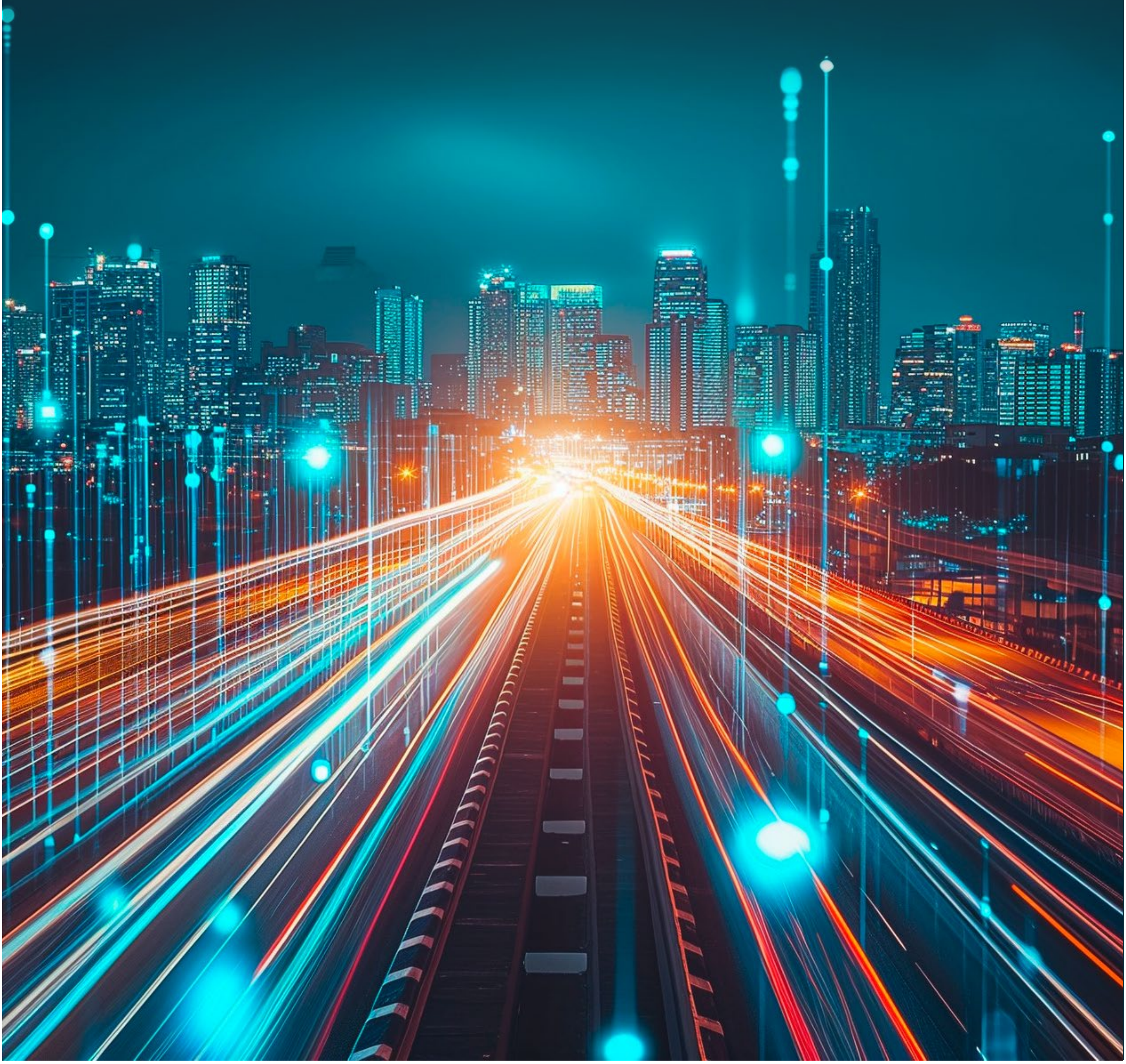
TaylorWessing

Tech Transformation, Data and Privacy in Automotive – Predictions for 2025



Mobility is going digital

The automotive industry is currently in a phase of profound upheaval. In particular, the constant tech transformation, development of Autonomous Driving and Advanced Driving Assistance Systeme (ADAS as well as the introduction and spread of electronic vehicles (EVs) is presenting companies with new challenges and opportunities. German car manufacturers, known for their high-quality combustion engines, must now focus more on the development and production of EVs in order to remain competitive and face great competition and cost pressure from the far east and the overall political climate with the fear of rising tariffs on trade especially in the US as a key market.

