Open Insurance

Interoperability of Insurance and Automotive Data Standards

Legal ⚙ Regulatory Examination

A dialogue between the Legal & Regulatory Working Group and the Mobility Working Group to discuss and reflect upon issues emanating from sharing access to the data generated by connected vehicles with insurers.

The Open Insurance Think Tank May 2022

INTRODUCTION

This document has been prepared by authors established in different jurisdictions. The purpose of the present document is to raise awareness of Open Insurance Think Tank (OPIN) members on legal and regulatory questions that may arise in the context of mobility related projects. The answers provided are based on either European/local EU Member State legislation, international guidelines, or Brazilian law. Brazil indeed since December 2021 has adopted an Open Insurance framework which may serve as an inspiration for future frameworks in other jurisdictions. An overview of this framework is provided here.

The content for this paper is designed as a set of 14 questions developed by members of OPIN's Legal & Regulatory Working Group (LRWG) in its examination of the data alignment project carried out by OPIN and COVESA (the global automotive alliance behind the development of the Vehicle Signal Specification (VSS)). The writing of this paper also coincided with the European Commission's publication of the proposed Data Act thus an additional section has been appended to the document to discuss its main provisions and provide our views.

The information contained in this document is provided for information purposes only and should not be construed as legal advice. You should not act or refrain from acting on the basis of any content included in this document without seeking legal or other professional advice. The content of this document may not reflect current legal developments or address your situation. We disclaim all liability for actions you take or fail to take based on the present document.

CONTENT

Section 1: Data Protection

Section 2: Pricing & Underwriting

Section 3: Evidence rules

Section 4:
The EU’s Proposed Data Act

What are the main threats influencing the share and use of personal data in the mobility sector? And what are the potential measures to handle them?

Q
1

There are four main threats:

- Security
- Breach of purpose limitation
- Lack of recipients’ limitation
- Lack of free consent

The new insurance landscape will have to deal with respect for user privacy. Today it is not correct to already speak of problems or criticalities, but of challenges, because privacy is in effect a pillar of the insurance sector and every process is also elaborated under its own path.

IVASS (Italian Insurance Supervisory Body) itself, in June of last year, published some reflections on the Open Insurance theme, focusing precisely on the privacy aspect, noting how "It will be necessary to verify the tightness of the existing regulatory system (GDPR - General Data Protection Regulation) with respect to the new needs of protection and it will be essential to safeguard, at every stage of the process, the correct use of customers' personal data[1].

This innovative approach, therefore, can - and must - be tailored to the needs of individual data protection. The crux of the challenge is the consent of the interested party: in the Open environment, personal data - even sensitive ones - are shared among multiple stakeholders. A single consent, for multiple data controllers.

This innovative approach, therefore, can - and must - be tailored to the needs of individual data protection. The crux of the challenge is the consent of the interested party: in the Open environment, personal data - even sensitive ones - are shared among multiple stakeholders. A single consent, for multiple data controllers.

How can you obtain a consent that is free, specific, unambiguous and informed? One option could be to elevate the privacy information from a mere bureaucratic fulfillment to a true instrument of trust owner-interested party, in accordance with the principles of the European Privacy Regulation (GDPR).

Q
1

Create information that is clear, simple and intelligible to enable the interested party to be able to express consent that is GDPR compliant.
This "new" information, combined with a discrete digital education of the user, will certainly be a valid tool from this point of view. The consent, then, must also be compliant with the E-Privacy Directive: all data processed by "terminal equipment" - such as those of the so-called connected vehicles - require specific consent. In this case, there is a double protection: the general one of the GDPR and the specific and sectoral one of the E-Privacy Directive.

The sharing of data between different stakeholders (financial, Big Tech, etc.) must also be viewed with the lens of the proportionality of the processing of personal data: only data that is strictly necessary to achieve one or more specific purposes can be shared; indiscriminate sharing of all data - even sensitive data - risks being non-compliant with the GDPR. It will be necessary to decide whether this sharing will be reciprocal or not.

The reference is to Big Tech, that is, to large technology companies - such as Google and Amazon - which offer services to both data subjects and data controllers (such as cloud computing services). Big Tech have a lot of information of commercial origin; insurance companies, on the other hand, have insurance data, which are in part sensitive.

At the moment, we are not talking about transmission reciprocity, but only about sharing insurance company-Big Tech and not vice versa. From this point of view, competition and consumer protection challenges arise, as business partners are not subject to extremely binding standards such as supervised partners. Particular attention must then be paid to the adoption of effective security measures for the transmission and sharing of data. The risks of these activities are many but they can be neutralized - or at least significantly reduced - upon the outcome of an impact assessment of the treatment and with the application of appropriate security measures.

What are the initiatives being studied by the EU that may have an impact on personal data protection (also) in the mobility sector?

Q
2

In 2021, at European level, was one that was characterized by an intense application of EU Reg. 679/2016 and by regulatory ferment, both in terms of privacy and antitrust. The protagonists of 2021 (and, without doubt, of 2022 in foresight), were, in particular:

- Proposal for a Digital Services Act (so-called DSA)[2] ;
- Proposal for a Digital Markets Act (so-called DMA)[3] ;
- Proposal for a Data Governance Act (so-called DGA)[4] ;
- Proposal for an E-Privacy Regulation[5] ;
- Proposal for a Network and Information Security (NIS) Directive (so-called NIS II)[6].

The aforementioned legislation represents, each for its own area and sector of competence, the concrete realization of an entire regulatory ecosystem that affects, in the whole, digital platforms, digital services, online marketing, data intermediaries and much more. Also of importance will be in 2022, the AI Act[7] , which will have a strong impact above all on companies and industrial groups that make use of decision-making processes, and the Data Act[8] , which - very briefly - extends some of the legal obligations envisaged for personal data, including restrictions on cross-border transfers, including non-personal data (read our perspective on the proposed Data Act at the end of the document).

