Tesla comments on EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications

Tesla, Inc. is a recognized automotive leader in the fields of Information and Communications Technology ("ICT"). We are actively developing Autopilot with the intent of offering Full Self-Driving capability to our customers in the coming years. All Tesla vehicles are currently equipped with the required hardware which allows for Tesla's pioneered concept for making cars more capable over time, due to over-the-air software updates (www.tesla.com/support/software-updates). While traditional cars have static features, a Tesla receives new functionality and enhancements throughout its life, transmitted to the vehicle through either a cellular or Wi-Fi connection. Our over-the-air software system enables us to continuously improve both passive and active safety capabilities as well as the cybersecurity of our vehicles, furthering our mission to offer the safest vehicles on the road.

Tesla welcomes the European Data Protection Board's ("EDPB") draft guidelines on the processing of personal data in the context of connected vehicles and driving-related mobile applications ("Guidelines"). In this context, the Guidelines outline the applicability of both the General Data Protection Regulation ("GDPR") and the ePrivacy Directive 2009/136/EC ("ePrivacy Directive") in this context. Tesla supports the EDPB's efforts to ensure privacy and data protection are maintained as increasing amounts of data are collected and processed in the context of connected vehicles and mobility-related applications. We look forward to the EDPB's future revision of these guidelines based on the input received from stakeholders, as this effort will also be crucial to accelerate confidence in the needed shift towards electromobility in Europe.

At Tesla, we put significant effort into ensuring that data protection and privacy controls are considered throughout the entire product development lifecycle, from beginning to end. We also strive to ensure that our data subjects have expanded rights and choices in a variety of areas such as access, deletion and the restriction of processing certain related data.

To begin with, Tesla does not sell the personal data of customers to anyone for any purpose, period.

In addition, Tesla has implemented several measures to ensure our customers have appropriate knowledge of what data may be collected at any given time, as well as the methods that are used in the process.

- Tesla applies the principles of data minimization in general and only collects specific data points (e.g. relating to speed) in the event of technical analysis or a safety critical event.
- Autopilot data sharing is off by default in our vehicles and requires explicit consent from the customer before this can be activated.
- Data sharing can be turned off at any point in time should our customer desire to do so.
- Tesla's Privacy Notice (www.tesla.com/about/legal) is written and designed in a format that is easy to read, understand and navigate for our customers.
- Data privacy requests are handled through a formal, standardized channel for intake (www.tesla.com/support/contact) which is easily accessible and seamlessly integrated with the customer's Tesla account. Our support page provides clear instructions explaining the data access request process (www.tesla.com/support/privacy), including frequently asked questions, as well as what kind of data the customer can expect to be provided as part of their request.

Scope & General Comments

The concept of a connected vehicle is defined by the EDPB as a "vehicle equipped with many electronic control units that are linked together via an in-vehicle network allowing it to share information with other devices both inside and outside the vehicle." The Guidelines specifically apply to both connected vehicles and mobile applications that relate to driving.

To fall within the scope of the Guidelines, applications need to relate to "the environment of driving." This includes for example applications that provide drivers with information on weather conditions, traffic congestion, monitor a driver's ability/fitness to drive, and partial/full automated driving, while an application that suggests places of interest would not be in scope. Employers providing company cars and monitor an employee's actions within the context of employment are likewise considered outside of the Guidelines' scope. Similarly, camera recordings of public spaces (e.g., dashcams, parking assistance, or driver monitoring) are also out of scope.

We note the following key conclusions from the Guidelines:

1. Consent is required to store or access any information on a connected vehicle.
2. Personal data retrieved from a connected vehicle may not be used for a secondary purpose without consent.
3. Location data should only be collected if required by a functionality launched by the user.
4. Vehicle data controllers are encouraged to consider activities that would facilitate local-processing-by-default.
5. User profiles are recommended to manage consent and deletion of personal data.

General Feedback

The EDPB guidelines posit that consent should generally be the legal basis for the processing of personal data in connected vehicles.

