
- Insurance domain




The Security support domain is included to support the security context recommended to adopt the standard, and the Event support domain indicates standards can be consumed as both a consumer and/or publisher of a Data Standard, as events occurring through the lifecycle of insurance.

### 2.1.1. OPIN and VSS Data Models

The data model behind VSS can be generally applied to similar data items that are organised in a hierarchy. Reusing the same methodology for a different data set enables reuse of ideas and software technologies that are compatible with VSS.

This describes how to apply the same method to the OPIN data set.

The full VSS documentation could give some additional understanding, but here are the most relevant details.

Data is described in VSS using files in YAML format, with a predefined set of constraints:

- Available (allowed) data types - (not recommended to extend/change)
- Available (allowed) units - (extensible by adopters)
- Required metadata (fields) for every definition
- Optional metadata (fields) for every definition
- Layers for extending the model (see below)

When interpreting the VSS specification, YAML will allow you to discern the types and digest the formats. Whilst YAML is a language used to describe the specification, it is an open, agnostic approach to describe data and serialisation, and being a superset of the JSON format, interpretation and translation between YAML and JSON is permissible.

The following examples provide you with a view of the domain name reference and types expressed in VSS.

Examples:

```
OPIN.motor.claim.lossDate:
   datatype: string
   description: Date of event pertaining to the loss claim, stored in ISO8601
format

OPIN.motor.vehicle.cabinTemperature:
   datatype: float
   min: -50.0
   max: 120.0
   unit: celsius
   description: Current temperature inside the vehicle
```

(min and max values are only an example)

The primary difference between VSS model and the OPIN model described here is that the node type (metadata name "type:") is used in VSS but not in OPIN. In VSS, the node type can be one of the following:

- Branch - a container for multiple sub-nodes in hierarchy
- Sensor - generally indicating a value that is produced in vehicle and readable from an external system
- Actuator - indicating a value that is writable from an external system, to trigger an action in the vehicle
- Attribute - indicating a readable value that is constant (at minimum unchanged) for the duration of one driving cycle

## 2.2. Data Entities in Scope

The data entities approved and aligned with OPIN and COVESA are provided in a separate document named the Data Catalogue, which indicates the OPIN entity and VSS entity using a notation that describes the domain and subdomain relationships. The model will show how the Vehicle domain in the OPIN domain maps to the attributes provided in the VSS model whose structure is also explained in this proof of concept (PoC) guidance paper.

The specification contains attributes which are also clarified according to a particular frequency type i.e. static or dynamic.

### 2.2.1. Static Data Type

Static data is an attribute in the data schema that is not volatile and does not change, this could be referred to as the Vehicle make or model for example. Information that is static may often be used as keyed data that can be used as part of referential integrity. The static data can certainly operate in this manner and the standard does not dictate that this data must be held in systems for referential integrity purposes, it may well be used in this way. Future changes to the data specification may accommodate such changes.

The main purpose for static data is to ensure that the information volatility and change is likely to be low if not zero, and as such can be likely stored in Insurance, OEM and third party systems.

### 2.2.2. Streaming Vehicle Data Scope

This section describes the nature of real-time data interchanges, from Insurance, Vehicle and third party systems. The ability to support real-time events, is a key pattern in the implementation of the data standard, and directly relates to a number of the scenarios developed.

It is expected that data is provisioned in real-time and broadcasted to those systems consuming the data and are able to act and operate in real-time on the scenarios that are real-time critical.

Because of this, the nature of dynamic data means a number of systems will require more frequent access to data signals and/or insurance events, and it is expected that when implementing the OPIN and VSS standard you must be able to support the reliable and secure interchange of data according to dynamic frequency. This can be achieved by streaming information across all system owner's depicted in the Proposed Architecture section.

### 2.2.3. Dynamic Data

This section describes the nature of dynamic data and the need to have persistence logic within the boundaries of an Insurance, OEM or 3rd party system. Dynamic data is data whose state is constantly changing, acceleration has a dynamic context, as does tire-tread or tire-pressure, however, both undergo change in its state related to the condition of the vehicle, condition of the insurance policy holder, conditions of the insurance system, conditions of the driver or occupants of the vehicle. All these dynamic contexts have varying degrees of state change and will require a data cache storage to support the frequency of the data, as well as being shareable in a streaming context.

### 2.2.4. Vehicle Signals and Data standards

COVESA (formerly GENIVI) alliance provides and governs the VSS model for how to describe vehicle data, and also a standard catalogue of vehicle signals (= named and well-defined data items that can be communicated from the vehicle). The VSS provides both a standard way to describe (any) vehicle data and a defined list of signals and attributes which supports the capability of the connected car. Numerous signals exist and are well defined. The industry is gradually adopting these standard catalogue(s) in order to make data available in a common format.

Vehicle data (a.k.a. Vehicle Signals) stems from *sensors* and calculated information within the vehicle and will often flow from vehicle to an OEM-controlled cloud initially (more details

in chapter 3). VSS signals designated as *attributes* are generally considered constants (at minimum guaranteed to not change during a driving cycle). Signals defined as sensors are primarily for reading data from the vehicle. Some signals are even defined as *actuators*, so there is in theory a possibility of providing interfaces that affect vehicle behaviour or settings in the vehicle, by writing to *actuator* signals. (Specific access-control and security measures must of course be implemented on such features, but that is true even for reading information).

Some companies use the VSS model/method inside the vehicle, and that may include use of the signals as defined in the standard catalogue. Others still have proprietary internal data formats and may prefer to translate to a standard data model like the VSS, just before the data transfer from vehicle to offboard databases (a.k.a. OEM cloud), or even after the data has reached those offboard systems.

Further information can be gathered from the VSS definition at https://github.com/COVESA/vehicle_signal_specification and by following the **Common Vehicle Interface Initiative (CVII).**

The Common Vehicle Interface Initiative (CVII) is an overarching initiative to coordinate companies, member-organisations, formal standards organisations (ISO), researchers, legislators and other stakeholders towards establishing a common data model in the whole automotive industry. VSS is being proposed as the starting point for this model, and appears to be accepted and developed into becoming the chosen standard.