The rising competition and cost pressure forces automotive manufacturers to explore new roads: One trend is the rising monetization of data created by connected vehicles as a key asset in the competition. Another is the development of market leading Autonomous and ADAS technologies. Also, vehicle ecosystems become more and more a complex media landscape in which a wide range of services can be offered and consumed – the vehicle becomes a "mobile concierge" that seemlessly integrates and supports daily life.

At the same time, the legal requirements for car manufacturers and mobility service providers are becoming increasingly complex. Recently, a wave of digital regulations is crashing over businesses in the EU tech sector, making legal support for tech transformation in the automotive industry considerably more challenging. In particular, the EU's Digital Strategy and its related pieces of legislation will bring a wide range of innovations, some of which will have a significant impact on the automotive industry in 2025 such as the Data Act and – of course – the AI Act.

While data protection has been the dominant topic in tech transformation projects in the automotive industry for many years, the GDPR is now facing serious "competition" from other comprehensive regulations. Time for another update of our Taylor Wessing "Predictions: What's hot in tech transformation, data and privacy in the Automotive Industry in 2025" (formally known as "Digitization in the automotive industry") as 2025 holds a multitude of exciting legal challenges for legal teams in the automotive industry.

In the following we illustrate

- the main legal challenges that the industry will face in 2025 and the following years
- which of the topics should be at the top of the checklist, and
- how in-house legal teams can successfully manage and navigate through the flood of new regulations and growing complexity.

Also in 2025: Data Protection

Data protection is and will remain a defining compliance issue for the automotive industry although it is getting "company" in 2025. Several far-reaching provisions which are introduced in 2025 (amongst other the Data Act) will govern the processing of (non-) personal data and will create complex questions in terms of OEM's and suppliers rights to use vehicle data and the legal interplay with GDPR.

Data protection regulations (almost) always apply to the processing of vehicle data whether combined with clear data such as holder / driver name or not. In deviation of the opinion of the European data protection supervisory authorities, European Court of Justice established in a ruling that a Vehicle Identification Number (VIN) by itself is not necessarily to be considered personal data, unless the data holder has additional data (or knowledge) to link it to a natural person. The ruling itself is not surprising, as it simply reflects the principles of the GDPR. However, against the background of the strict practice of the (German) supervisory authorities and the automotive industry in recent years and member state regulations such as § 63f (1) No. 6 StVG (*Straßenverkehrsgesetz*) according to which the VIN is generally understood as personal data without consideration of the context of use the ruling seems to open up for a less strict interpretation.

Will the recently much-discussed ruling by the ECJ now make it noticeably easier for OEMs to process vehicle data? As always, the answer is: it depends. If (as will often be the case) the OEM has additional information on the owner / driver of a vehicle (e.g. through additional information from the area of sales / aftersales or connectivity services), the link required for the assumption of a personal reference usually exists already. This could be different if vehicle data is pseudonymized and processed in compliance with strict access concepts, e.g. by different group companies. However, the clarifications of the ECJ may make things easier, e.g. in the context of cooperation with development partners or suppliers, while in these cases the new regulations of the Data Act will play a major role (for details see below).

Regardless of the discussion about the personal reference of vehicle data, a distinction must always be made between the specifications for in-car data processing (= everything that happens exclusively in the vehicle) and external data processing (= everything after data has been transmitted to the outside). Not all companies in the industry are aware of the fact, that even for pure in-car data processing activities, in which the car manufacturer does not have any access to the data in the vehicle, certain data protection rules apply, not least, the principle of privacy by design and default and transparency. These require OEMs to explain to car owners and users at an early stage which data is processed in the vehicle and how one can affect the storage (see, among others, the guidelines of the CNIL and the joint statement of the Verband der deutschen Automobilindustrie (VDA) and the German data protection supervisory authorities).

With regard to GDPR rules for processing vehicle data the statement of the European Data Protection Board on connected vehicles, most recently with the update of the guideline in 2021, remains the go-to guideline for GDPR compliance in the connected vehicle landscape and provides valuable help on a wide range of questions.

And yet, significant questions remain.