We believe however that the guidelines risk undermining the agreement that was reached on the General Data Protection Regulation in favour of a risk-based approach for the processing of personal data. The ePrivacy Directive protects the data subject's terminal equipment, which is different than protecting the processing of the personal data itself.

It is also crucial to acknowledge that the ePrivacy Directive came into force in 2011 following its publication in 2009, i.e., before significant technologies related to connected vehicles and mobility applications were introduced at a larger scale on the market. For over three years, the ePrivacy Directive has been under review to adapt to the quick changes in technological developments.

As many products and services will continue to advance and become suitable for connection to the network, everything will be deemed to be a terminal equipment, and then subject to a rule designed for a very different case, such as cookies in the case of Internet. In our view, the EDPB Guidelines should consider relying on principles set forth in the GDPR such as the risk-based approach, and the flexible applicability of the most suitable legal processing ground depending on the concrete case scenario.

The ongoing implementation and enforcement of the ePrivacy Directive may prove inappropriate or obsolete and should be delayed until the revised ePrivacy directive is published. Similarly, a review of GDPR is planned which may likewise other introduce significant changes that should be considered herein.

In such a context, we question the validity of interpreting the relationship between the existing GDPR and ePrivacy Directive in the case of data collected by connected vehicles until the relationship between these two legal texts can be reevaluated in light of their respective revision. Issuing guidelines at this stage, before these revision processes take place, risks conditioning and stymieing innovation in the sector.

Tesla Remarks & Recommendations

1. **Comments on the Special Categories of Personal Data**. The Guidelines identify three categories of personal data which warrant special considerations:

    a. Geolocation data (para. 60): The Guidelines consider geolocation data to be potentially invasive, arguing that it may reveal many personal aspects of a data subject's life. Therefore, Controllers must be "particularly vigilant" not to collect location data except where "absolutely necessary" for the purpose of processing. The Guidelines further recommend that users should be informed when location data is being collected, in particular by using icons, and that they should have the option to deactivate location collection at any time.
    b. Biometric data: The use of fingerprints, eye movements, facial recognition or voice commands by connected vehicles to enable certain functions should be stored locally in the vehicle and not be mandatory.
    c. Data that could reveal criminal offenses or traffic violations: In certain circumstances, personal data from connected vehicles could reveal a potential criminal offense (e.g. the speed of a vehicle combined with precise geolocation data could be considered offense-related data). Therefore, appropriate safeguards are required to protect the rights and freedoms of data subjects under GDPR Article 10.

Remarks

Special Categories of Personal data would require – as described above – specific safeguards to prevent the surveillance of individuals and the misuse of data. The guidelines suggest that, for example, geolocation should only be used when strictly necessary and would require a manufacturer to put in place different measures - such as informing the user that the geolocation has been activated by using icons, giving the option to deactivate the geolocation, and defining a limited storage period.

This requires a more in-depth assessment as it may inadvertently have significant implications for safety and comfort functions that would otherwise be normally available to the driver and other passengers, and potentially other vehicles, bicycles and pedestrians on the road.

Indeed, some safety functions require or can be augmented by geolocation data without specific identification of the end-user. For example, some Tesla vehicles are currently equipped with smart air suspension allowing for the vehicle to intelligently adjust its height for better handling, efficiency, and ride comfort. This can be useful when entering a steep driveway, navigating snow, or unloading passengers and belongings. Using GPS location detection, a customer's Tesla vehicle will remember and reapply those settings automatically where needed detected (or as manually set by the customer).

Recommendation

The EDPB guidelines should clarify the meaning and implications of using geolocation 'only where absolutely necessary', which we consider a subjective and restrictive formulation. If additional requirements are introduced, more consideration should be given to whether these requirements would introduce drawbacks, complications or other issues, or broadly prove unjustified. As noted in other stakeholder contributions, Article 9 of GDPR does not identify location data as a special category of personal data. The intended aim of data's processing, not its nature, appropriately defines the sensitivity of personal data.