CVII is a cross-organization effort started by GENIVI/COVESA and W3C. At COVESA the CVII home page: https://wiki.covesa.global/x/EYBX, includes information about how to join various community mailing lists, weekly teleconferences and other activities related to the CVII.

### 2.2.5 API Methods in Scope

The OPIN domain model also defines the interface to query from the Insurance system. The interface relevant to the insurance organisation is specifically the GET/PUT restful interface you must adopt on the vehicle domain. All implementations must be accessible over the HTTP/HTTPS protocol and must be enabled using a RESTful interface on the Vehicle domain in the OPIN model, and is expected to be published using JSON format, however other formats may be supported.

## 2.3. Guidance to Implement the Data and API Interface

This section describes the implementation of an API and Data schema, and supports a basic introduction to the API and schema adoption, any further questions and clarifications can be submitted with further guidance planned.

### 2.3.1. Technical Steps to Adopt the Standard

In order to adopt and start with the data standard the following steps are recommended.

1. Access to the schema and supporting documentation can be found here, and you will require to register and request access to the files/libraries.
2. The libraries will provide the data contracts and API interface the system must implement.
3. You may need to interpret or serialise the contract into the corresponding formats your systems apply, but must maintain the principles and guidance for conforming to the open standard.
4. To seek guidance or further clarifications you can also request additional guidance on GitHub.
5. In order to submit changes to the OPIN mobility standard or indeed provide feedback you can submit requests, more details on change management can be found in the Use Cases document

## 2.4. Testing Scenarios and Access to Support

The following test scenarios are designed to ensure that there is sufficient test coverage of the critical elements of the POC such that the POC can be determined to have proved the logical and technical implementation of the concept. This is not intended to be a comprehensive set of scenarios, rather it sets out a format and approach that should be built upon by any organisations wishing to implement any of the OPIN use cases.

The use cases that OPIN has developed cover steps that occur outside of the OPIN solution but are either precursors to OPIN activity or impacted by data or activity from OPIN enabled insurance. To support this concept, the test scenarios will only cover the points in a use case where OPIN receives data, processes data or produces data.

All use cases are detailed here.

| **Test Scenario for Use Case Scenario 1/A - Vehicle Purchase** | | |
|---|---|---|
| In this scenario (Scenario 1/A - Vehicle Purchase), the driver takes ownership of a vehicle and the Original Equipment Manufacturer (OEM) arranges a connected insurance policy. | | |
| **Use Case Step** | **Scenario ID** | **Scenario Description** |
| The OEM confirms whether there is an existing policy | 1/A.01 | Verify that the driver does not have an existing insurance policy for the vehicle |
| | 1/A.02 | Verify that the driver does have an existing insurance policy for the vehicle |

| | | |
|---|---|---|
| If a policy exists, the existing policy is updated to reflect the new vehicle | 1/A.03 | Verify that the policy provided covers the driver |
| | 1/A.04 | Verify that the policy has not lapsed |
| | 1/A.05 | Verify that the policy is updated to cover the vehicle |
| If the policy is new, the driver is asked to supply relevant risk details e.g. driver particulars, claims history etc. | 1/A.06 | Verify that the risk details are acceptable to the underwriting rules of the insurance product |
| | 1/A.07 | Verify that the risk details are valid in regards to the driver |
| For either new or existing policies, the vehicle data is derived from the OEM | 1/A.08 | Verify that the data retrieved from the vehicle is consistent with the data requirements to generate a quote. |
| The OEM sets the coverage of the policy and updates the vehicle account with this information | 1/A.09 | Verify that the cover object is set with the appropriate data pertaining to the vehicle. |
| | 1/A.10 | Verify that the cover object is set with the appropriate data pertaining to the driver |
| | 1/A.11 | Verify that the cover object is set with the appropriate data pertaining to the policy |
| | 1/A.12 | Verify that the vehicle account is updated with cover details |
| The OEM binds the driver to the vehicle and policy in order to create a connected policy | 1/A.13 | Verify that the connected policy is generated |
| | 1/A.14 | Verify that the connected policy contains the correct details relating to risk |
| | 1/A.15 | Verify that the connected policy contains the correct details relating to vehicle |
| | 1/A.16 | Verify that the connected policy contains the correct details relating to driver |



| **Test Scenario for Use Case Scenario 1/D - Operate Vehicle** |
|---|
| In this scenario (Scenario 1/D- Operate Vehicle) the driver operates their vehicle, driving it, parking it, taking it for a service, responding to recalls and taking it for a repair. The OPIN insurer records this information to build a view on the driver and |

| how they drive, maintain and operate their vehicle. | | |
|---|---|---|
| **Use Case Step** | **Scenario ID** | **Scenario Description** |
| The insurer collects driving behaviour from the telemetry available from the vehicle | 1/D.01 | Verify that the behaviour data received links to the correct insurance account |
| | 1/D.02 | Verify that behaviour data received is consistent with known parameters |
| The insurer collects parking information (times, location etc…) from the vehicle | 1/D.03 | Verify that the behaviour data received links to the correct insurance account |
| | 1/D.04 | Verify that the parking time received is consistent with known parameters |
| | 1/D.05 | Verify that the parking location received is consistent with known parameters |
| The insurer updates the driver's driving record | 1/D.06 | Verify that the correct driving record is updated |
| | 1/D.07 | Verify that the record update is successful |
| | 1/D.08 | Verify that the driving record is immutable without appropriate API access |
| The vehicle notifies the driver that a service is due, given locality information the vehicle could also recommend the most convenient location for a service | 1/D.09 | Verify that the service notification is generated |
| | 1/D.10 | Verify that the service notification is generated within acceptable parameters (miles driven since last service/date) |
| | 1/D.11 | Where applicable, verify that the service location is appropriate in regards to distance from vehicle's location |
| | 1/D.12 | Where applicable, verify that the service location is appropriate in regards to vehicle type (electric vs Internal Combustion) |
| | 1/D.13 | Where applicable, verify that the service location is appropriate in regards to vehicle manufacturer |
| | 1/D.14 | Where applicable, verify that the service location is appropriate in regards to any prioritised lists from OEM/Insurer |
| The OEM updates the service record for the vehicle | 1/D.15 | Verify that the service record has been appropriately updated |

