DSI | DIGITAL SOCIETY INSTITUTE BERLIN

ESMT BERLIN

DSI Industrial & Policy Recommendations (IPR) Series

Recommendations for safety, security and data policy in automotive IT

Sandro Gaycken, Martin Schallbruch, Georg Becker (Digital Society Institute, ESMT Berlin)

Issue 4, 2017

The car of the future will collect a wide range of data. Ownership and usage of those data must be clarified, and legal and technical characteristics have to be established in order to ensure data protection, data security, vehicle safety, and a fair market.

On these issues, DSI has carried out stakeholder workshops with the automotive sector, mobility digital startups, automotive insurers, and vehicle inspectors and, on this basis, has developed the following recommendations.

The right to personal data collected in the vehicle should be first due to the customer (owner or driver, depending on the context). Customers should be transparently informed about the collected types of data and the depth of the data collection to decide how to make the data accessible, to whom and for what purpose. Data should be bundled into understandable packages based on types and use context. On the other hand, the rights to strictly vehicle-related technical data – in which a person is not directly identifiable, which are produced by and in technologies of the vehicle, which fulfill essential functional and safety-relevant functions, and which the vehicle manufacturers or associated OEMs are most capable to understand and process – should be given to the vehicle manufacturers or the OEMs first, in order to achieve a clear and effective distribution.

In order to enable a large and fair market as well as the broad development of the automotive and mobility market, all service providers and third-party providers should be in an equivalent, fair, appropriate, and non-discriminatory position to offer their services to respective data owners. This is the only way to ensure a high level of innovation in the automotive and mobility sectors. When using the data, service providers and other third-party providers must ensure their security and data protection in accordance with applicable national law. Decisions regarding the wishes of service providers or third parties for special access to or specific surveys of data to enable new business models should be made by vehicle manufacturers in order to ensure the safety and integrity of the vehicle's overall architecture. These decisions must be factually justified and independently verifiable. Because of the security implications, it is particularly important that service providers and third parties do not receive "write" access to vehicle systems, except through explicit bilateral agreements with vehicle manufacturers or OEMs for purposes of maintenance and diagnostics in the garage via the OBD interface on the parked vehicle. Third-party software in the vehicle must not have direct access to the CAN bus.

For data that is critical for data protection, data security, or vehicle safety, access must be explicitly managed in order to establish responsibility and accountability as well as to ensure a correct implementation of technical standards. A centralized, technical management of the data transmission by OEMs is conceivable for these data types, but the service providers working with these data should not be placed at a disadvantage to the OEMs. An automotive platform could be a different or complementary measure of warranty.

For data types with relevance to auto safety and security, the State should define – in consultation with insurers, inspectors, and law enforcement authorities – whether and in what form these data must be collected and deposited and in what manner and under what conditions access to these data may take place, provided that such data are relevant for accreditation processes, accidents, thefts, manipulations, or similar processes that necessarily involve external parties. For highly automated vehicles (level 3 and above), transparent, cross-manufacturer standards are required for a set of relevant data to be recorded, for

the data formats to be used, and for access to these data. For the implementation of the handling of relevant data in practice, a model of an independent data trustee can ensure that the raw data is encrypted and treated impartially and that access is only possible with legitimate interest, taking into account legal requirements. Such a model could also be considered for the provision of other personal data.

In order to consistently achieve the desired goals despite technical and legal complexity, it is necessary to guide technical and regulatory development via principles that address future automotive concepts and architectures. After consultation in the stakeholder workshops, DSI proposes the following principles:

1. Privacy by design: The privacy of private data should be made architecturally, not only legally. The underlying technical concept shall be “trustworthiness" not “trust.”

2. Privacy by default: As described, personal or person-generated data should first belong to the driver/owner of the vehicle.

3. Security by design: The security of critical functions should also be secured architecturally and “trustworthy.” The underlying technical concept, whenever possible, should be provable security, not assured security.

4. “Safety First” principle for IT security: If data or informational processes have implications for safety, the risk must be considered high – regardless of the probability of attack – and safety requirements must be met according to this risk expectation.

