EDPB Draft Guidelines on the Processing of Personal Data in the Context of Connected Vehicles

Introduction

RSA Insurance Group PLC ("RSA") is a UK domiciled global insurance business. We serve circa 9,000,000 people in over 100 countries and have a significant footprint in the UK, Ireland, Scandinavia and Western Europe. RSA provides general insurance products to consumers and commercial entities and has several connected insurance and telematics insurance products which are sold to the market.

We are pleased to be able to respond to your call for views on your draft Guidelines on the Processing of Personal Data in the Context of Connected Vehicles.

The Call for views

Connected insurance and telematics is a key consumer insurance product offered by insurance companies throughout Europe, including RSA. The provision of these general insurance products are paramount to both the UK's and the EU's ambition to make the UK and Europe the centre of connected vehicle and device development which is seen as being key to attracting investment in our collective culture, work forces and national infrastructures and is of considerable benefit to consumers.

The draft guidance is intended to apply to all connected vehicles determining those on board and added systems as terminal devices. The guidance identifies telematics insurance as being a key example of the need for this guidance and we hope that this response assists those drafting the guidance in their understanding of how connected and telematics insurance products work in practice.

Connected insurance and telematics insurance policies are an active conscious choice of a consumer. They are generally purchased by consumers considered to be a higher risk, young drivers for example and the provision of the data to which this guidance applies is a fundamental requirement of these policies, without which they cannot operate.

This note sets out our views on elements of the draft guidance to aid the EDPB in its consideration of the wording of its guidance paper.

Legal Basis (paragraphs 105 and 106)

Paragraph 105 confirms that Consent will be required to access the data already held on the vehicle systems, but paragraph 106 states that "performance of a contract" would be sufficient for accessing data on the telematics boxes installed onto the vehicle. There remains the key question as to which legal basis should apply to those vehicles which have a telematics box already installed by the vehicle manufacturer as a part of the vehicles own onboard systems. For example, the future design plans of Original Equipment Manufacturers are to fit a telematics box which can then be accessed by different insurers as the insurance provision moves from provider to provider. It is not clear whether this means that Consent would be required as opposed to "performance of a contract" to access data held on the device prior to Insurer B taking over from insurer A and how that works with the principle of data portability as set out in the GDPR.

There are further considerations in respect of how this will fit with the right of the data subject to turn off the geolocation device in the black box, this seems to operate outside of the "performance of a contract" legal basis and it is suggested in the draft guidance that this should be an absolute right for the data subject.

On the basis that connected and telematics insurance products are a conscious choice for the consumer, if "performance of a contract" is not available as suggested by the draft guidance and

"consent" is the only legal basis for processing data already present on connected devices, this could have serious ramifications on the operation of a product of insurance that is entirely reliant on the data collected by these connected devices. Such action could see insurers withdraw from this type of product, lead to consumer detriment, and impact efforts to innovate in the connected device space.

We would recommend that the guidance is amended to confirm that the legal basis of processing in the context of connected and telematics insurance products is "performance of a contract" and that this extends to all of the data necessary for the processing, administration, and administration of the product of insurance and includes relevant data wherever and whenever it was stored.

Data Collected (paragraph 108)

RSA are concerned with Paragraph 108 which states that usage data would be split into 2 types, raw data and aggregated data. It is recommended in the draft guidance that insurers do not have direct access to the raw data due to the potential to profile data subjects from their geolocation data. This could clearly be an issue for insurers writing telematics businesses, especially those which do not rely on a telematics provider to assess the data collected from the telematics devices. The suggestion that the telematics providers should provide insurers with a score instead of the raw data is unlikely to work in practice as many insurers collect raw data themselves and rely on their own algorithms to identify relevant driving behaviour.

In addition, insurers will also use geolocation data in the event of a vehicle theft and locating the vehicle. This is covered by consent of course, however, geolocation data is also used as part of an insurer's fraud investigations either at claims stage, or when considering application fraud, for example, checking that a vehicle is kept where the policyholder said it would be kept when they presented the risk at inception. This guidance would in effect prohibit this wider use and would frustrate fraud investigations and an insurer's regulatory obligation to fight fraud and economic crime.

Retention Period (paragraph 110)

It should be noted that for commercial and transactional data (not usage data) it is recommended that data is retained for no longer than the statutory limitation period. In the UK, statutory limitation is set out in the Limitation Act 1980 which provides a general period for tortious matters of 6 years, adding 4 months to cater for those instances where claimants issue on the eve of limitation and who acquire a further 4 months in which to serve those proceedings.

Whilst limitation is a useful comparator when considering the retention period, when it comes to products of insurance, longer retention periods are applied in the event that a customer renews a policy as that data is required for the continued pricing of the product of insurance for that individual customer.

We would therefore suggest that aligning retention to limitation is unhelpful and instead, the EDPB should pin retention to the principles of the GDPR where controllers are encouraged to develop clear and documented thought processes in respect of their retention periods balancing the minimisation principle with the need to maintain data to provide services and products to the individual data subject concerned.