For example, the meaning and **scope of Article 5 (3) Directive 2002/58/EC – (ePrivacy Directive)** (access to data in "terminal equipment") or its implementing regulations in Member State law (including Article 25 of the TDDDG in Germany) remain controversial. The EDPB follows a broad interpretation of the scope of Article 5 (3) ePrivacy Directive with the consequence that the use of vehicle data for secondary purposes such as product development, profiling, marketing etc. without the consent of data subjects is made considerably more difficult. It also remains unclear to what extent vehicle data may be stored for the purposes of **product monitoring and defence** and, if so, for how long. And what about data from vehicle sensors or cameras that are installed in the vehicle and support or monitor the driving process?

Much of this data can play an essential role in development, quality control and product monitoring. It is often difficult to determine the boundaries between the legal obligations of manufacturers (in the area of product compliance, among other things) and what is legally permissible in terms of data protection. The topic seems to be picking up speed in 2025 because individual OEMs have announced that they want to use vehicle data for more purposes in the future (including for product development and, in particular, the development and testing of algorithms and technologies for autonomous driving with AI). Data protection authorities have recently commented on the further use of vehicle data and are in contact with the OEMs concerned in order to develop joint solutions that will set certain standards for the secondary use of vehicle data in the future. It should be noted that the data protection authorities have already published comprehensive guidelines for the use of personal data and the training of algorithms in the context of AI, which are of course also relevant for the automotive industry. Similar questions arise against the background of the requirements of UNECE regulations R155 (Vehicle Cyber-Security Management System) and R156 (Updates of vehicle software / systems), which apply since 2024. Here, it is often unclear exactly which (personal) vehicle data must or may be used under which conditions for the purposes of cybersecurity of the vehicle ecosystem, e.g. when establishing a vehicle SIEM (Security Information and Event Management System). We highlight the tension between data protection, cybersecurity and product liability / product monitoring in this article.

Manufacturers of connected vehicles also have to consider **additional data protection regulations** which apply to this sector under European or national law. These include the special data protection requirements in EU member state laws such as the German Law on Autonomous Driving that came into force in Germany in 2021 (§§ 63 a ff. StVG (*Straßenverkehrsgesetz*)) as well as, for example, the European legal requirements for eCall (Regulation EU 2015 / 758), driver assistance systems (Regulation EU 2019 / 2144) or the requirement for transmission of (VIN-based) vehicle consumption data to EU authorities (implementing Regulation Regulation (EU) 2018 / 2043). The list goes on. This is a complex framework for legal teams when it comes to assessing the data protection law compliance of new car features which will get even more complex when Data Act and AI Act will apply (see below for details).

The increasing interconnectedness of the various players in the connected vehicle ecosystems also raises the question of which party has which **data protection responsibilities**. When should OEMs and external service providers be considered joint controllers? Where data flows can no longer be easily secured with a data processing agreement under Article 28 GDPR, there may be joint responsibility or controllership, requiring complex contractual arrangements in accordance with Article 26 GDPR, for example in the area of (cross-border) sales / aftersales, connected vehicle services and third party arrangements, especially when making third party services available in the vehicle via the head unit or the supporting connectivity services app. And which additional features in connected vehicles ecosystems, e.g. in the area of navigation or entertainment, are services commissioned by the user and can thus be justified via Art. 6 (1) lit. b GDPR and which of these may require special solution approaches such as separate consent in accordance with Art. 6 (1) lit. a GDPR? This topic also has a huge impact on the correct provision of information requests in accordance with Art. 15 GDPR, which often cause headaches for car manufacturers in practice, especially with regard to the amount of data to be provided and the verification of the claimant, especially in so-called multi-user scenarios.

Speaking of data access: Extended vehicle concepts and data access according to Data Act remain to give rise to data issues in 2025. In particular, whether and to what extent vehicle manufacturers must make data arising in connection with the operation of vehicles available to third parties, e.g. to enable other market participants to develop and offer comparable products and services. Under Regulation (EU) 2018 / 858, manufacturers are obliged to provide so-called repair and maintenance (RMI) data within the scope of applicable data protection rules. German car manufacturers addressed the urge for data sharing between vehicle users and third parties and developed specific concepts for data access, which are already in use today. Read our article for more on this issue.

The topic will gain momentum under the EU Data Act, coming into force in September 2025. It aims to facilitate access to vehicle data for customers and participants in the aftermarket. Existing concepts for data access for customers and third parties must be promptly put to the test and adapted to the new requirements of the Data Act (please see below for details) while several data protection law related questions remain unsolved which are addressed below in the context of EU Data Act.