Moreover, the European Commission intends to release towards the middle of 2022 a legislative proposal for an Open Finance framework, “promoting business-to-business data sharing in the EU financial sector and beyond”[9]. This Open Finance framework will most probably impact the insurance sector. The Open Insurance Think Tank is closely following this initiative and is represented within the European Commission Expert group on European financial data space[10] and within a subgroup dedicated to Open Finance[11].

2021 also saw the publication, by the European Data Protection Board (formerly WP29), of a series of important guidelines and opinions, aimed at harmonizing the text of the GDPR with the previous guidelines issued by WP29 and providing more practical indications for data controllers and processors (such as, for example, the guidelines on the meaning of international transfers[12] and on the notification of data breach)[13]. Although the guidelines are not binding regulatory instruments such as laws and regulations, they fall into the category of the so-called soft law.

They represent the sum of the best practices in the sector and constitute an evaluation element in the phase of ascertaining the violation of the GDPR by the Guarantor Authorities. In 2022, therefore, the EDPB will address new and important issues related to the correct application of the GDPR.

What mobility related personal data may be processed by insurance companies? For which purpose and for how long?

Q
3

For the avoidance of doubt, the following processing table solely considers processing for which insurance companies are acting as data controllers. Similar analysis should be performed for other stakeholders involved in the data processing, such as OEMs.

Also, it should be noted that the present analysis is performed in the light of GDPR. ePrivacy Directive also applies to the different processing listed below to the extent data are collected through a publicly available electronic communication service. In accordance with Article 5(3) of this ePrivacy directive, data subjects should consent to “the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user”[14] . This concretely means that in the context of “pay as you drive” or “pay how you drive” for instance, the policyholder must have the choice to subscribe to a non-usage-based insurance policy[15]. Please refer to the Mobility Use Cases document, previously published by OPIN, to be able to follow the analysis.

Name of process	Sub-processing	Lawfulness of processing	Categories of data subjects and of personal data	Retention duration
Policy subscription on vehicle purchase	Cf. Scenario 1A, 1B[16] and 1C (*Vehicle purchase, vehicle purchase with embedded finance, insurance purchase*)	Contract to which the data subject is a party (Art. 6 (1) (b) GDPR)	**Data subjects:** policyholders **Personal data:** **Commercial and transactional data:** data subject's identifying information, driving licence related information, transaction related data, data relating to means of payment **Risk details pertaining to policyholder:** driver history, claims history, historical driving behaviour (if available and to the extent the insurance policy is subscribed under "Pay as you drive" or "Pay how you drive").	Local limitation period

Name of process	Sub-processing	Lawfulness of processing	Categories of data subjects and of personal data	Retention duration
“Pay as you drive” “Pay how you drive” Creating driver profiles to offer driving behaviour-based insurance policies	Processing of personal data following the storage or access to the end-user’s terminal equipment (Use case 1G, *Driving style and intensity*)	Contract to which the data subject is a party (Art. 6 (1) (b) GDPR) provided it can establish both that the processing takes place in the context of a valid contract with the data subject and that processing is necessary in order that the particular contract with the data subject can be performed[17].	**Data subjects**: **policyholders**. Personal data: - **Commercial and transactional data:** data subject’s identifying information, transaction related data, data relating to means of payment, etc.; - **Usage data:** personal data generated by the vehicle, driving habits, location (however if only the mileage is necessary for the performance of the contract, location data shall not be collected), etc. As far as possible, raw data regarding driving behaviour should be either processed: - inside the vehicle in telematics boxes or in the user’s smartphone so that the insurer only accesses the results data (e.g., a score relating to driving habits), not detailed raw data; - or by the telematics service provider on behalf of the controller (the insurance company) to generate numerical scores that are transferred to the insurance company on a defined basis. In this case, raw data and data directly relating to the identity of the driver must be separated[18].	**Commercial and transactional data:** full duration of the contract + at the end of the contract, physical or logical archiving in the event of possible litigation. Thereafter, at the end of the statutory limitation periods, the data shall be deleted or anonymised; **Usage data:** Raw data: if processing 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[19].

Name of process	Sub-processing	Lawfulness of processing	Categories of data subjects and of personal data	Retention duration
Roadside assistance	Assistance in the event of an incident (Scenario 1J - *Vehicle Incident - Impact - Vehicle led notification* and 1K - *Early detection, warning and assistance during a flood*)	Contract to which the data subject is a party (Art. 6 (1) (b) GDPR)	**Data subjects:** policyholders. **Personal data:** policyholder's identification details, geolocation.	Local limitation period

Name of process	Sub-processing	Lawfulness of processing	Categories of data subjects and of personal data	Retention duration
Damage	Scenario 1M (*Assessing and costing damage in real time*), 1N (*Crash of autonomous car into a moving vehicle*),1O (*Damage to third party property*)	Data of the policyholder: contract to which the data subject is a party (Art. 6 (1) (b) GDPR) Data of other claimants: legitimate interests pursued by the controller (Art. 6 (1) (f) GDPR)	**Data subjects:** policyholders. **Personal data:** policyholder's identification details, geolocation, damage description and liability allocation	Local limitation period

Name of process	Sub-processing	Lawfulness of processing	Categories of data subjects and of personal data	Retention duration
Theft	Scenario 1L (*Vehicle Incident - Stolen- Vehicle led notification*)	Contract to which the data subject is a party (Art. 6 (1) (b) GDPR)	**Data subjects:** policyholders. **Personal data:** policyholder's identification details, driving behaviour.	Local limitation period