| | | |
|---|---|---|
| The OEM queries the vehicle locations and triggers a recall to a convenient location based on the vehicle's location | 1/D.16 | Verify that the service location is appropriate in regards to distance from vehicle's location |
| | 1/D.17 | Verify that the service location is appropriate in regards to any prioritised lists from OEM |
| The OEM updates the vehicle record (recall) | 1/D.18 | Verify that the vehicle record has been appropriately updated |
| It (the vehicle) queries location and OEM dealer network to make suggestions of where to take the vehicle for resolution (Vehicle identifies issue) | 1/D.19 | Verify that the service location is appropriate in regards to distance from vehicle's location |
| | 1/D.20 | Verify that the service location is appropriate in regards to any prioritised lists from OEM |
| The OEM updates the vehicle record (Vehicle identifies issue) | 1/D.21 | Verify that the vehicle record has been appropriately updated |

| **Test Scenario for Use Case Scenario 1/E - Vehicle Returned/Sold** | | |
|---|---|---|
| In this scenario (Scenario 1/E-Vehicle Returned or Sold) the driver returns or sells their vehicle. The OPIN model requires that the driver and vehicle are delinked. | | |
| **Use Case Step** | **Scenario ID** | **Scenario Description** |
| The OEM removes digital keys, removes driver data from the vehicle and updates vehicle ownership record | 1/E.01 | Verify that the digital key access is revoked from the vehicle |
| | 1/E.02 | Verify that the driver data is removed from the vehicle |
| | 1/E.03 | Verify that the vehicle ownership record is updated |
| The Vehicle/OEM removes driver access (revokes accounts) | 1/E.04 | Verify that the driver access accounts in the vehicle are revoked |
| | 1/E.05 | Verify that the driver data is removed from any OEM linked accounts |
| The insurer updates vehicle information and driver data | 1/E.06 | Verify that the customer's insurance record has been updated to remove the vehicle. |

| **Test Scenario for Use Case Scenario 1/G - Driving Style and Intensity** | | |
|---|---|---|
| In this scenario (Scenario 1/G- Driving Style and Intensity) the driver operates their vehicle, driving it, and the data from the vehicle sensors is recorded by OPIN Insurer to build a driver profile. | | |
| **Use Case Step** | **Scenario ID** | **Scenario Description** |
| Driver operates vehicle | 1/G.01 | Verify that the sensor recordings indicate that the vehicle is in motion |
| The driver enables real time monitoring | 1/G.02 | Verify that the driver has enabled real time monitoring |
| | 1/G.03 | Verify that, if the driver has not enabled real time monitoring, that driver intensity data is not captured |
| The vehicle provides data to the OEM about the driver's driving style (Speed, braking, distance, driving time, highway driving time, urban driving time etc…) | 1/G.04 | Verify that the data received is consistent within known parameters |
| | 1/G.05 | Where data is inconsistent, highlight for further analysis |
| The insurer returns any accidents or incidents relating to the driver/vehicle | 1/G.06 | Verify that the driver relevant insurance data relates to the driver |
| | 1/G.07 | Verify that the vehicle relevant insurance data relates to the vehicle |
| The combination of vehicle specification, driving behaviour and accident history is written to the driver's driving behaviour profile. | 1/G.08 | Verify that the record is consistent with known parameters |
| | 1/G.09 | Where the record is inconsistent, highlight for further analysis |

| **Test Scenario for Use Case Scenario 1/J - Vehicle Incident - Impact - Vehicle Led Notification** |
|---|
| In this scenario (Scenario 1/J- Vehicle Impact) - The vehicle detects an impact event which triggers in-vehicle systems to reach out for assistance either from an |

| insurer or a concierge service. | | |
|---|---|---|
| **Use Case Step** | **Scenario ID** | **Scenario Description** |
| A vehicle sensor is triggered | 1/J.01 | Verify the content of the signal message for data (location, time, severity, telemetry) |
| | 1/J.02 | Verify the content of the signal message for context (has an impact actually occurred?) |
| Is the vehicle concierge equipped? | 1/J.03 | If appropriate (concierge equipped), verify the message is routed to the appropriate OEM concierge service |
| | 1/J.04 | If appropriate (concierge not equipped), verify the message is routed to the appropriate insurance service |
| If support is required, the concierge service triage the needs of the driver<br>● (If there is immediate danger, the concierge service notify the emergency services) - optionally to consider<br>● (Otherwise the concierge service contact the insurer) - optionally to consider<br>● The insurer initiates the FNOL/recovery process. | 1/J.05 | Verify that the details received from the incident and concierge service are sufficient to instigate FNOL |
| | 1/J.06 | Where appropriate, verify that recovery action is initiated |

| **Test Scenario for Use Case Scenario 1/M - Assessing and Costing Damage in real time** | | |
|---|---|---|
| In this scenario (Scenario 1/M - Assessing and Costing Damage in real time) the insurer is able to simplify FNOL initiation by vehicle allowing for automated accident recognition by the insurer as soon as the driver is involved in an accident. | | |
| **Use Case Step** | **Scenario ID** | **Scenario Description** |

| | | |
|---|---|---|
| Vehicle systems recognize a crash | 1/M.01 | Verify the content of the signal message for data (location, time, severity, telemetry) |
| | 1/M.02 | Verify the content of the signal message for context (has an impact actually occurred?) |
| | 1/M.03 | If an impact event has not occurred, flag the event for further analysis |
| Vehicle captures several seconds worth of data leading to and after the accident (a snapshot) | 1/M.04 | Verify that the incident is recorded in the snapshot |
| | 1/M.05 | Verify that calls to additional data sources are triggered (weather APIs etc…) |
| Insurer initiates FNOL using snapshot data | 1/M.07 | Verify that there is sufficient data in the snapshot to initiate FNOL |
| | 1/M.08 | If there is insufficient data to generate FNOL, flag record for further analysis |
| Insurer guides driver in capturing images/video recording of damage | 1/M.09 | Recall the policy details to enable an outbound contact to the driver |
| | 1/M.10 | Verify the driver's details |
| | 1/M.11 | Confirm driver is content to capture details |
| | 1/M.12 | Verify response from driver |
| If data analytics capability is available to insurer<br>● Reconstruct accident<br>● Estimate list of damaged parts and cost of repair | 1/M.13 | Verify that there is sufficient data in the snapshot to reconstruct accident environment |
| | 1/M.14 | If there is insufficient data to generate accident details, flag record for further analysis |
| | 1/M.15 | Verify that there is sufficient data in the snapshot to determine damage to vehicle |
| | 1/M.16 | If there is insufficient data to determine the full extent of vehicle damage, flag record for further analysis |
| Resolve claim<br>● Initiate repair process<br>● Declare total loss | 1/M.17 | Verify that the appropriate data and analysis is available for the resolution decision |
| | 1/M.18 | If there is insufficient data to make a resolution decision, flag record for further analysis |