Connected vehicles are undoubtedly at the focus of data protection regulators. In the past years, various car manufacturers including Tesla and VW have come under scrutiny and supervisory authorities are in contact with automotive manufacturers such as Porsche on these and other issues. Sales / aftersales data protection remains a "hot" topic for data protection authorities which has been subject to ongoing regulator audits and enforcement actions for some time now. And as indicated above, secondary use of vehicle data especially for the testing and development as well as the operation of autonomous technology in enabled vehicles will be a huge issue in 2025 with more clarification by authorities to come (hopefully) soon. Setting up a functioning car data protection management system is vital given the present regulator's focus and the extent of the legal requirements involved. Read more about it here.

EU Digital Strategy

The automotive industry is highly data-driven and this goes far beyond personal data. This means the sector is particularly affected by the EU's Digital Strategy. Alongside the Data Governance Act, the Data Act forms the basis of the European Digital Strategy. The regulatory framework is supplemented by other legislation, including the Digital Services Act and Digital Markets Act, which have already come into force. These legislations are now accompanied by the AI Act which will determine how data is handled in the EU in the future and has far-reaching consequences for OEMs in terms of data ownership and the design of respective processes.

Data, data, data …

Access to vehicle data is a long-running issue in the automotive industry, which has been the subject of considerable dispute between industry stakeholders for many years. With the Data Act, the EU legislature is now creating new regulations for access to data from networked devices (IoT), which explicitly also applies to vehicle data. The **Data Act** (DA) has been adopted in December 2023 and came into effect in January 2024. It is casting its long shadow already as companies will have to comply with DA's requirements in stages starting in September 2025, which is a very short timeline. It has a significant impact on the automotive industry. The objective of the DA is to regulate the most efficient possible access to and usability of data from networked devices for the benefit of those affected and companies. Vehicle data is explicitly included in the scope (see Recital 14). According to the provisions of the DA, so-called data holders (e.g. the automobile manufacturer if it holds vehicle data) will be required to provide access to the data not only to users (e.g. vehicle owners) but also to providers in vehicle related business areas such as aftersales, connected vehicle services, insurance or other sectors that may offer services in the vehicle ecosystem to customers. Access is to be granted at the request of the user (e.g. the vehicle owner) and has to meet strict formal requirements, such as data being readily available, without undue delay, of the same quality as is available to the data holder (= the OEM), easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. To meet these requirements a specific process and interface design between vehicle, manufacturer backend, user interface and third party systems will be required which at present (almost) no OEM will have fully in place. Several questions remain unanswered: How does DA interplay with data access rules for RMI data according to automotive specific regulations according to Art. 64 ff. Regulation (EU) 2018 / 858? How would an interface for third party data recipients (competitors) look like? How must OEMs factor that a vehicle is sometimes used by several users (multi user scenarios) and how shall a corresponding interface design in a multi-user scenario look like? How shall the authentication of several users for one vehicle take place? And in the light of the latest ruling of the ECJ on data access according to Regulation (EU) 2018 / 858 what restrictions can the OEMs impose on third parties when obtaining vehicle data, e.g. in the area of IT security? DA will present vehicle manufacturers with further major legal and practical challenges, including DA specific extended transparency obligations and the obligation to conclude a data license agreement in order to be allowed to use non-personal vehicle data for secondary purposes.

DA will be supplemented by specific vehicle data rules by way of a more specific EU Data Spaces Regulation. The regulation is pending and will likely not be provided before the taking effect of Data Act in September 2025 which sets OEMs under pressure.

The relationship of DA to the requirements of the **GDPR** is also unclear. Under what conditions may personal data be made available to third parties within the scope of the DA right of data access, in particular in the context of shared vehicles, fleet constellations and within company groups, if the user according to the DA (e.g. the employer as owner of the fleet) is not the data subject in the sense of data protection law? What role does the OEM assume if it grants third parties access to data at the behest of the user? That of a processoror of a controller or joint controller? And what is the correct legal basis for the related data transmission (consent, DA as legal permission or the balancing of interests pursuant to Art. 6 (1) lit. f GDPR)?

The GDPR aspect shows that "data" is a cross-cutting issue that cannot be managed by one legal or business team in the company alone in the future. The questions that arise here are: Where is the topic of "data" best located in the compliance organization? Are there conflicts of interest if the data protection organization is also responsible for "data" compliance? Does the company need a "data officer" and how would a "Data Compliance Management System" (DCMS) look like and work together with the company's Data Protection Management System (DPMS)?