Name of process	Sub-processing	Lawfulness of processing	Categories of data subjects and of personal data	Retention duration
Delinking vehicle / driver	Cf. Scenario 1E (*Operate Vehicle - Return/Sold*)	Contract to which the data subject is a party (Art. 6 (1) (b) GDPR)	**Data subjects:** policyholders. **Personal data:** policyholder's identification details, plate number.	Local limitation period

Name of process	Sub-processing	Lawfulness of processing	Categories of data subjects and of personal data	Retention duration
Vehicle Insured Status	Cf. Scenario 1F (*Vehicle insured status*)	Data disclosed to driver: Contract to which the data subject is a party (Art. 6 (1) (b) GDPR) Data disclosed to telematics application / OEM: either contract to which the data subject is a party (Art. 6 (1) (b) GDPR) if such a contract has been entered into between the data subject and the data recipient requiring disclosure of vehicle insured status or consent (Art. 6 (1) (a) GDPR).	**Data subjects:** policyholders. **Personal data:** policyholder's identification details, connected insurance policy, plate Number, registration Data.	Local limitation period

Name of process	**Sub-processing**	**Lawfulness of processing**	**Categories of data subjects and of personal data**	**Retention duration**
Analytics	Scenario 1P (*Prescriptive analytics*)	Contract to which the data subject is a party (Art. 6 (1) (b) GDPR)	**Data subjects:** policyholders. **Personal data:** policyholder's identification details, plate number, vehicle use.	No longer than necessary, i.e. in the present case a few weeks or a few months after collection of personal data (unless specific need can be evidenced).

Box 1

View from Brazil

From the Brazilian perspective, data shall be processed by insurance companies on the exact limits of need and for as long as the data shall last for the purposes and on the limits established by the consent given by the client[20] or consumer. In Brazil, Open Insurance is regulated by Resolução CNSP 415/2021 and Circiular SUSEP 635/2021. As set forth by these regulations, along with the Open Insurance scope of data and services guidelines[21] , data shall be considered in two distinguished spheres: (i) open data related to insurance, which are information on service channels and insurance products, open supplementary pension and capitalization products, available for sale; and (ii) personal insurance data, which are information on the registration of customers, natural or legal persons, and their representatives, transactions related to insurance plans, open supplementary pension plans, financial assistance and capitalization, including the characteristics of the policy, ticket, certificate, contract or capitalization certificate, and the data of records made by electronic devices embedded, connected or used by the customer[22] . It is also important to consider, when analyzing the open insurance perspective, that data shall be analyzed along with the General Personal Data Protection Law[23] . It is important to note that driving behavioral data may not necessarily be analyzed through the open insurance ecosystem. In Brazil, this analysis is already made by some insurance companies, when the direct, restricted and undoubtful consent from the insured person is required. There are already some insurtechs (or even big insurance companies) that do this analysis by offering the consumer the possibility of, when good driving habits are configured, getting a discount on the premium or other benefits, either at renewal or at the current insurance policy. The data subject should receive a direct and explicit consent clause that shall be agreed by customer in order for the driving to be monitored.

In the event the insurance company intends to offer “Pay As You Drive” coverage, what specific information should be provided to the data subject?

Q
4

The data controller shall inform the data subject in accordance with Article 13 or 14 of GDPR, as the case may be and shall, where relevant, provide clear information about “the existence of automated decision-making, including profiling that produces legal effects concerning the data subject or similarly significantly affects the data subject, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject”[24].

Also, it should be noted that “where data are not processed inside the vehicle but by a telematics provider on behalf of the controller (e.g. the insurance company), the information could usefully mention that, in this case, the provider will not have access to data directly relating to the identity of the driver (such as names, licence plates, etc.). Also, considering the importance of informing data subjects as to the consequences of processing of their personal data and the fact that data subjects should not be taken by surprise by the processing of their personal data, the EDPB recommends that the data subject should be informed of the existence of profiling and the consequences of such profiling even if it does not involve any automated decision-making as referred to in art. 22 of GDPR”[25].

Could the mobility data processed by an insurance company be shared with third parties?

Q 5

Sharing of data with third parties may occur with a commercial partner, a competing insurer or when processing is outsourced subject to a lawfulness basis for such sharing. Motor claims and vehicle ownership data may be shared with consumer reporting agencies, insurers use these reports for underwriting decision making. Drivers' motor vehicle records (MVR) and CLUE reports (in the US) are most commonly requested by insurance companies when determining premium rates. This data is applied in the background while the quotation information is being collected.

In fact, with some agencies[26], a consumer may be able to get a free copy of his/her report upon request if an 'adverse action' notice is received. The consumer has a right to dispute these reports if they are inaccurate or incomplete. Notwithstanding, sharing of driving data with third parties requires thorough assessment of the impact on the data subject. The security of data must be strictly complied with and the processing must have a lawfulness basis as per Article 6 GDPR.

It will be prudent for third parties to have a contract with the owner/driver to describe the purpose of such data sharing. The third party should only receive data that is relevant and necessary to perform the contract. Whether they act as a new data controller or as a data processor, they must comply with all the obligations imposed by GDPR.

When sharing data with a third party, the insurer, with prior consent of the customer, should permit and transmit only the data required by the contract and sufficient information should be provided to the vehicle user on the functioning of the service provided by the third party. Data anonymization where possible and putting the customer in control of how and when data is accessed is of paramount importance. Law and order enforcement authorities, when authorized by law, may be considered as third parties within the meaning of art. 4(10) of GDPR. This would entitle an insurer to provide them with information while subject to compliance with applicable laws and regulations.

What mobility related personal data should not be processed by insurance companies?

Q
6

Data that is not relevant or necessary for processing of an insurance service should not be processed. The insurer should not record or process data that the customer isn't aware of its collection.