2. **Comments on the Role of Consent**. The Guidelines posit that when the data accessed or stored on the 'terminal equipment' is also 'personal data' under GDPR's definition, Article 5(3) of the ePrivacy Directive takes precedence over the GDPR. This means that the legal basis for data processing under Article 6 of GDPR cannot be used to justify accessing or storing personal data, from or to, connected vehicles. Exceptions to obtaining consent include: (1) if processing is for the sole purpose of "carrying out the transmission of a communication over an electronic communications network"; and (2) when it is strictly necessary in order to provide the requested service.

   The first exception would apply, for example, when a user downloads content, or sends a message using the infotainment in the vehicle. The second exception, for example, would be a user booking a parking space through an app offered by a third-party provider, and processing the vehicle's 'navigation data', in order to provide this service explicitly requested by the user.

   For the processing of personal data stored in the vehicle, such as contact details, license plate number, payment information, the lawful basis for processing under the GDPR will be 'necessity to enter a contract', under Article 6(1)(b). The Guidelines (para. 121) further caution Controllers to be mindful of the potential complexities of obtaining consent from different participants, which could vary from car owners, users, or passengers.

Remarks

The Guidelines heavily rely on consent as the primary legal basis for processing data related to connected vehicles. However, this general recommendation by the EDPB fails to recognize or appreciate that consent often is not the most suitable legal ground supporting data processing. Personal data can be processed for myriad different purposes such as safety, insurance, efficient navigation, etc.

These purposes would each need to be consented to by the user, and should always be specific, explicit and freely given. They also should not include secondary purposes that may be incompatible with the original consent request. However, in the rapidly developing, multi-actor environment which connected vehicles navigate, the consent scheme can prove too static, inhibitive and slow. This could jeopardize the pace of innovation in a field that has been recognized by authorities as having the potential—if not certainty—of bringing significant economic, environmental and safety benefits.

Recommendations

a. As noted in other stakeholder contributions, and acknowledged by the EDPB (para. 49), consent may be difficult, impracticable, or even impossible to obtain in many instances (e.g., when the drivers or passengers are not related to the vehicle owner, cases where passengers cannot be identified, etc.). It is not practically feasible to collect informed consent from the end-user in the context of connected vehicles for all processing activities. As such, consent should not be considered the primary legal basis for data processing. Other legal bases that embed the risk-based approach, such as 'legitimate interest' or 'performance of a contract', are more suitable in this context.

b. Instead of systematic consent procedures, users should be able to configure their device or vehicle settings up front to: (a) either accept or reject specific tracking; or (b) grant this right only to selected parties (including trusted partners or third-party providers offering an indispensable service). This consent model would further allow users to subsequently revoke or rescind their consent as their personal preferences evolve or other circumstances arise. Defaulting to the user-selected default consent decision, subject to change at the discretion and direction of the user, is far more feasible to manage, implement and enforce than the systematic and situational consent procedures contemplated.

3. **Data Subject Rights**. The Guidelines (para. 88) recommend for vehicle manufacturers to facilitate data subjects' control over their data by implementing a profile management system inside connected vehicles to store the privacy preferences of known drivers, and to allow the ability to directly access, delete or remove their personal data from the vehicle's systems. A change of ownership of the vehicle would also trigger the permanent deletion of any personal data of the previous owner.

Remarks

Tesla supports the notion that a customer's privacy preferences should be easily accessible including the ability to exercise rights – e.g. deletion. As such, we already provide vehicle owners with a mechanism to factory reset their settings and preferences directly from the vehicle's interface at any time. The EDPB, however, prescribes a specific method for reaching this objective in stating that "[…] a profile management system should be implemented *inside the vehicle* in order to store the preferences of known drivers and help them to change easily their privacy settings anytime" (emphasis added).

The method for reaching this objective should not be limited to implementation inside the vehicle's interface alone, which does not allow for continued innovation of connected vehicles in this area. Alternative methods include the ability for individual drivers to pre-select their privacy preferences online (e.g., through their Tesla Account), mobile app-based dashboard, or other similar means. Each method would equally accomplish the goal by recognizing the individual driver's privacy preferences and then automatically adjusting its communications and sensor technologies to accommodate for those choices.