Many questions that need to be clarified in corporate practice!

The EU Digital Strategy is accompanied by **Data Governance Act** (DGA), which was published on 30 May 2022, and applied from 24 September 2023. It includes, among other things, rules for providers of data intermediation services (so-called data intermediaries, such as data marketplaces) to ensure that they act as trustworthy organizers of data exchange or pooling within the common European Data Spaces. The specifications are of great importance for providers of corresponding data services, since the exchange and trade of vehicle and mobility data already represent a relevant business field, which is constantly emerging, e.g. in the area of product development. Respective services such as data marketplaces and data pools will be heavily regulated under DGA, for example, data intermediaries will not be allowed to process data for own business purposes (neutrality), must act neutral (other business areas to be legally separated), apply "fair" pricing models acc. to FRAND principles and will need to register with competent authorities. This is a major topic to watchout for – read more here.

Digital Services Act

In addition, the **Digital Services Act** (DSA), which came into force in 2022, will bring various issues with it. Most of its provisions will apply starting February 2024. A look into the calenders: The deadline has already passed! For this reason, many legal teams in the automotive industry are currently working at full speed on its implementation. Certain services offered by automotive manufacturers to customers and / or business partners can be subject to the new regulations, e.g.

Whenever data is transmitted, stored or made accessible to third parties, the DSA might apply, for example

- in the area of connected vehicle services, when third party content is included in the OEMs offering ("platform"; e.g. in user forums),
- in connected vehicle eco systems when OEMs offer a platform where businesses can sell products and services to consumers ("market place"; e.g. in mobile commerce applications in the vehicle), in the sales and aftersales domain, when OEMs provide platforms for third parties (or dealers) to market their product and services, ("platform" or "market place"), or
- where OEMs offer IT services including the hosting of data and systems "as a service" for other companies, including within company groups ("hosting").

DSA brings various obligations including regarding transparency, the establishment of complaint channels and a notice-and-take-down procedure, specific rules for marketing and recommendation systems and supplier compliance screening and management operations. Find more on how DSA will affect OEMs in 2025 in a series of articles dedicated to this particular topic here.

See more about DSA in general here and for an overview of the EU's various digitisation plans, check out our Deep Dive Session from Taylor Wessing's Digital Legal Academy.

The Big One: AI

With the **Artificial Intelligence Act** (AI Act), the EU creates the first and comprehensive regulation for the development, deployment and use of AI systems in the EU. It applies to AI system developers and providers as well as companies and organizations that use or operate AI systems in the EU – so basically all enterprises! It introduces regulations that prohibit certain AI systems ("prohibited") while the use and deployment of other risky AI systems will be highly restricted ("highrisk"). AI Act provides additional requirements for all AI systems, providers and users, as to data quality, human monitoring and control, transparency and traceability of decisions and compliance with ethical principles, including special rules for a conformity assessment and certification of high-risk AI systems. It will come into effect in stages in the next years, while the most relevant requirements for high risk AI will apply starting 2026 and 2027.

AI systems that are **safety components of products or systems**, or which are themselves products or systems falling within the scope of certain EU type approval framework regulations ("TAFR", e.g. (EU) 2018 / 858 and 2019 / 2144 e.g. for driver assistance) shall be deemed a high-risk AI system for which, however, special rules shall be enacted (see Recital 29 of AI Act). These specific rules are not available at this stage but will be drafted and enacted by the EU lawmaker in the near future as AI Act provides for that the EU will adapt existing automotive related regulations with more specific requirements while the EU Commission is supposed to support this process by issuing related guidance (see Art. 82 ff. AI Act).

Insofar as AI Act will generally apply to the automotive industry, it remains to be seen what **special vehicle regulations** are to come. In this respect, the situation is similar to that under the Data Act: More specific regulations that are (hopefully) better tailored to the needs of the automotive industry are also expected there, although time is becoming increasingly short for corresponding rules and their implementation. Complex follow-up and demarcation questions arise in particular where individual AI-based functions and services in the vehicle are subject to the regulations of the special TAFR (and thus not to the requirements of the AI Act), whereas other functions and services are "only" subject to the general requirements of the AI Act. Consequently, automotive manufacturers may have to apply different regulations for services in the same ecosystem that may follow different principles, which will further complicate implementation in the vehicle environment. It remains to be seen whether the automotive industry will come up with its own **standards** in a similar way to other areas (e.g. IT security), which seems conceivable. In any case, OEMs will have to keep a close eye on the market environment in 2025 in order to be able to react quickly to corresponding developments in terms of making use of AI which will certainly one of the (if not the) dominating topic of the next years! Find more on AI Act and its effect for the automotive industry here.