Examples include:

- Data that is intrusive in nature, revealing of lifestyle habits or implies undue surveillance of individuals.
- Vehicle geolocation data may in some instances fall under this category.
- Content of messages or calls made by the vehicle driver while driving if the insurance app interacts with the infotainment system.
- Data that could reveal speeding offenses or traffic violations[27].
- Phone unique identifiers, the call logs made or received and list of contacts.
- Video snippets from cameras installed in or on the car.
- Biometric data including face recognition and fingerprint information or this data is necessary should be processed in real time without being ever stored.
- Radio music taste, streamed media content and internet search history.
- Voice commands, WiFi data usage, and movement of occupants.
- Physical, health or mental state of the driver or passengers.

Do these restrictions also apply where the policyholder is a legal entity?

Q7

Restrictions apply in the same manner where the policyholder is a legal entity as drivers can only be individuals, i.e. data subjects. The legal entity, acting as employer or provider of the data subject, will have to ensure that the information about the processing provided by the insurance company as data controller will be appropriately shared with the data subject.

Could an insurance company make the granting of an insurance cover subject to the sharing of personal data?

Q8

Yes, an insurance company may make the granting of an insurance cover subject to the sharing of personal data by the insured (or potential insured) to the insurer.

he insurance sector is structured, basically, by means of analyzing the potential client's risk and calculating the correspondent premium to assess acceptance of the risk. Afterwards, if the risk is considered acceptable, an insurance proposal that reflects the monetary sum at risk as calculated from determined aspects that vary in each case, is issued by the insurer and, if accepted by the potential insured, the insurance policy is formed.

For this process to be concluded and for the risk analysis itself to be done, the sharing of personal data that is necessary for the risk analysis from the potential insured to the insurance company is mandatory.

This does not mean that sensitive data[28], as established by LGPD or "special categories of personal data", as established by GDPR, such as color, race or faith must be shared by the potential insured. On the contrary, an insurance company should not require this data if this is not proven necessary data to assess the risk and thus calculate the insurance premium.

Also, the insurer is only allowed to share the insured's personal data if there is a freely given consent collected in accordance with Article 7, GDPR. Further, according to the same Article 7, GDPR, the data subject shall have the right to withdraw such consent at any time by means that are as easy as and thus, correspondent, to those that required such consent:

"The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent."

However, there is some data that, even if classified as sensitive data, shall be collected by the insurer in order to

(i) In the event that data processing shows that driver displayed dangerous behavior towards third parties, is the insurance company allowed/obliged to inform the competent authorities? (ii) Same question, in the event mobility data show that the vehicle has been stolen or involved in an accident.

Q 9

(i) As expressed in question 8 above and, according to GDPR and LGPD (considering the Brazilian scenario) the insurance company may only share the insured's personal data if a specific consent is freely given by the data owner. The Brazilian Open Insurance regulation (Resolução CNSP 415/2021) classifies the recorded data made by embedded electronic devices connected or used by customers as 'personal insurance data' (dados pessoais de seguros). This specific data may be shared only after prior consent is given by the client and, further, shall be submitted to the confirmation procedure in which the participant data transferor society must request the client the confirmation for the data sharing and inform it (i) which will be the data receptor society; (ii) the term applied to the specific consent given; (iii) the specific data that will be shared[29].

In this sense, it is not likely that the insured may give consent for the insurance company to share his/her data when a (potential) personal dangerous behavior is observed.

Further and, on an international and global perspective, the International Covenant on Civil and Political Rights, which compliance to rules is monitored by the United Nations Human Rights Committee, established on its Article 17 that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[30]

Moreover, the American Convention on Human Rights (Pact of San Jose of Costa Rica), establishes in its Article 11, item 2 that "No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation."[31]

Therefore, even though a driver may have exhibited dangerous behavior towards third parties, the insurance company, as a private entity, is not allowed to inform competent authorities if the specific consent to do so was not previously given by the data owner.

Exceptions to this rule are applicable when the government or any of its divisions (Executive authority, Legislative authority or Judiciary authority, as applicable) request determined data relied on what is authorized by the applicable law. For instance, there may be cases in which data is requested as a matter of proof in a criminal case that analyses a homicide car accident.

(ii) While item (i) foresees an obligation and/or allowance of data sharing by the insurance company without any direct gain for the personal data owner, item (ii) foresees a situation in which the insured may benefit from the previous consent given.

In this sense, the same insured person who has refused to share data for his/her harm may choose to anticipate consent on a free basis to the insurance company to share his/her personal data and/or his/her car mobility data if the vehicle has been stolen or in the event of an accident.

As a matter of fact, geolocation trackers are usually contracted by insured persons within the sole objective of acquiring the insurance company and/or authorities with the car location when in cases of theft/robbery. This specific situation does not require a specific consent from the data user as there is no personal data involved, but only the data related to the car location.

Can an insurer refuse to cover damage in the event were behavioral data show that the driver was unauthorized at the time? Is it possible to use behavioral data to inform the policyholder where an unauthorized person is driving? How should the data post car sale or return of a rental vehicle be treated?

Q 10

In the UK, an insurer for the vehicle at fault will normally be liable for covering the costs to third parties regardless of the driver, so the issue lies with the insurer refusing to cover damage to the insured’s vehicle if there is data available to suggest that the driver was not covered by the policy.

There are many cases in UK law where insurers have used telematics data to determine liability, In the article reference below, Zurich UK were able to determine via a black-box fitted to their insured's vehicle that the point of impact was insufficient to cause the whiplash injuries that the 3rd party attested to and led to the claim being withdrawn[32]. In the second article, telematics data was used in court to support a driver’s version of how the incident occured and ultimately led to a settlement in their favour[33].

