BELRON SUBMISSION TO THE EDPB GUIDELINES 1/2020 ON PROCESSING PERSONAL DATA IN THE CONTEXT OF CONNECTED VEHICLES AND MOBILITY RELATED APPLICATIONS

Belron® is the parent company for a number of well-known vehicle glass repair, replacement and recalibration businesses, such as Carglass® and Autoglass® in Europe and Safelite® in the US. We are present in 39 countries with over 30,000 employees, serving more than 16 million consumers a year. Customer service is our key focus and we are proud of our high customer feedback score (average Net Promoter Score in 2019 was 85%). The Belron® purpose is "making a difference with real care".

Our services also include total vehicle recalibration of cameras and sensors relating to vehicle safety systems, as well as vehicle body repair, including full collision damage. In 2019 we carried out over 350,000 recalibrations of Advanced Driver Assistance Systems ("ADAS") in Europe.

Europe is a very important region for Belron®, with three out of our four largest markets here, with 13,000 employees in the region. Belron® is part of the automotive aftermarket which employs 2.8m people in the EU across 500,000 businesses.

Introduction

Belron welcomes the opportunity to comment on the EDPB Guidelines on processing personal data in the context of connected vehicles and mobility related applications. As the Guidelines rightly note, vehicles are increasingly connected, and with that connectivity, becoming data hubs. This is no longer limited to premium or luxury brands. Connected vehicles generate various types of personal and non-personal data which can be remotely collected and processed for a variety of purposes, including diagnosing issues, improving features, and enhancing safety and preventing accidents.

At Belron we see having access to connected car data as of fundamental importance to our business already today, and increasingly in the future. As more cars become connected, competitive access to data for all mobility stakeholders will be critical in shaping the future of the European mobility ecosystem for years to come. We fully support the work being done to ensure that car data can be shared in a secure and well framed way, in line with both competition rules, and holding the highest standards in terms of compliance with data privacy rules.

Distinction between personal and non-personal data

Belron welcomes the EDPB's recognition that there are distinctions between personal and non-personal data (para. 28) in terms of what data comes from vehicles. When data points are combined, it is highly likely that the owner or driver can be identified, thus making this person identifiable and requiring full compliance with GDPR rules.

When however, and as is recognized in the Guidelines, data points that cannot lead to the identification of an individual this should not be considered as personal data. This includes the vehicle identification number (VIN), data of high importance to a business like Belron's. The VIN alone can help us in two distinct ways – firstly by allowing us to source the right parts for the particular car in question. The VIN allows us to ensure the right glass and accessories are available, when we compare with OE codes.

Secondly, having access to the VIN ensures that we are able to carry out appropriate checks and audits to ensure that work to the vehicle has been carried out in the correct manner, with the right parts, ensuring safety and quality for the consumer.

Gaining Consent

Belron supports the EDPB's emphasis on the need for all elements of consent to be adhered to (1.5.2,) and in particular welcome the clarity that consent (para. 46) "may not be bundled with the contract to buy or lease a new car." This is of paramount importance for the offering of e.g. maintenance services on a level playing field, thus ensuring fair competition in the use of the data being generated. Bundled consent would clearly give vehicle manufacturers and dealers a competitive advantage in offering aftermarket services, depriving the driver of choice.

We do have concerns however that the EDPB interprets vehicle data – whether personal or not – to fall under the ePrivacy Directive (para. 47) by the virtue of it being a 'connected' device. This would require granular consent for any remote collection of data, despite the fact the same data collected via e.g. maintenance works in the garage, would not be subject to these rules. The impact of this is that a company like Belron would not be able to collect anonymous technical data remotely without first obtaining consent – but would be able to access the same data without consent should the vehicle be in one of our garages.

This seems overly burdensome and beyond what is strictly necessary to ensure full protection of personal data. In addition, rather than allowing for innovation and a remote customer seamless experience which can occur through our innovation and ability to write in the vehicle, such requirements will in fact keep aftermarket service providers in the analogue world.