Information and rights of data subjects (paragraph 112)

There is an inference within the guidance that there should be a telematics "privacy notice" which provides data subjects with specific information on their telematic data. This could seem somewhat

excessive and most insurers will already provide a general privacy notice as well as additional terms and conditions to those acquiring telematic insurance.

Geolocation data (paragraphs 60 & 61)

Paragraph 60 states that the controller shall be particularly vigilant not to collect geolocation data except if doing so is absolutely necessary for the purpose of the processing. With telematics, it may not always be necessary to **process** geolocation data, but it will be **collected** and used where appropriate in the event of an enquiry relating to an accident or a theft, or for application fraud purposes. It is also used in addition to the accelerometer to provide a rich picture of how the car is being driven and multiple data sources helps ensure accuracy and is used for investigating any potential faults.

Paragraph 61 sets out proposed principles requiring compliance on geolocation data which include an ability of the data subject to turn off geolocation data. This would hinder the underwriting, administration, and operation of a telematics insurance product which is entirely reliant on the relevant data collected from the connected device.

We would refer to our comments that these products of insurance are specifically chosen by consumers who wish to have this type of product. The ability to turn off geolocation data could put the consumer in a position of breach in respect of their contract with their insurer which could have financial consequences.

We would recommend that thought is given to this point and the unintended consequences that may well follow the provision of such an ability.

Criminal offences (paragraphs 64 & 65)

The guidance suggests that connected devices can collect data which could suggest that a user has broken the law. It is suggested that processing of this information must only be carried out under control and the authority of an official authority within the Member State. However, connected vehicles and telematics devices regularly collect data on the speed driven versus the speed limit on roads as well as driving style. This is a fundamental element of connected and telematics based insurance products.

If this guidance is issued as currently drafted, it could erode the ability of insurers to provide such insurance and remove the accessibility of telematics insurance for consumers.

We would suggest that this guidance is expanded to allow insurers to process that data for the purposes of a connected and telematics insurance policy.

Ancillary issues

Paragraph 28 uses the phrase “data that can be associated with a natural person.” This is potentially an extension of the principle of what constitutes a data subject, which at the very least could be confusing. Data associated with a natural person could include data which is not expressly or indirectly about them. We would recommend that the definition of personal data is restricted in scope to that set out in Article 4 of the GDPR:

“any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more

factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Paragraph 37 defines the data subject for the purpose of these guidelines as including the passenger of a vehicle. We would question how a passenger's consent would be obtained in the context of connected and telematics insurance and would question whether this is workable. We would recommend that reference to the passenger is removed.

Paragraph 74 gives the data subject control over how their data is used, including a requirement for information regarding the processing to be provided in the driver's language, provide users with an ability to turn on or off certain processing activities, restrict data transfer to third parties, restrict data retention, and allow the data subject to permanently delete their personal data prior to the sale of the vehicle, as well as giving them direct access to the data. There are also references to car hire companies installing technology where users can delete their data at the press of a button. These guidelines appear to be largely impractical and we recommend that the EDPB give further consideration as to how this would actually work in practice as well as consideration of the costs of implementation and the impact on normal commercial operations as a result.

Paragraphs 81 and 82 require a data controller to provide a privacy notice to all data subjects, this could be somewhat cumbersome with multiple data controllers providing services to vehicles and data subjects, not necessarily just from the insurance sector. This links into paragraph 83 which requires any data controller picking up a vehicle crossing their jurisdictional border to provide privacy notices too. Whilst the rights of data subjects must be protected, this must be proportionate and practical, taking into account the realities of commercial interactions.

Conclusion

RSA fully support the protection of the privacy and rights of data subjects. Indeed, protecting the data of its customers is one of RSA's core principles.

We are of the view that the draft guidelines do not fully take into account how connected and telematics insurance products work in practice and whilst we do not believe that this is the intention of EDPB, if published in their current form, the guidelines could frustrate the administration of such insurance products making them unworkable from a practical perspective. The unintended consequences of such could see such products removed from the market which would reduce consumer choice, block higher risk consumers from accessing insurance at a reasonable price, and could hamper the further development of connected devices.

We would be grateful if the EDPB would give further considerations as to how their guidance could impact all those that it regulates, and in particular the insurance sector.

We would recommend the establishment of a working group to further inform the EDPB on the issues the draft guidance raises. We would be delighted to assist the EDPB ABI in further discussions as they develop their guidance if deemed appropriate.

Contact us

If RSA can be of any further assistance, please do not hesitate to contact us:

Peter Townsend
Group Head of Financial Crime,
Group Data Protection Officer and Legal Counsel

Tel: 0044 207 1117282
Email: peter.townsend@gcc.rsagroup.com

Anthony Aronin
Head of Smart Wheels
Connected Insurance

Tel: 0044 1403 231657
email: Anthony.aronin@uk.rsagroup.com