**AVIVA RESPONSE TO EDPB CONSULTATION ON DRAFT GUIDELINES ON THE PROCESSING OF PERSONAL DATA IN THE CONTEXT OF CONNECTED VEHICLES AND MOBILITY RELATED APPLICATIONS**

Aviva welcomes the opportunity to provide feedback on the EDPB's Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications (version 1.0).

Aviva is an international savings, retirement and insurance business. We serve 33.4 million customers in the UK, continental Europe and globally.

We have contributed to the ABI's response to the guidelines and fully support their submission. We would like to take the opportunity to set out some additional points that we believe warrant further attention.

We fully support the ambition that underpins the guidelines, which seek to ensure that the protection of customer data is paramount during the use of telematic technology. However, we do not believe that the proposed approach adequately recognises the nature of insurance applications and finds the correct balance between consumer protection and access to the best quality products built on advanced and secure technology. In particular:

- Further clarity is required on the legal basis under GDPR and the interaction with consent required under the ePrivacy directive.

- The proposals for geo-locational data, in particular the restriction to limit access to continuous data, are not compatible with usage-based insurance applications. These proposals would limit the potential for European consumers to benefit from existing usage-based insurance products and technological developments in telematic products.

- If adopted, the proposals on the processing of raw data would put the provision of existing telematics products at significant risk and substantially undermine the development of future connected vehicle-based propositions. It would limit the scope of insurers to apply their analysis and expertise to raw data to create the best products and stifle any competitive element in the market. Affordable motor insurance solutions for young drivers would inevitably be affected. We therefore, strongly disagree with the proposed approaches outlined in this section.

We fully support the intentions of the EDPB Guidelines n respect of data privacy in the emerging connected vehicle world. However, we believe that the Guidelines have been created to cover several potential use cases for data use, as well as insurance. This generalised approach, and the recommendations proposed will lead to some negative outcomes for a high number of insurance customers including young drivers.

**We would recommend that the EDPB engage directly with the insurance industry to better understand the technical details of usage-based insurance and supporting propositions to ensure customers today are not disadvantaged by these Guidelines. We would welcome the opportunity to discuss these issues in greater detail.**

**In addition, this engagement would give the EDPB an opportunity to gain insight as to how we (the insurance industry) see the widescale emergence of connected vehicle insurance benefitting customers in new and innovative ways that meet their individual needs and circumstances.**

1. **Use of the legal basis in Article 6.1(b) GDPR to process data for usage-based insurance.**

   Aviva believes further expansion in the Guidelines is needed in relation to the following points:

   - **Paras 105 – 106** provide that Article 6.1(b) can be relied on as the legal basis for the *processing* of data which is *necessary* for the provision of the telematics insurance contract, but it also appears to require consent under 5(3) ePrivacy Directive to *access* the data from the end-user's terminal equipment/electronic communication network. Our understanding therefore is that there is a requirement for ePrivacy consent *in addition to* the GDPR legal basis under article 6.1(b) in relation to telematics insurance products. However, we believe the Guidance could be clearer on this point. We also feel that this distinction is helpful to insurers who historically may have been relying solely on consent in these circumstances for both ePrivacy and GDPR purposes. This is problematic as it is difficult to show a valid GDPR consent when the provision of a service is conditional on that consent. However, further guidance on obtaining valid consent, given that this would be conditional consent, would be useful.

   - For collection of data from the connected vehicle which is over and above that which is strictly necessary for the telematics insurance contract (for example data collected for analytical purposes to build insurance pricing algorithms or for fraud prevention purposes), we believe Article 6.1(b) is unlikely to be available and another legal basis would therefore be required. This is not addressed in the Guidelines, but instead the Guidelines suggest such further data should not be obtained by insurers. The Guidelines should acknowledge that data can be processed where a legal basis under GDPR exists, and also subject to any necessary ePrivacy consent being obtained where applicable.