In practice both examples referenced indicate how it is expected that aggregated and analyzed data such as driving behaviour would be used. In the cases referenced, telematics provided an indication of liability or fraud and further evidence was collected to substantiate that position.

The driving behavior would unlikely be considered a sole data point for the refusal of cover, but instead it would be an indicator that the claim would require further investigation and therefore further evidence would be requested (dash cam, CCTV, Witnesses, Crash Impact Analysis etc…). There is an ongoing trend to increase the use of external data sources in settling liability in insurance claims and driver behaviour is one such data point[34].

In regards to driving behaviour identification, back in 2016 researchers from the University of Washington and the University of California were able to identify drivers from a test group using only the collected data from a Vehicle’s CAN bus, with a greater than 90% accuracy[35].

This technology has only improved with the proliferation of Machine Learning and Data Science models as well as further advances in the data available from vehicles.

Q
10

So can a driver be identified by driving behavior, the answer is yes.

Can the policyholder be advised that an unauthorized person has driven a vehicle they are responsible for?

Insurers are increasingly extending their involvement in driving from provision of one aspect of legal compliance to drive a vehicle (Uk vehicles must be insured to drive on public roads) to the monitoring and rewarding of driver behaviour via telematic based policies. In theory, with appropriate consent, driver behaviour data could be collected and analysed to “fingerprint” a driver and this could be used as described above to support liability in a claim scenario but would it be beyond the insurer’s remit to advise on car usage by other drivers?

There does not appear to be any test cases or legislation in the UK to support this but given that insurers are able to lower their risk by rewarding or correcting driving behaviour via telematic policies then it is not beyond reason that they would be granted license to further protect the risk by identifying potentially uninsured usage of the vehicle. Pushing the notification back to the insured would be beneficial to the insurer (in the same way that insurers don’t report speeding to the police) as it allows the insured to take corrective action or to correct the notification for example, it could be that a driver with comprehensive insurance on another vehicle had borrowed the car and was legally covered to drive. Driving behaviour data is in a similar vein to Telematics, it provides useful information, it does not provide context.

In regards to using the data post car sale or return of rental vehicle the data collected is personal data if it is linked to a driver. The link between the data and the person that the data relates to would, in the UK, be covered by GDPR and therefore should only be retained and used in accordance with that act unless it has been anonymised for analysis purposes.

In practice, this would mean that the data should be removed from the vehicle post sale or return and could only be stored where it is reasonable to keep the data.

In some cases, analyzing mobility data may lead to unvoluntary discrimination in price determination. What measures should be implemented to avoid this? How will insurers address unintended bias in AI algorithms used for underwriting purposes?

Q 11

First step is understanding the distributions of the training data. This can provide an early indication of bias. One of the main ways to understand if there is unconscious bias is by model explain-ability. Advanced ML models are powerful, but they don't explain why that decision was made by default. Effort is required to engineer explainability into models in order to provide a view on the decision-making progress. If explain-ability is engineered from the start, it becomes easier to uncover patterns of bias.

All models degrade, and if they are not given regular attention, performance suffers. Models are like cars: to ensure quality performance, you need to perform regular maintenance. Model performance depends not just on model construction, but also on data, fine-tuning, regular updates and retraining. A robust model ops process is essential. E.g. deploying drift detectors. A robust model ops process allows a company to systematically identify when models drift and therefore initiate re-training.

Q 12

What transparency measures should be implemented towards the policyholders/the regulator with respect to personalized policy conditions?

Similar to Q11. The key point is model explanation, which requires focused engineering effort. With appropriate explain-ability engineered into models from the start, transparency across personalisation will be achievable.

Q 13

Following an accident, an increase in premium or the termination of a policy by the insurance company may result, what is the probative value of the mobility data?

The answer to this question varies from one country to another. The parties may however contractually agree on specific evidence rules such as granting the in-vehicle data the status of evidence in the event of a claim.

Q 14

Could telematics data be used as evidence in an disputed accident or court case. Does it matter if it is civil or criminal (including infraction) case?

Certain data collected from connected vehicles can infer that a criminal offense has been committed, for example when vehicle speed data is combined with geolocation data to disclose an accident caused by a red traffic light violation.

As already explained in question 5 above, law and order authorities would be considered as third parties when authorized by law. Processing of data for a particular inquiry can only be carried out under the control of the law and order authority (article 10 of GDPR) to investigate a criminal offense or conviction.

Box 2

Legal Precedents

Case 1: Telematics data led to the criminal conviction of a driver in the United Kingdom who was involved in a hit and run accident that resulted in the death of a pedestrian in 2014[36]. Police experts analyzed data from the telematics device Omar Tariq was driving at the time of the accident, which showed that he was speeding—driving more than 20 miles over the posted speed limit[37]. Confronted with that evidence, Tariq pled guilty to causing a death by dangerous driving and was sentenced to more than three years in prison[38].

If the data stream ownership is vested in the owner of the car thus is the property of the owner or lessee, then the owner has the right to prevent a third party from receiving access to that data in reliance on the personal nature of vehicle data. The owner may refuse to provide consent for the data to be used against him in a civil case. For consent to be granted the third party has to transparently state how the data will be used as evidence, the forensic tools that will be used and how it may affect the outcome of the case.

Case 2: Data from a telematics device enabled a driver in the United Kingdom to successfully challenge a speeding charge by contradicting the evidence that allegedly supported it[39]. Police charged Neil Herron with driving 10 miles over the posted speed limit[40]. Herron insisted that he had not been speeding[41]. At the time of the alleged speeding incident, Herron had been conducting a trial of a telematics device in his car[42]. The data from that device enabled Herron to prove that the car had been traveling far below the speed limit, as he had claimed[43].