| **Test Scenario for Use Case Scenario 1/O - Damage to third party property** | | |
|---|---|---|
| In this scenario (Scenario 1/O - Damage to third party property) issues such as determining the nature of objects collided with, or the extent of damage caused to multiple third parties can be further complicated when multiple insurers are involved. | | |
| **Use Case Step** | **Scenario ID** | **Scenario Description** |
| Vehicle detects impact damage | 1/O.01 | Verify the content of the signal message for data (location, time, severity, telemetry) |
| | 1/O.02 | Verify the content of the signal message for context (has an impact actually occurred?) |
| | 1/O.03 | If an impact event has not occurred, flag the event for further analysis |
| Insurer uses scenario 1/M to assess and cost damage in real time | 1/O.04 | Verify the output from scenario 1/M to ensure that is is suitable to instigate FNOL |
| | 1/O.05 | If there is insufficient data or analysis to generate FNOL, flag record for further analysis |
| Insurer initiative FNOL<br>● If third party is insured by an OPIN insurer<br>○ Verify accident information<br>○ Receive claim recovery information and quantum | 1/O.06 | Verify theThird Party insurer's OPIN status |
| | 1/O.07 | Verify the information received from the insured in relation to the claim |
| | 1/O.09 | Verify the information received from the Third Party in relation to the claim |
| | 1/O.10 | Verify the additional data that is available in relation to the claim (Weather APIs, witness dash cam etc…) |
| | 1/O.11 | Compare the claim recovery information against the available data and proceed to settle or review. |

| | | |
|---|---|---|
| ● If third party is not insured by an OPIN insurer<br>○ Estimate loss to third party | 1/O.12 | Verify the information received from the insured in relation to the claim |
| | 1/O.13 | Verify the information received from the Third Party in relation to the claim |
| | 1/O.14 | Verify the additional data that is available in relation to the claim (Weather APIs, witness dash cam etc…) |
| | 1/O.15 | Compare the claim recovery information against the available data and proceed to settle or review. |

Please refer to the Use Case paper for full details of all use cases and their business scenarios.

# 3. PROPOSED ARCHITECTURE, TECHNOLOGY APPROACH AND GUIDANCE

This section describes the logical composition of the end to end technology system and the boundaries of responsibilities that would be typically needed to implement a scenario that supports both the OPIN and VSS API and Data standard. This section provides technical guidance to support all adoption approaches and is not a constraint or a solution that must be followed.

## 3.1. Logical View of the Solution

The diagram below describes the boundaries of ownership of technical solutions and systems that we would expect to be required to adopt the data standard and elaborate one of the use cases that we have provided.

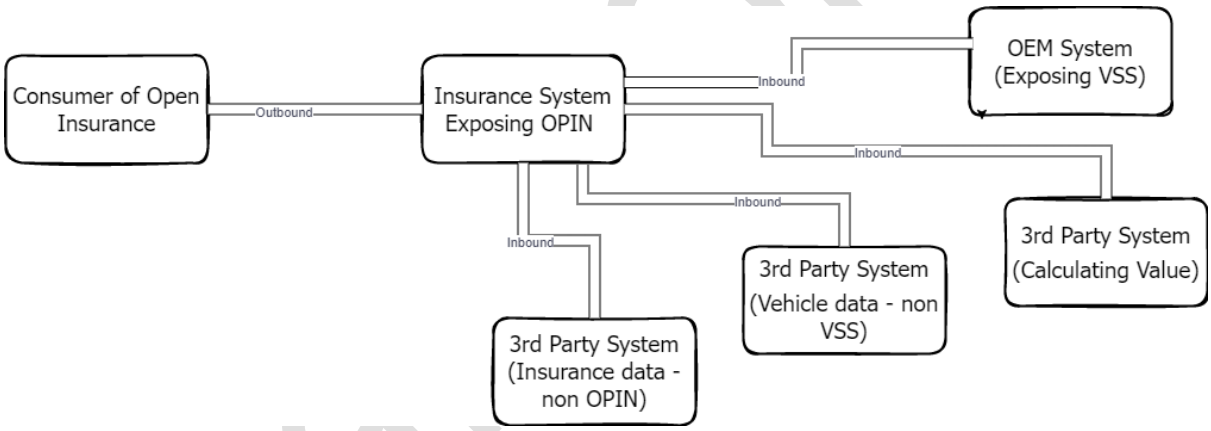



**Figure 1 - Logical View of all potential systems of ownership**

A system of ownership means a boundary of technical responsibility for each element of the solution. A system of ownership has a context and responsibility needed to ensure the adoption is successful.

### 3.1.1. Systems of Ownership

There are three systems of ownership:

**Insurance system(s) exposing OPIN**

- To provide an interface that supports the OPIN data schema and can be consumed on a open technical standard (e.g. JSON) and can maintain performance of the

indicative frequencies of information required on the attributes defined

- The insurance system must be able to perform to non-functional needs, including
    - Service concerns separation
    - Service contract
    - Service abstraction
    - Service autonomy
    - Service reusability
    - Service state
    - Service loose coupling

Service orientation and these concepts whilst not technology specific, drive a vendor and technology generic composition of the system. This is a key tenant of an open insurance model to support the ability to be truly open, portable and vendor agnostic. Much deviation and derivation has since evolved from the principles of service orientation, however the key basis remains true today, that in order to drive an open model for adoption, these principles allow for any organisation to participate.