5. Consistency of safety and security requirements: Standards and assumptions expressing the reliability of safety-functions must be applied in the exact same quantitative expression - “one-to-one” - to the security of the systems carrying these function.

The DSI Industrial & Policy Recommendations (IPR) Series is published by the Digital Society Institute of ESMT Berlin, http://dsi.esmt.org.

DSI | DIGITAL SOCIETY INSTITUTE BERLIN

ESMT BERLIN

DSI Industrial & Policy Recommendations (IPR) Series

Empfehlungen zu Sicherheit und Datenpolitik bei automatisiertem und vernetztem Fahren

Sandro Gaycken, Martin Schallbruch, Georg Becker (Digital Society Institute, ESMT Berlin)

Ausgabe 4, 2017

Das Auto der Zukunft wird eine Vielzahl von Daten erheben, zu denen Besitz und Verwertung zu klären sind und an denen rechtliche und technische Eigenschaften festgemacht werden müssen, um Datenschutz, Datensicherheit, Fahrzeugsicherheit und einen gerechten Markt zu gewährleisten.

Das DSI hat zu diesen Fragen Stakeholder-Workshops mit dem Automotive-Sektor, digitalen Startups aus dem Bereich Mobility, den Automobil-Versicherern und den Fahrzeugprüfern durchgeführt und auf dieser Grundlage die folgenden Empfehlungen erarbeitet.

Das Recht an den im Fahrzeug erhobenen personenbezogenen Daten sollte zuerst den Kunden (je nach Kontext Halter bzw. Fahrer) zustehen. Die Kunden sollten transparent über die erhobenen Arten von Daten und über die Tiefe der Datenerhebung informiert werden und darüber entscheiden können, wem diese Daten zu welchem Zweck zugänglich gemacht werden. Daten sollten aufgrund ihrer hohen Anzahl nach Arten und Verwendungszwecken in kundenverständliche Pakete gebündelt werden. Die Rechte an rein fahrzeugtechnischen Daten dagegen, bei denen ein Personenbezug nicht gegeben ist, die durch und in Technologien des Fahrzeugs erstellt werden und die wesentliche funktionale und sicherheitsrelevante Funktionen erfüllen und zu deren Verständnis und Verarbeitung die Fahrzeughersteller, beziehungsweise die ihnen zugeordneten OEMs, am ehesten in der Lage sind, sollten zur Erreichung einer eindeutigen und effektiven Zuordnung zuerst den Fahrzeugherstellern bzw. den OEMs zustehen.

Um einen möglichst großen und gerechten Markt und eine breite Entwicklung des Automotive- und Mobility-Marktes zu ermöglichen, sollten alle Dienstleister und Drittanbieter in einer gleichwertigen, fairen, angemessenen und diskriminierungsfreien Position sein, den jeweiligen Dateneignern ihre Dienste anzubieten. Nur so kann eine hohe Innovationskraft in den Bereichen Automotive und Mobility gewährleistet werden. Dienstleister und andere Drittanbieter müssen bei der Verwendung der Daten deren Sicherheit und Datenschutz nach geltendem nationalem Recht selbst gewährleisten. Entscheidungen über Wünsche von Dienstleistern oder Drittanbietern für besondere Zugänge zu oder besondere Erhebungen von Daten zur Ermöglichung neuer Geschäftsmodelle sollten die Fahrzeughersteller treffen, um die Sicherheit und Integrität der Gesamtarchitekturen des Fahrzeugs gewährleisten zu können. Diese Entscheidungen müssen sachlich begründet sein und unabhängig prüfbar getroffen werden. Aufgrund der Sicherheitsimplikationen ist es insbesondere wichtig, dass Dienstleister und Drittanbieter keinen schreibenden Zugriff auf Fahrzeugsysteme erhalten, ausgenommen durch explizite bilaterale Vereinbarungen über die Fahrzeughersteller bzw. OEMs sowie für Zwecke der Wartung und Diagnose in der Werkstatt über die OBD-Schnittstelle am parkenden Fahrzeug. Fremdsoftware im Fahrzeug darf keinen direkten Zugriff auf den CAN-Bus erhalten.