Recommendations

The Guidelines (para. 88) could benefit from clarification by rewording the following sentence: "To facilitate settings modifications, a profile management system should be implemented ~~inside the vehicle~~ *[to be easily accessible by the user]* in order to store the preferences of known drivers and help them to change easily their privacy settings anytime" (emphasis added).

Connected vehicles are dissimilar from mobile smartphone devices as they allow for multiple users. This should be well considered and can affect the degree to which type of data can be associated to the varying data subjects. Although the Guidelines state that profile management is related to "known drivers," it may be beneficial to explicitly clarify that passenger data is out of scope and that it would be the driver's responsibility to inform passengers of the individual driver's privacy preferences.

4. **Local Processing of Personal Data on the Vehicle**. Where possible, the personal data collected should not be transferred, but rather processed locally on the vehicle. Local processing presents fewer cyber security risks and mitigates the risks of cloud processing. In particular, the Guidelines (para. 70) recommend developing a secure in-car application platform, "physically divided from safety relevant car functions so that the access to car data does not depend on unnecessary cloud capabilities." If local processing is not possible, the Guidelines recommend anonymizing or pseudonymizing personal data to minimize the risks generated by the data processing.

Remarks

Tesla supports the Guidelines' interpretation with respect to the local processing of personal data on the vehicle *where possible*, as this balances the data subject's privacy interests with safety and the practicability of implementation of many data processing activities (para. 70). However, while local processing of data offers the advantage of being under the vehicle owner's control, it does not necessarily provide for an inherently higher level of cybersecurity if not adequately safeguarded (as it may otherwise be, if processed by cloud computing).

Additionally, the Guidelines provide some examples of local processing activities representing instances of purely personal activity by a natural person, which would fall outside the scope of GDPR in accordance with Art. 2(2). We would however urge the EDPB to provide explicit clarification that the data solely processed locally on a vehicle would not be subject to the Guidelines or GDPR, as the vehicle driver would be the controller for such processing activities.

Recommendations

The Guidelines would benefit from clarification related to data processed locally on the vehicle. In keeping with the EDPB's smartphone device analogy, mobile phone manufacturers are not expected to maintain control of the local data processed on a customer's smartphone – as opposed to the data processed on its servers, local processing is considered outside of a manufacturer's control.

For data locally processed or stored in a car, it is not the vehicle manufacturer who is responsible or obliged to provide information, but rather, this is the responsibility of the vehicle owner (similar to when an individual uses their personal computer, for example, and usage data logs are stored internally when doing so). In accordance with GDPR Art. 15 and the jointly prepared Declaration of the Conference of Independent Data Protection Authorities (unabhängigen Datenschutzbehörden des Bundes) and the Association of the Automotive Industry (Verbandes der Automobilindustrie)[1], we urge the EDPB to consider adopting the German data protection supervisory authorities' guidelines by clarifying that only personal data leaving the car to be processed on the vehicle manufacturers or third party servers would be in scope of the Guidelines.

Other Key Issues for Consideration

1. Does the EDPB consider consent to be the only valid legal basis for connected vehicles or can alternative approaches (such as device configurations embedded in the vehicle) be considered?
2. If personal data is processed and stored locally on the vehicle, is the Controller required to transmit that personal data to its servers in order to fulfill data subject access rights?
3. If personal data is maintained in a de-identified manner by methods of de-identification (e.g., pseudonymized, anonymized), is the Controller required to re-identify or otherwise link the personal data back to the user to fulfill data subject access rights?

Closing Remarks

At Tesla, people come first in everything that we do. We care deeply about our Tesla community around the world, and the planet that we all share. Our dedication is reflected in everything from our Supplier Code of Conduct, to our efforts to eliminate our comprehensive carbon footprint, and our support of fundamental human rights. This includes our individual right to privacy. Tesla continually aims to enhance and improve its data practices throughout each stage of the product development lifecycle. We therefore appreciate your attention to, and clarification of the suggested guidelines related to the protection of privacy rights and the processing of personal data in the context of connected vehicles.

Respectfully Submitted,

Tesla, Inc.

[1] Joint declaration by the independent data protection authorities of the federal and state governments and the Association of the Automotive Industry (https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/ErklaerungDSKVDAVernetzteKfz.pdf)