The insurance system exposing OPIN will consume data to augment the motor insurance proposition, from OEM systems (e.g. a VSS cloud capable system), 3rd party systems that augment the Insurance proposition from other 3rd party vehicle systems or 3rd party insurance systems.

**OEM System Exposing VSS**

Is a system that exposes vehicle data according to the signals and attributes supported by the system. The OPIN standard will support the vehicle VSS specification. The OEM system will provide attributes according to the data catalogue and frequencies identified.

A vehicle will be sharing and communicating signals with the OEM system according to the events occurring within the vehicle.

**Consumer of Open Insurance**

Is a system, person or organisation that subscribes to information exposed from the insurance system exposing OPIN. This scenario could be an Insurance customer platform, an insurance claims platform or a third party partner platform providing insight.

**Third Party System**

Scenarios articulated in the use cases document may require additional enrichment of information from other data sources, or also from a third party system that calculates value using the standard for a given scenario, for example, calculating driver behaviour factors and exposing this data. This may occur for example when consuming or providing data from organisations that openly share service history for a vehicle, for example from a reparier

system. This document does not explicitly state those systems or organisations or intend to recommend vendors to adopt.

**Network and Connectivity System**

The network and connectivity system refers to the connectivity from vehicle, insurance and third party systems that would typically be needed to support inbound and outbound requests/responses, and identifies the potential for ensuring reliability is in place on the connectivity system, and if not the mechanism by which all data is managed and persisted to support transactions securely.

Each System of Ownership has a sub classification of Application and Data components. For example, an Insurance system has a Claims application and Data component, of which that component(s) will need to provision the relevant data standard.

The following diagram illustrates a typical vehicle-to-cloud data architecture. The exact details (e.g. choice of protocols and component names) is still being evolved and subject to change.

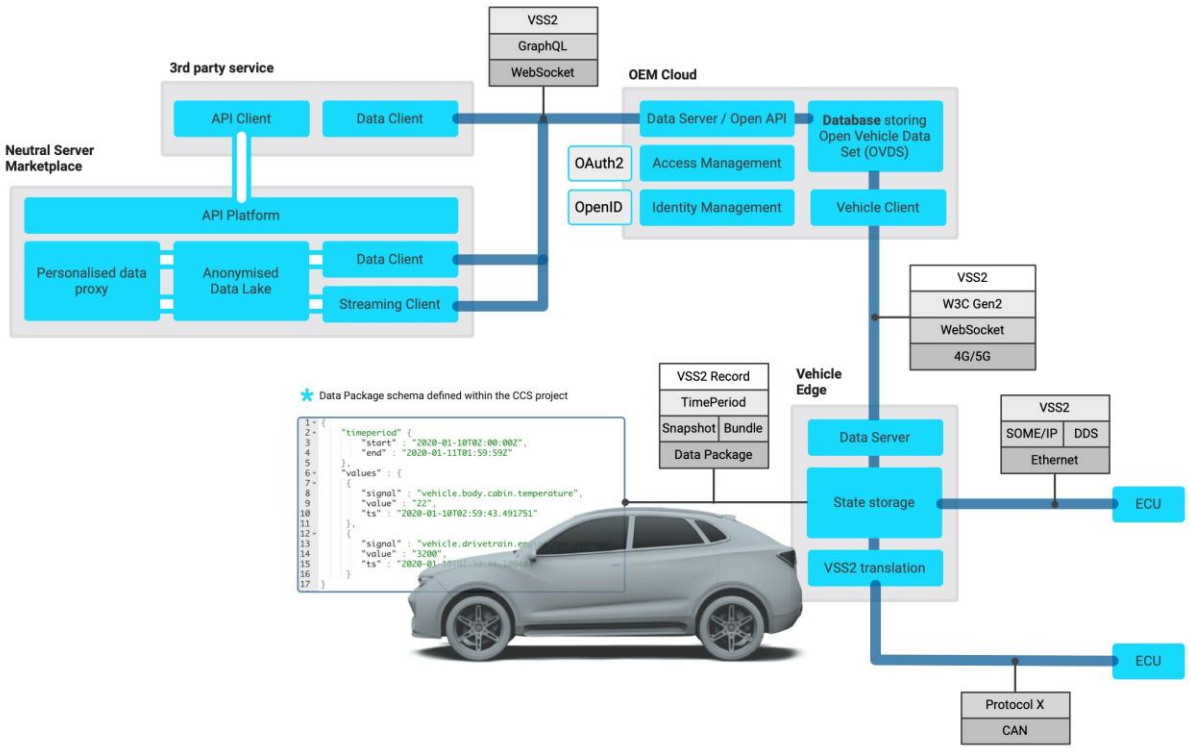



**Figure 2 - COVESA Cloud and Connected Services**

There are few ways that vehicle data is made available to third parties:

- In-car applications that have internet access. This is common in Android-based infotainment systems but vehicle data APIs are generally limited to only what popular applications need, and each application has to separately apply for API privileges (in our context meaning they get access only to a selected *subset* of the available data), and these privileges usually involve approval by some combination of the car OEM, as well as the car owner/driver/operator.
- OEM's may have contracts with data brokers, a.k.a. "neutral servers", that broker data from (multiple) OEM's to third parties, such as the insurance industry. OEM's are generally in control of the conditions for sharing that data, e.g. involved in approving which third party is allowed to get access.
- OEM's may strike deals where they deliver data directly from the OEM cloud to insurance partners (companies or organisations).

The analysis of the required data (ref chapter 2.1) also yielded different categories of data to fulfil the needs of each insurance use case:

1. Some information is static and typically collected by the insurance companies directly from their customer
2. Some information may be collected by the OEM in their own customer relationship databases
3. Some information needs to be real-time information coming from vehicles while they are operational

The combination of typical data-access methods and varying nature of data lead to that the solution must consider multiple data-sources and data paths. Simply put, the complete information needed to fulfil insurance use cases must gather data from several sources that are reflected in the logical architecture:

In addition to the vehicle-to-cloud architecture shown above, we must add some additional data sources and API endpoints.