Box 2

Legal Precedents

Case 3: GPS data is also used as evidence in civil cases, such as the wrongful termination action brought by a cable company employee against his former employer, Pacific Bell Telephone Company[44]. Pacific Bell terminated Blake Smith's employment after an investigation into the theft of his work truck led the company to conclude that Smith had failed to safeguard company property and that he had lied during the investigation into the theft[45] . Smith claimed he parked the truck, took the keys out of the ignition, and locked the truck[46] .

A significant factor in Pacific Bell's determination that Smith was lying was the data obtained from the GPS technology in the truck, which revealed that the truck was idling when it was stolen[47] . In an affidavit filed in support of its motion for summary judgment, Pacific Bell explained that the GPS technology in its trucks generates a report in a Microsoft Excel spreadsheet that records various data, including the time and location of every vehicle, each time the ignition is turned on or off, the time and location of the vehicle every seven seconds, and the time and location of the vehicle every one mile it is driven[48].
The Court ultimately granted Pacific Bell's motion for summary judgment. In France, an Ordonnance n° 2021-442 dated 14 April 2021 introduced some new rules on the access to vehicles data.

In accordance with Article L-1514-5 of the Transports Code introduced by this Ordonnance, in the event of a traffic accident, the following companies are granted access to the data held in the system recording the driving delegation status with respect to the activation, de-activation or the control recovery of the automated driving system:

Box 2

Legal Precedents

“insurance companies that are insuring vehicles involved in the accident, in order to determine the indemnification necessary to perform an insurance contract, exclusively in the event such data processing is necessary to perform the relevant insurance contract.”

This access might be subject to the acceptance of the financial conditions, which may only cover the costs of collection and transmission of the data related to the characterisation of the activation status of the driving delegation.

The consent of the data subject - driver or user of one of the vehicles involved - to the data processing is not necessary for the above mentioned purposes.

The scope of data transmitted is limited to what is strictly necessary to determine the activation or not of the vehicle driving delegation, or the control recovery, in order to indemnify victims in accordance with the Law n° 85-677 dated 5 July 1985.

The EU's Proposed Data Act

On February 23rd, 2022, the European Commission published a proposal on harmonised rules for fair access to and use of data (the Data Act). The proposal further empowers consumers and businesses' right to access, share and port their data, irrespective of its personal nature to third parties. It does so at several important levels:

1- It complements the data portability right afforded by the GDPR to include all data generated by the consumer out of the use of a connected product or related service whether it is purchased, rented or leased.

2- clarifies that the sui generis database right created by the Database Directive does not apply nor interfere with the rights of users to access data generated by their use of a product or related service.

3- forces data holders to make available upon the request of the user or a party acting on behalf of user (within the EU), all data and metadata generated by the user while using the product or service, through a simple and secure digital interface, without delay, continuously, in real time, of the same quality as is available to the data holder and free of charge to the user.

4- covers any physical components such as IoT sensors, digital personal assistants, motor vehicles, consumer goods, smart industrial machinery, medical devices and any connected product and related service connected to a publicly available electronic communications network.

5- highlights a need for harmonized and interoperable data standards for data to be reused across different sectors.

6- tries to avoid undermining the investment incentives for the product from which data is obtained by its use to develop competing products.

7- allows the data holder to set a reasonable compensation to be paid by third parties for the cost incurred in providing direct access to the data generated by using the product.

The proposal inter alia addresses the need for new rules "to ensure that existing vehicle type-approval legislation is fit for the digital age and promotes the development of clean, connected and automated vehicles. Building on the Data Act as a framework for the access and use of data, these rules will address sector-specific challenges, including access to vehicle functions and resources"[49].

OPIN's views on the proposed Data Act

The sui generis database right is independent of copyrights and provides the database maker protection if a substantial investment was involved in the obtaining, verification and presentation of the contents. The proposed Data Act clarifies that a database containing data generated by the use of a product or related service does not apply, therefore allowing the data subject to access, use and share their data.

The Data Act provides significant protection to micro and small businesses (as long as they are not an entity of a larger group of companies) excluding them from the requirement to provide third parties with shared access to user data. Moreover, the Act takes a bold step in preventing and excluding core platform services (gatekeepers) from receiving direct or indirect access to data of users generated by use of other products or related services. It also prevents gatekeepers from combining certain data without consent.

Unless the data generated by a user is available on a remote server, product designers and manufacturers will be expected to configure and perhaps reconfigure in-production products to be able to provide their users with the data they generated. This may be achieved by implementing a user interface on the device or by developing an accompanying mobile app to manage granting and withdrawal of access permissions with granular options.

Manufacturers will be required to explain to users how the data may be accessed prior to the conclusion of a purchase, lease or rent. Notwithstanding, the Act allows for manufacturers to enable edge computing of the data on device or on a computing instance. OPIN finds the provisions that stipulate simple request mechanisms for automated access without requiring examination or clearance by the data holder as significantly progressing for the concept of user data access and portability.

Data can be obtained by almost any third party and not necessarily by similar or an adjacent product domain, this removes the need for whitelisting directories and allows for cross product innovation, but, personal data can only be requested by the data subject or the data controller. Research, think tanks and not-for-profit organizations will benefit from receiving access to data for scientific and social innovation purposes.

A restriction however applies as the relevant third party shall not use "the data it receives to develop a product that competes with the product from which the accessed data originate or share the data with another third party for that purpose"[50]. OPIN considers the concept of "competing product" quite broad and is encouraging to strictly define this concept (e.g. direct competition only) in order to avoid legal uncertainty.

The introduction of and allowing for compensation to be demanded by data controllers for providing access to third parties to the data generated by users is somewhat contrary to the spirit of the Act and is inconsistent with its effort to support startups. Introducing compensation could directly impact the ability of micro and small businesses to take part effectively in the data economy if we consider that many startups start out in life in bootstrapped mode.