The Guidelines also stress that Article 6 of the GDPR cannot be relied upon by controllers in order to lower the additional protection provided by article 5(3) of the ePrivacy Directive (para. 15).

We find this view to be limiting and disproportionate as it should be possible to rely on alternative legal bases for processing under Article 6 of the GDPR in certain circumstances – which the Guidelines demonstrate in the case studies. For example, in the context of 'pay as you drive' insurance, the EDPB allows for insurance companies to rely on Article 6(1)(b) (processing necessary for the performance of a contract) for the processing of personal data following the storage or access to the end-user's terminal equipment (the vehicle). Moreover, where there is a legal obligation to process personal data, the EDPB considers Article 6(1)(c) to be applicable. The question must surely be raised as to whether a company and service provider like Belron can also rely on the same legal basis – especially if it ensures a full and safe job can be done for our customers.

Finally, Belron is concerned by the example being used in paragraph 57 in relation to demonstrating the cyber security risks involved with connected cars. It is true that should there be a technician wanting to cause harm during the maintenance check of a vehicle, then s/he could potentially do so, but this is no more real in the digital, connected world than it is the analogue world.

General Recommendations: Observations

1) Data Location (2.1.1)

In relation to the three categories of special data that the EDPB has identified, Belron only has concerns in relation to location data. As an aftermarket service provider, we are not interested in gaining access to biometric data or data that could reveal an offence.

Our interest in gaining access to location data stems from the fact we want to be able to offer our services to our customers and allow them to be helped as soon as is possible. No one actually ever wants to be in a position where they need to call on us; but circumstances often mean that our customers do need to come to us or for us to go to them. Chipped and cracked windscreens together with recalibration of safety systems are the most common cause for people to seek our services, and in order for us to get to our customers quickly – or in order for them to get to our nearest garage – it is of paramount importance to know where the vehicle is located.

In this respect, we do not require continued access to geolocation data, and we do not need to continuously track the vehicle. We agree with the Guidelines that such access to this data should only be when absolutely necessary for the purpose of processing, and should be activated when needed, and clearly deactivated once our team has arrived at the vehicle. We also agree with the Guidelines that there is no need to store this data beyond the timeframe necessary.

2) Data Mimimization (2.3)

In terms of data minimization, Belron requires certain data sets in order to provide services to the vehicle. These, for the moment, are clear and limited in scope and we know what is needed to carry out particular jobs. In the future, it may be difficult to assess what other data sets may be required in order to provide new, innovative services, and we therefore call on the EU institutions to ensure that a regulatory framework is established in order to maintain a level playing field for all economic actors in the automotive chain. A proper consideration on accessing this data, in line with the Data Package presented by the Commission, should also be considered in order to fully realise the value of the data being generated.

3) Processing (2.4.1)

The Guidelines set out that processing of data should take place in the vehicle. Belron fully supports this, as per the requirements under the GDPR, especially as the data that we require in order to perform a service for our clients (either inside of the vehicle or outside) can be anonymized and need not relate to an identifiable person, but rather to a Diagnostic Trouble Code (DTC) or other fault that requires fixing. Once we have consent from our customer that they require our services, we would expect that this extends to all data required (non-personal) in order to perform the work.

Case Studies

The EDPB has set out some helpful case studies that allow some actors in the automotive world to better understand how to ensure full compatibility with data protection rules when accessingconnected car data. Belron considers it is a missed opportunity that there is no case study in relation to the offering of services in the aftermarket – which in itself is a bigger contributor to jobs than vehicle manufacturers in the EU, and yet remain at risk from being cut out of the market via being denied access to connected car data. Perhaps this is something that can be added.

Final Comments (Part 3)

At Belron we put safety at the forefront of everything we do, which includes keeping our customers personal data well protected. In order to ensure that only reputable companies can have access to connected car data, Belron considers it a necessity for the EDPB and the EU institutions to consider setting up a specific body to certify all companies dealing with data in this space. Only certified companies would then be granted access, upon receiving the required consent from customers.

* * *