**OEM-Controlled Customer Related Data**

This requires the definition of an API at each OEM that insurance companies/organisations can get access to.

**Vehicle-related Data Gathered from Vehicle**

This requires the definition of an API either at a *neutral-server* data provider or at each OEM. Projects such as COVESA's CCS and CVII are working to find alignment in the industry towards agreed data-formats and APIs.

The following section describes the API's exhibited in the OPIN standard and the endpoints, which includes the data requested/responded. The diagram below shows an illustration as guidance of how the application and data components fit in the architecture, and also provides indications of the expected performance of the system.

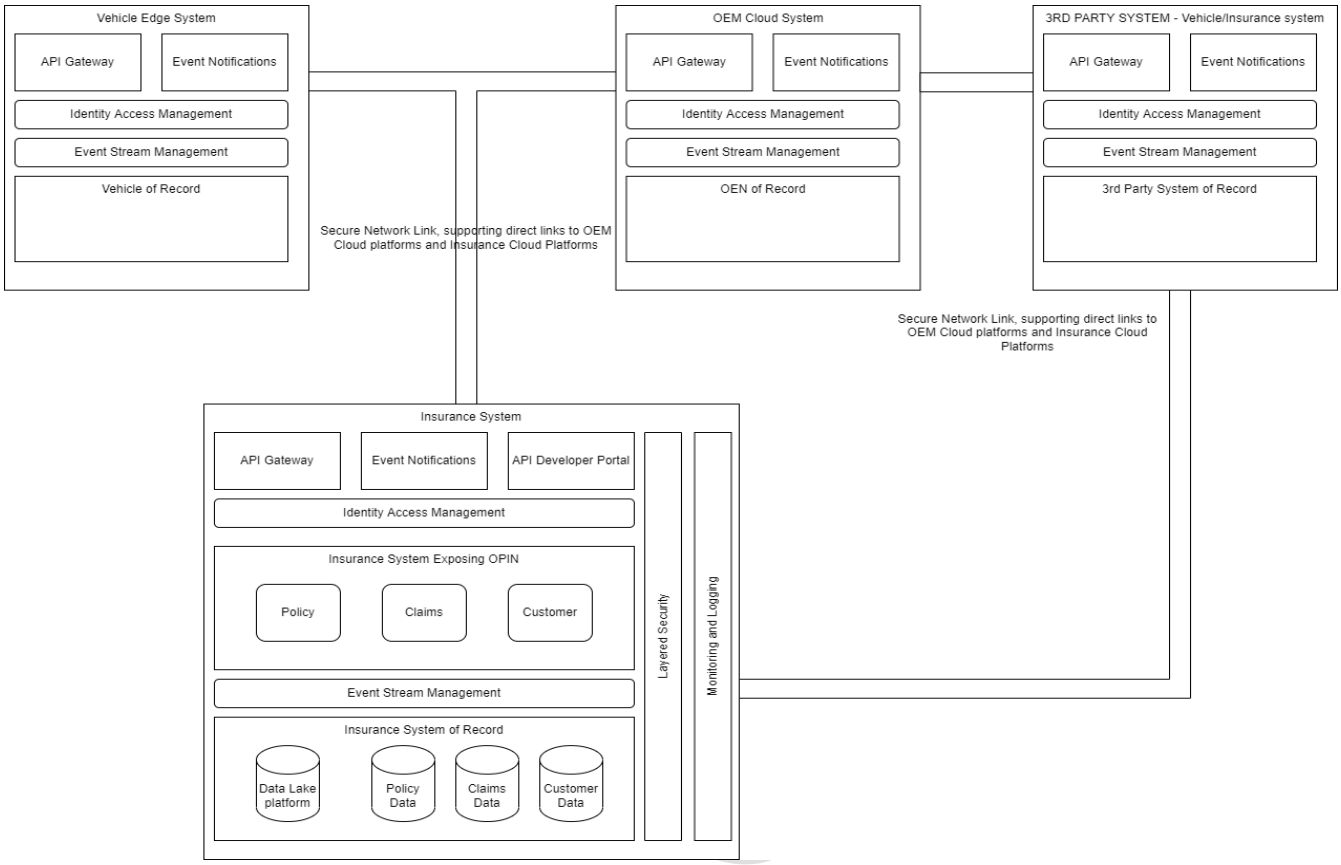



**Figure 3 - Logical View of all Application and Data components**

The diagram above shows the Application and Data components in four system areas, the Insurance System, Vehicle Edge System, OEM Cloud system and third party system.

## 3.1.2. Technology, Application and Data System Components

**API Gateway** - An API Gateway that supports:

- Portability – can be deployed anywhere.
- Flexibility – multiple gateways can be controlled from a single admin console.
- Extensibility – off-the-shelf plug-ins provide the ability to extend the platform, offering a wide range of functionality. Can also develop custom plug-ins.
- Stability & Performance – offers a resilient API gateway, which can be monitored to a detailed level, as well as the capability to scale for high throughput.

**Event Notifications** - Providing the capability to share state change events with partner organisations streamlines the exchange of data (e.g. removes inefficient polling processes), and allows partners to optimise how they use that data.

- This will provide the ability for trusted partners to subscribe to Event Streams via self-serve web-hooks, i.e. the consumer calls a Open API (the web-hook) for a specific type of event, and provides an endpoint to which to send the change events.

- Once the subscription is created, events will be sent automatically to the consumer who can act on the event.

**Insurance Systems Exposing OPIN** - Open Insurance services architecture based on the domain model explained in this document, this provides:

- Improved agility – able to make changes and deploy much faster (multiple releases a day)
- Continual improvement/quality – as change is easier to effect, qualitative modifications can be made and released more often
- Scalability & availability – stateless services provide the ability to significantly scale horizontally to meet growing or peak demand. Coupled with capabilities for automated 'elastic' scale-out, the overall service availability improves.