Although the Act sets out to define the manner at which compensation is calculated, it fails to set clear measures or benchmarks to ensure fairness and transparency from the outset. Alternative means of resolving domestic and cross border disputes through dispute settlement bodies and courts of tribunal will add an additional barrier for small market entrants.

While compensation will provide small businesses with the means to comply with the Act, it nonetheless appears to reward large businesses at the same time. Large businesses may have better and larger resources for processing raw data to produce what may be valuable derived data thereby introducing an incentive to make such data more valuable than the raw data itself.

Finally, for clarity and legal certainty purposes, OPIN considers necessary that the proposed ePrivacy Regulation is adopted before the Data Act adoption in the EU.

The OPIN and COVESA data alignment project sets an example for cross sector standards-interoperability

The data alignment project initiated between The Open Insurance Think Tank (OPIN) and the Connected Vehicle Systems Alliance (COVESA) was started in January of 2021 and over a period of almost 13 months the teams working on the project succeeded in harmonizing their relevant data standards for the benefit of the users and the global insurance and automotive industries.

OPIN's community of participants, as can be witnessed by the work presented herein and the related published documents, displayed a tri-pronged approach combining; the creation of data and API specifications, legal and regulatory examination and POC technical implementation. It is a ready example of how cross sectoral interoperability can be achieved.

The proposed Data Act **adds legal and regulatory support for OPIN's efforts** to promote the concept of shared access to data and its continuing efforts to introduce interoperability between insurance and other connected product domains.

REFERENCES

EDPB	European Data Protection Board.
ePrivacy Directive	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. This Directive might be replaced by an ePrivacy Regulation which proposal was adopted by the Commission adopted in 2017. The negotiations are still ongoing.
GDPR	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.
LGPD	General Personal Data Protection Law, which is the law in Brazil of 14 August 2018 that regulates personal data with regard to processing and movement of such data.
OEM	Original Equipment Manufacturer
SUSEP	Superintendência de Seguros Privados, which is the Brazilian regulator for the insurance, private pension and capitalization sectors.

REFERENCES

[1] The debate on Open Insurance", 15.06.2021

[2] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

[3] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act).

[4] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act).

[5] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

[6] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

[7] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.

[8] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en.

[9] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU, COM(2020) 591 final.

[10] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3763.

[11] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3763.

[12] Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (public consultation), https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en.

[13] Guidelines 01/2021 on Examples regarding Personal Data Breach Notification (adopted), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en.

[14] "*Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service*".

[15] Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0., adopted on 9 March 2021, §§107-108.

[16] Please note that the embedded finance part of this use case is not addressed in this table as it is our understanding that the related processing of personal data is performed by the payment service provider, acting as data controller and not by the insurance company nor the EOM.

[17] Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0., adopted on 9 March 2021, §109 and French Data Protection Authority (CNIL), Compliance Package, Connected Vehicles and Personal Data, October 2017, p. 25 .

[18] Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0., adopted on 9 March 2021, §§110 - 112.

[19] Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0., adopted on 9 March 2021, §113.

[20] Client means any natural or legal person interested in acquiring insurance, capitalization or open supplementary pension products, as well as the applicant, the insured, the guaranteed person, the borrower, the beneficiary, the assisted person, the holder or subscriber of a capitalization certificate or the participant of pension plan *(Resolução CNSP 415/2021).*

[21] Available at https://openinsurance.susep.gov.br/documentos-de-referencia/.

[22] Open Data Related to Insurance and Personal Insurance Data are defined by Resolução CNSP SUSEP 415/2021 (article 2, XII and article 2, XIV). Available at https://www.in.gov.br/web/dou/-/resolucao-cnsp-n-415-de-20-de-julho-de-2021-333272165.

REFERENCES

[23] Available at http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

[24] Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0., adopted on 9 March 2021, §84.

[25] Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0., adopted on 9 March 2021, §115.

[26] Adverse Action Notice Requirements Under the ECOA and the FCRA

[27] EDPB

[28] LGPD classifies the sensitive data as "personal data on racial or ethnic origin, religious conviction, political opinion, membership of a trade union or organization of a religious, philosophical or political nature, data relating to health or sex life, genetic or biometric data, when linked to a natural person". This data shall be compared with the special categories of personal data as defined by Article 9, GDPR.

[29] Article 22, *Resolução* CNSP 415/2021.

[30] Article 17, Covenant on Civil and Political Rights.

[31] Article 11, item 2, American Convention on Human Rights.

[32] https://www.insurancebusinessmag.com/uk/news/commercial-vehicles/three-motor-claims-that-prove-telematics-is-a-must-228965.aspx

[33] https://www.pinsentmasons.com/out-law/news/telematics-data-used-to-defend-against-claims-of-liability-in-uk-first-says-insurer

[34] https://www.postonline.co.uk/market-access/motor/7921471/spotlight-motor-trends-the-use-of-data-in-claims-and-underwriting

[35] https://www.schneier.com/blog/archives/2016/05/identifying_peo_7.html

[36] *Telematics Data Helps Jail Courtesy Car Driver for Hit and Run Collision*, FleetNews (Jan. 26, 2016), http://www.fleetnews.co.uk/news/fleet-industry-news/2016/01/26/telematics-data-helps-jail-courtesy-car-driver-for-hit-and-run-collision, *archived at* https://perma.cc/THN5-SVKM.

[37] *See id.*

[38] *See id.*

[39] *Telematics Successfully Used to Overturn Speeding Prosecution*, FleetNews (Feb. 10, 2015), http://www.fleetnews.co.uk/news/manufacturer-news/2015/10/01/telematics-successfully-used-to-overturn-speeding-prosecution, *archived at* https://perma.cc/38XF-5NKS.