   - **Para 106** appears to assume that in order to rely on Article 6.1(b) the insurer will ultimately always enter into a contract with the data subject. Clarity is needed where data is used, for example, to provide an insurance renewal quote where a contract is not ultimately taken up. Confirmation would be appreciated that Article 6.1(b) is still available here, on the basis this is done 'in order to take steps at the request of the data subject prior to entering into a contract'.

   - **Para 46** highlights that consent should be separately obtained from all drivers/users to process their data. When processing the data however, it is unlikely the insurer will be able to identify third parties driving the car for any particular journey unless they are told, for example as a result of a claim. Furthermore, there are potential difficulties in obtaining consent as there is usually no direct contact with a named/occasional driver and the telematics insurer by which to obtain this consent. Generally, insurers will only know that the data relates to the vehicle which is directly linked to the policyholder of the insurance contract. Further guidance is therefore requested on this area.

**2 Geolocation data – paragraphs 60 and 61**

We note the EDPB's concerns in respect of geo-locational data, but we do not feel the approach is compatible with insurance applications.

We feel strongly that access to continuous geo-locational data is critical for usage-based insurance applications to perform and to deliver real value to customers. Specifically, continuous geo-locational data is needed for the following reasons:

- **To validate speed vs speed limits on specific road segments** – this is a key component of risk assessment and without it, insurer pricing models for user-based insurance are severely weakened

- **Customer feedback** – this is key to behavioural change. Being able to demonstrate specific events at specific times and locations (road name/number) enable customers to better understand their driving behaviour and how they can improve their own safety

- **Claims validation and investigation** - geo-location data allows claims handlers to achieve better claims outcomes by providing environmental context to the verbal description of events. Often, this can help build an accurate picture of the events leading to an accident and improve decision-making in areas such as liability.

- **Fraud detection** – geo-locational data can be used to detect fraud. For example, where a false address is given in order to reduce premiums, geo-locational data can be used to prove the 'kept address' is in fact false and therefore fraudulent

- **Accident detection** – future propositions may include accident detection and response. Geo-locational information will be required to identify where the vehicle is, for the insurer to respond by, for example, calling emergency services or for vehicle recovery

Aviva go to great lengths to ensure we protect the personal data of our customers and we always ensure that any profiling is carried out with the specific objective of determining driving risk behaviour and not for any other purpose, for example, religion or sexual orientation derived from places visited.

In addition, and in line with GDPR requirements, we ensure we have the necessary permissions from customers and a legal basis for accessing and processing their personal data.

**3 Paragraph 74**

We have the following comments on the recommendations in paragraph 74: -

**Only data strictly necessary for the vehicle functioning are processed by default and data subjects should be able to activate/deactivate the data processing for each other purpose**

- This assumes that telematics products will only use data items strictly necessary for the vehicle functioning in the telematics product and pricing. Telematics insurance may use data items that do not solely relate to the functioning of the vehicle such as time of day, location (as discussed elsewhere) and other data items available from the vehicle where these factors are indicative of insurance risk. If new telematics propositions are developed which use other data elements, because analytics show they are significant indicators of risk, these would become product critical and the product could no longer be provided if those elements were deactivated by the data subject. We would suggest that data *necessary for the telematics contract* should be used by default and that data subject would have control over wider data elements as appropriate.

**Data should not be transmitted to third parties**

- Further guidance is requested on this point. For example, it may be necessary for the performance of a contract to share telematics data with a third-party service provider.

**Data should be retained only for as long as necessary for the provision of the service**

- We agree where the data is processed under Article 6.1(b), and this will include a time period to service claims and deal with legal disputes under the contract.

**Data subjects should be able to delete data when vehicle is put up for sale**

- We agree that the data should no longer be used for telematics propositions in relation to the vehicle, however if the data is anonymised or pseudonymised for other purposes, provided there is a legal basis and adequate transparency, this should not be restricted by this recommendation. We have answered this on the assumption that the guidance refers to data stored in the vehicle or transferred elsewhere for processing. Further clarity is requested as to whether our assumption is correct.