**Event Stream management** - The ability to capture change as events from all systems, and stream those events so that they can be consumed and acted upon is a cornerstone of the architecture. The main benefits of enabling event streaming include:

- Loosely-coupled applications – enables a dynamic delivery cycle due to low dependencies between applications
- Innovation driver - new applications can easily subscribe to the stream to consume data and present that in innovative ways
- Can track state change over time of data – not simply the current state. Event Stream, with event stores and services enable EDA (Event Driven Architecture)

**Insurance System of Record** - is a data and analytics service. The main goals are:

- Enhanced analytical capabilities
- More data, easily accessible
- Improved data quality, reporting and MI
- Scalable, flexible products offering easier internal and external integration
- A governance structure to ensure data is protected to meet legislative standards, and most importantly, the expectations of customers.

**Layered Security** - A distributed architecture comprised of multiple layers, e.g. API Gateway, Cloud Infrastructure, microservices, service mesh etc, exposes, for the individual components, a reduced attack surface

- It can, however, provide multiple entry points to the platform.
- This approach to securing our data, services and infrastructure takes a tailored, layered approach, i.e. providing appropriate levels of security to the data being handled, throughout each layer of the technical stack.

**Monitoring and Logging** - A comprehensive view of infrastructure health indication of service status, as well as managing alerts to ensure the correct resources are informed of failures/warnings at an appropriate time.

• For distributed systems, monitoring is a critical feature. Monitoring will be built into each component of the architecture, from API Gateway to individual service, with logs being aggregated centrally.

**Third Party system** - Integrate with Insurance systems e.g. Underwriters to access policy and quote details for customers, and integration to other Third Parties including product catalogues, or for example for booking vehicle repairers. Services and components which together provide the ability to drive UX applications, and interface with Claims services.

## 3.2. Application and Data components

The inner workings of a component that publicises an OPIN standard would be similar to the composite pattern below, whereby any consumer or internal, external or partner system can consume the API via a reliable API Gateway.

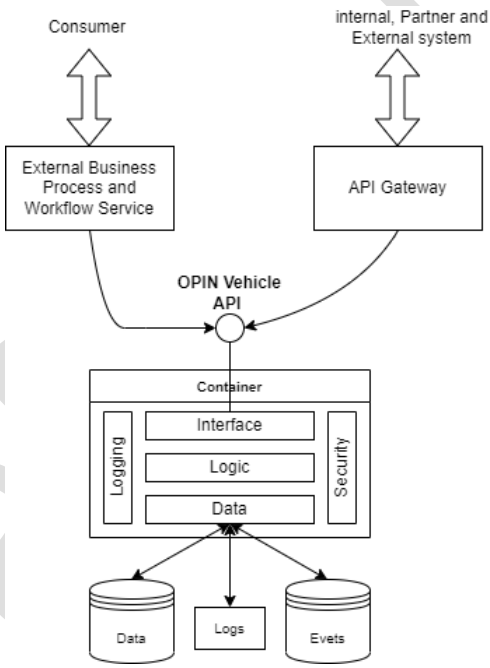



**Figure 4 - Application and Data component, the inner composite design**

This model represents how the decoupling of the OPIN API sits on a modular design that represents interface, logic and data. Data has many modes of transition or storage and can be persisted in a data store, for insurance transaction to perhaps a Policy administration system or a Claims administration system, but also supports real time events that may be persisted in an Event store that supports real-time publishing of a given event. Logs represent the suitably anonymised mechanism by which performance and alerting could be managed in a supporting system.

Having these layers of decoupling in a technology approach allows for service change and loose coupling, which abstracts the publisher or the consumer from any tightly coupled vendor specific schematic or notation, and allows the standard to be implemented in an open manner.

## 3.3. API Components

An API on the insurance system must expose a service and data contract to that which confirms to the OPIN standard v2.0, the standard will be expressed in a non-native, standard open source format, and can be serialized/deserialized into any interpretative native language you require for your own processing. No native schematic standards representative of a specific vendor or internal system must be exposed as part of the implementation, and as so it is recommended you follow the principles of service orientation, by taking a contract-first approach and abstracting all implementation specific languages, functions and notations, or this would break the implementation of the open standard.

## 3.4 Business Process Illustrations

The OPIN Mobility Group has developed a series of use cases complete with high level business processes. The use cases cover the main aspects of an insurance journey.

This includes Purchase, Claim, Cancel, as well as key aspects of operating a motor vehicle, Drive, Park, Maintain, Incidents and Sale, these scenarios are not exhaustive but were designed to allow the development of end to end processes by combining scenarios. For example, combining Scenarios 1A - Vehicle Purchase (including insurance) with 1/G Driving Style and Intensity, 1/H Safety Feature and Usage, and 1/E Vehicle Returned/Sold would allow for a scenario covering the major points of owning and driving a connected and insured vehicle.  This is just an example and more detailed scenarios can be built from the selection of scenarios that have been elaborated into use cases.

The full list of available use cases is as follows:

**Insurance Distribution - Pre Sale and Sale**

- 1A - Scenario: Vehicle Purchase
- 1B - Scenario: Vehicle Purchase with Embedded Finance
- 1C- Scenario - Insurance Purchase (Direct)

**Vehicle Operation and Maintenance**

- 1/D- Scenario - Operate Vehicle - Servicing
- 1/E- Scenario - Operate Vehicle - Return/Sold
- 1/F- Scenario - Vehicle Insured Status
- 1/G- Scenario - Driving Style and Intensity
- 1/H- Scenario - Safety Feature Usage
- 1/I- Scenario - Safety Feature Deployment

**Vehicle Incidents**

- 1/J- Scenario - Vehicle Incident - Impact - Vehicle led notification
- 1/K- Scenario: Early detection, warning and assistance during a flood
- 1/L- Scenario: Vehicle Incident - Stolen- Vehicle led notification
- 1/M- Scenario: Assessing and costing damage in real time
- 1/N- Scenario: Crash of autonomous car into a moving vehicle
- 1/O- Scenario: Damage to third party property
- 1/P- Scenario: Prescriptive analytics

The full use case document is available here.

# 4. INFORMATION, DATA AND TECHNOLOGY SECURITY

The systematic security controls for the POC are not defined explicitly in the entirety however the following provides recommended guidance to consider when implementing the systems identified.