[40] *See id.*

[41] *See id.*

[42] *See id.*

[43] *Driver Wins Speeding Case Through Telematics*, The Driving Instructor Leicester (Oct. 5, 2015), http://www.the-driving-instructor-leicester.co.uk/Blog/uncategorized/driver-wins-speeding-case-through-telematics/, *archived at* https://perma.cc/YFW8-YKM9; *see also supra* note 23.

[44] Smith v. Pac. Bell Tel. Co., 649 F.Supp.2d 1073, 1076 (E.D. Ca. 2009).

[45] *See id.* at 1079–80.

[46]*See id.* at 1078.

[47] *See id.* at 1079–80.

[48] *See id.* at 1078.

[49] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), page 5.

[50] Article 6 (2) (e) of proposed Data Act.

ABOUT THE AUTHORS

Andrea Maura (Italy)
Partner at Aliant Legal Grounds

Andrea provides legal assistance to Italian and foreign insurance companies and insurance and financial intermediaries, mainly supporting them in preparing pre-contractual and contractual documentation, distribution structures, collaboration agreements, compliance with IVASS regulations, AML and data protection matters.

Andrea is a member of the Italian Insurtech Association, a member of OPIN (Open Insurance) Italy Working Group and a member of the faculty of CINEAS, a non-profit university consortium founded by the Politecnico di Milano (management training school in risk management and loss adjusting).

Andrea also has to his credit three monographs on Motor TPL and D&O insurance and numerous collaborations in collective works, where he dealt, among other things, with insurance contracts and insurance brokerage.

Anne-Sophie Morvan (Luxembourg)
Business Development Manager at LUXHUB

Anne-Sophie Morvan is Business Development Manager at LUXHUB, an Open Finance Fintech. After having worked several years as a solicitor at different law firms in the field of data protection, IT contracts, payment services and e-commerce, Anne-Sophie changed her career path and took up a business position at LUXHUB in 2019. Nonetheless, Anne-Sophie is still very involved on regulatory matters and is for instance representing OPIN within the Expert group on European financial data space, which is providing advice and expertise to DG Financial Stability and Capital Markets Union (FISMA).

Anne-Sophie holds a Master degree in E-Commerce and Digital Economy Law from the University Paris I-Panthéon Sorbonne and a LL.M. in German law from the Ludwig-Maximilian-University of Munich. Anne-Sophie was admitted to the Paris Bar in 2014 and to the Luxembourg Bar in 2015.

ABOUT THE AUTHORS

Carolina Samea (Brazil)
Lawyer at Mattos Filho Advogados
focused on the insurance, reinsurance and private pension area. Post graduated in Contract Law (FGV-SP).

Within the insurance field, she is actively involved in Open Finance, specially in Open Insurance discussions in Brazil.

She is a member of the Institute of Innovation in Insurance and Reinsurance of Fundação Getúlio Vargas – FGV.

Fouad Husseini (UK)
Director at The Open Insurance Think Tank (OPIN)
An insurance transformation consultant with a successful career in insurance and reinsurance. Fouad is founder at OPIN and spearheads the development of data standards and open APIs. He is an expert at the United Nations/ Centre for Trade Facilitation and Electronic Business and contributes to the development of global electronic trade standards. His recent achievements include being a finalist at the Insurance Nexus Innovation Awards 2018.

He is a graduate in Aeronautical Engineering, a Fellow of The Chartered Insurance Institute (FCII) and a frequent speaker and writer. His most recent major work includes writing and publishing the textbook "The Insurance Field Book".

ABOUT THE AUTHORS

Martin Dennehy (UK)
Chief Enterprise Architect at Covea
Martin Dennehy is the Chief Enterprise Architect for Covea, a UK general insurer. Martin has over 25 years experience in IT with 18 years experience in Solution, Business and Enterprise Architecture working across the Government and Financial Services sectors. Martin has been supporting OPIN Mobility Group in the production of design materials to support connected vehicles and insurers. Martin Holds a BSC Honors Degree In Computing with Business and is certified in Technical Architecture, Infrastructure and Design by the British Computer Society.

Cassio Gama Amaral (Brazil)
Partner at Mattos Filho Advogados
A PHD candidate at Nova School of Law (Portugal). LLM from the Lyon International Business School - EM-Lyon, and MBA (stricto sensu) from the Federal University of Bahia (UFBA). He has experience in the Insurance, reinsurance, infrastructure industries and pensions, advising clients on regulatory and (re)insurance transactions. He is actively involved in claims and complex (re)insurance and infrastructure disputes in Brazil. He is a lato sensu postgraduate Professor at the Brazilian National Insurance School (Escola Nacional de Seguros) and the Brazilian Superior School of Lawyers – São Paulo Bar Association (Escola Superior de Advocacia – OAB-SP), in addition to being the author of several publications on (re)insurance and pensions Law. He is a member of the Institute of Innovation in Insurance and Reinsurance of Fundação Getúlio Vargas – FGV, the International Insurance Law Association (AIDA), the Insurance and Reinsurance Commission of the São Paulo Bar Association, the Legal Comission of ABRAPP, the Insurance, Mediation, and Litigation Committees of the International Bar Association (IBA) and Legal, Financing and Guarantees Committees of ABDIB.

ABOUT OPIN

As a think tank we are working on solving many of the challenges that insurance companies and their partners come across.

At OPIN, different innovation labs interact with each other on projects to produce coordinated and well studied output. The Mobility, Legal & Regulatory and Blockchain labs are OPIN's research hubs.

Within the Mobility Lab, corporate members and researchers work together on cross-ecosystem standards, the creation of new customer journeys and the exploration of insurer and OEM connectivity.

www.openinsurance.io

Open Insurance