**Data subjects should where feasible, have direct access to data generated by these applications**

- Currently this would be available from the insurer under a data subject access request. We would appreciate further guidance on what is meant by 'direct access' and 'data' in this context. For example, does the direct access go further than the customers' DSAR rights?

**4 Data collection - paragraph 108**

We acknowledge the intentions of the EDPB in respect of mitigating the risks of creating a precise profile of an individual's movements, however, we again feel strongly that the recommendations made in the Guidelines are not in consumers' best interests from an insurance point of view:

**….raw data regarding driving behaviour must either be processed :**

**Recommendation 1: inside the vehicle in telematics boxes or in the user's smartphone so that the insurer only accesses the results data not detailed raw data**

- Telematics devices do not have the capability to host the complex algorithms and databases required for usage-based insurance. These functions can only be performed 'off device' using the raw data collected by either the connected car or telematics device

**Recommendation 2 : 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. This means that the telematics service provider receives the real-time data, but does not know the names, licence plates, etc. of the policy holders. On the other hand, the insurer knows the names of policyholders, but only receives the scores and the total kilometres and not the raw data used to produce such scores.**

- Usage-based insurance risk and pricing models depend on insurers having on-going direct access to driving data which enables IP development and facilitates the creation of an individual's insurance risk profile.

- Using aggregated basic manoeuvre scores from a thirrd party would significantly weaken insurers' pricing capabilities and would probably lead to market distortion where all insurers pursue the same customer risk segments e.g. scores 7-10/10 only.

- We feel strongly that this could lead to an anti-competitive insurance market where all insurers have the same pre-defined (by a third party) view of risk. This could lead to significant customer pricing detriment, and even large parts of the market (e.g. sub 7/10 scores) being excluded or priced out of the market.

- It may restrict the development of new data-driven propositions, which meet individual customer needs more closely than traditional generic propositions, for example, providing more affordable solutions to young drivers. We see that there is a key opportunity to use connected car data to inform innovative proposition development to address specific or emerging customer needs that otherwise may not be met. This could also relate to current and future vehicle usage such as car sharing, enabling the blurring of personal and commercial risks via the sharing economy, or even the support of climate change initiatives or specialist driver needs.

**5. Additional comments**

We have the following comments on the paper:

- **Para 91 -** security and separation from a vehicle's vital functions (and risk of cyber interference) is of significant interest to insurers. The proposals in para 91 directed at manufacturers are therefore fully supported.

- **Para 103** - the assumption that the driver would need to 'install a built-in telematics service' is incorrect as connected vehicles could automatically collect the data needed.

- **Para 104** - we would request further guidance on the assertion that pay as you drive insurance should always be optional. Is this intended to mean that data subjects who own connected vehicles must not be required to purchase a pay as you drive policy, or is it intended to provide that insurers are always expected to offer a standard insurance policy where usage-based insurance is offered to specific customer groups? Different insurers have different risk appetites and may not, for example, wish to insure young drivers. By offering usage-based insurance such drivers can access affordable motor insurance where non usage-based insurance may not be available to them.

- **Claim data**

    - Access to data held in connected vehicles where the vehicle is also driving in autonomous mode (or has the capability to do so) is an important concern for insurers, to ensure they have access to sufficient data to assess liability under the Automated and Electric Vehicles Act 2018 in the event of a claim. The Guidance does not address that point and we feel this is a missed opportunity to provide guidance as to what data should be accessible as well as the privacy implications of such data access and use.

    - Another challenge facing insurers is the existence of personal data held electronically within a vehicle which remain in the vehicle when it is sold by a customer to their insurer (transfer of salvage rights/title as part of a total loss settlement). This is touched on in para 87 (requirement of a right to erase personal data) and para 89 (deletion of personal data on sale/change of ownership) and paras 170-176 (e-data being left in rental vehicles potentially accessible by the next customer). This has certain parallels to the salvage issue, to the extent that before taking ownership we would want the customer to be able to delete such data. We therefore agree with the proposal at para 175 that the manufacturers should provide standard functionality for deletion of in-car data.

**Jon Marsh – Personal Lines Category Director**
**AVIVA – 19 March 2020**