## 4.1. API and Data Security

Most vehicle data will be provided under vehicle OEM supervision, meaning that data gathering is unlikely to occur with direct connections from an insurance company to individual vehicles. Thus, referring to the logical design, the entrypoint for collecting vehicle-related data will be either individual OEM-clouds, or a data broker (a.k.a. Neutral Server) that aggregates data from potentially multiple car OEMs. These systems will build the necessary authentication and authorization mechanism for the data collection.
The OPIN API entrypoint must in turn provide adequate authentication and authorization implementations to ensure only authorised clients are able to access API services. Information handled by these systems may be privacy sensitive and/or commercially valuable and it follows that data shall be encrypted in transit on any non-private (Internet) communication links.

It is also expected that the relevant network protocols are suitably protected and encrypted to ensure the encryption of data being transmitted between all systems of ownership, and must ensure that data is not manipulated at rest or in-flight by any threats to the sovereignty or accuracy of the data interchanged.

## 4.2. Data Protection And Standard Requirements

In line with data protection standards , including Personally Identifiable Information (PII) and GDPR standards, to ensure data is protected whilst in rest, in transit or cached during any state persistence in the solution implemented.

In addition suitable testing must be conducted to demonstrate the relevant testing has according and accordance including conformance to Cloud Security and Open Web Application Security Project (OWASP), due to the sensitive nature of the use cases provided also and the impact to the public in scenarios that would include significant personal loss, the solution must be able to demonstrate the reliability and operational resilience to be considered a solution that ensures no intolerable harm to the public.

# 5. LEGAL AND COMPLIANCE GUIDANCE

Please note at the time of publishing the legal guidance to support the paper will be published in early 2022 and will be referenced here once published.

Attention to privacy and compliance was maintained during numerous discussion and use case development sessions. Emphasis was made on only receiving vehicle data that is directly relevant to the use case in question and at a data-request frequency that is reasonable for purpose.

Indeed, by inspecting the Data Catalogue - Use Case Data document containing the OPIN-VSS aligned data properties, it can be seen that less than 90 additional data properties (sensor and control data) have been added to the OPIN data schema to satisfy the use cases examined.

Data generated by connected vehicles fall into four general categories:

1. Location data relating to travel destinations.
2. Data relating to driver behaviour
3. Vehicle performance and state
4. Data related to the environment surrounding the vehicle

Proactive privacy by design and using data in an ethical manner will reinforce consumer trust. This also means compliance with GDPR, CCPA, IDD and numerous other important directives. Legal uncertainties around data access and privacy were common during group discussions. And the following sections will provide some clarity.

It will be difficult to discuss laws and regulations of different countries or economic regions within one document, therefore, this section will discuss EU and UK (to a lesser extent) laws and developments.

At this juncture it is important to mention that OPIN concurs with the views of the My Car My Data initiative that access to the driver's mobility habits can only happen with their informed consent thereby the vehicle owner controls whether data can be shared, with whom and how it is going to be used.

The EU's GDPR distinguished between personal and non-personal data. Data is treated as personal data if it can be linked to one or more identifiable individuals and that is where privacy laws require the informed consent of the user over who accesses and processes this data. Practically, much of the data produced by connected cars can be treated as personal data therefore privacy laws apply to car data. The law does not distinguish between the primary nature of data, be it technical or otherwise.

The data portability principle of GDPR empowers car owners to transfer their data to third parties and car manufacturers should not deny third parties access to this data. Vehicle Car owners can decide with whom car data is shared and processed independent of the vehicle

manufacturer. This means the data can be transferred from one data controller to another and it has to be in a common, machine readable format.

It should be noted that safety and liability obligations do not permit OEMs to permanently collect and evaluate data. This could apply to insurers within the context of UBI or other connected insurance products. The sale of such products does not permit insurers to permanently collect and process driving data.

In the EU, the European Data Protection Board (EDPB) has recently published guidelines on the processing of personal data in the context of connected vehicles and mobility related applications. In particular it identified three categories of data that require special attention by all stakeholders. They include location data, biometric data and data revealing offences or traffic violations.

A number of the use cases that were developed by the mobility working group involved or relied upon receiving location data. The EDPB guidelines recommend that only necessary or most relevant data be collected and at reasonable frequency and detail to satisfy a particular process. Collection of location data should definitely not happen by default and the user should be notified when it happens.

The guidelines place great emphasis on the security measures protecting data relating to user biometrics, criminal offences and traffic violations.

For regulations to stand the test of time they have to match consumer as well as user demands. In this context, it is important to take note of how Open Banking standards have evolved. There are lessons to be had in how regulators are adapting their rules to improve process efficiency and support FinTech startups.

One such example is how the FCA has given Open Banking a boost by removing the 3 months re-authentication requirement. Previously, consumers using third party applications had to authenticate via Strong Customer Authentication (SCA) every 90 days, a feature that caused consumers high drop off rate. Notwithstanding, consumers still have a right to withdraw their consent at any time.

**DISCLAIMER**

This paper is only a presentation of information, ideas and speculation regarding possible technologies, the possible uses of those technologies and a possible community of users and builders of those technologies. The statements contained in this paper do not provide any advice, representation, warranty, certification, guarantee or promise relating to these technologies, any uses thereof or any of the other matters discussed in this paper, nor does this paper provide an offer or agreement to make such technologies available, maintain or update such technologies, or sell or buy any asset or enter into any transaction. This paper and the matters described in this paper have not been reviewed, approved, endorsed or registered with any regulator or other governmental entity, and the authors of this paper are not licensed by any regulator or other authority to provide any legal, financial, technical or other advice or services. We undertake no obligation to update, supplement or amend any statement that becomes inaccurate or incomplete after the date on which this paper is first published, or to alert the public as to any such inaccuracy or incompleteness, whether such inaccuracy or incompleteness arises as a result of new information we receive, changes of our plans, unanticipated events or otherwise. The technologies described and legal or regulatory opinions expressed in this paper are highly experimental, have uncertain standing, and must be directly evaluated by relevant experts before use. Use them solely at your own risk. You should not rely on this paper as a basis for making any decision.