Für Daten, die kritisch sind für Datenschutz, Datensicherheit oder Fahrzeugsicherheit, müssen Zugänge gezielt und explizit verwaltet werden, um Zuständigkeit und Verantwortlichkeit herzustellen und um eine problemlose Umsetzung technischer Standards zu gewährleisten. Eine zentrale, technische Verwaltung der Datenvergabe durch die OEMs ist für diese Datenarten denkbar, wobei aber mit diesen Daten arbeitende Dienstleister den OEMs gegenüber nicht in Nachteil geraten dürfen. Eine Automotive-Plattform könnte eine andere oder ergänzende Maßnahme der Gewährleistung sein.

Für diese im Auto entstehenden Datentypen mit Relevanz für Safety und Security sollte zudem der Staat in Abstimmung mit Versicherern, Prüfern und Strafverfolgungsbehörden definieren, ob und in welcher Form diese Daten erfasst und hinterlegt werden

müssen und in welcher Weise und unter welchen Bedingungen der Zugriff auf diese Daten erfolgen darf, sofern diese Daten relevant für Zulassungsverfahren, Unfälle, Diebstähle, Manipulationen oder ähnliche Prozesse mit notwendiger Einbindung externer Parteien sind. Für hochautomatisierte Fahrzeuge (ab Level 3) bedarf es transparenter, herstellerübergreifender Standards für einen aufzuzeichnenden Satz entsprechend relevanter Daten, für die dabei zu verwendenden Datenformate und für die Bedingungen des Zugangs zu diesen Daten. Für die Umsetzung des Umgangs mit entsprechenden Daten in der Praxis kann ein Modell eines unabhängigen Datentreuhänders gewährleisten, dass die Rohdaten verschlüsselt und unparteiisch behandelt werden und dass der Zugriff nur bei berechtigtem Interesse unter Berücksichtigung der rechtlichen Anforderungen möglich ist. Ein solches Modell könnte auch für die Bereitstellung sonstiger personenbezogener Daten in Erwägung gezogen werden.

Um die angestrebten Ziele gegen die technische und rechtliche Komplexität konsequent zu erreichen, ist es erforderlich, die weitere Entwicklung durch Prinzipien anzuleiten, die sich an zukünftige Automotive-Konzepte und –Architekturen wenden. Das DSI schlägt nach Abstimmung in den Stakeholder-Workshops die folgenden Prinzipien vor:

1. Privacy By Design: Der Datenschutz privater Daten soll architektonisch hergestellt werden, nicht rein rechtlich. Das unterliegende technische Konzept soll „trustworthiness“ sein, nicht „trust“.
2. Privacy By Default: Wie beschrieben sollen personenbezogene oder personengenerierte Daten zuerst dem Fahrer/Halter des Fahrzeugs gehören.
3. Security By Design: Die Sicherheit kritischer Funktionen soll ebenfalls architektonisch und „trustworthy“ gesichert werden. Das unterliegende technische Konzept soll – wann immer möglich – beweisbare Sicherheit sein, nicht behauptete Sicherheit.
4. „Safety First“ Prinzip für IT-Sicherheit: Sofern Daten oder informationelle Prozesse Implikationen für Safety haben, muss das Risiko unabhängig von Angriffswahrscheinlichkeiten als hoch angesetzt werden, und es müssen Sicherheitsanforderungen entsprechend der Risikoerwartung erfüllt werden.
5. Konsistenz von Safety- und Security-Anforderungen: Für die Ausfallsicherheit von Safety-Funktionen geltende Maßstäbe müssen „Eins zu Eins“ auch für die Angriffssicherheit gegen die diese Funktionen tragenden Systeme gelten.

Die DSI Industrial & Policy Recommendations (IPR) Series wird herausgegeben vom Digital Society Institute der ESMT Berlin, http://dsi.esmt.org.