European Accessibility Act

After 28 June 2025 **European Accessibility Act** (EAA) requires accessible design of particularly relevant products and services including most forms of online shops and reservation platforms including related mobile apps placed for **handicapped persons**.

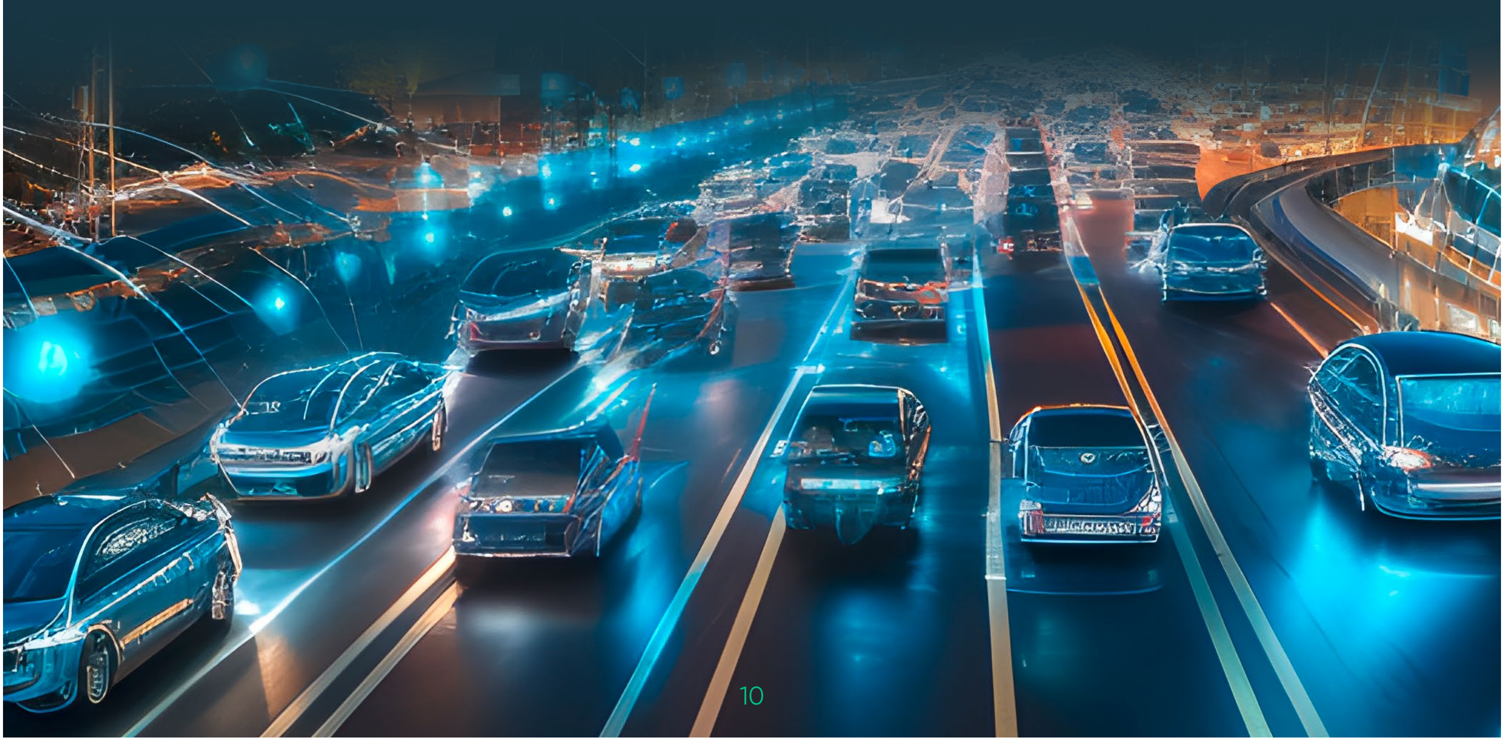
The new regulations require the implementation of various existing technical standards and guidelines for the removal of obstacles to the use of dedicated products and services, including webshops, apps or IT services, if these are connected to legal transactions with consumers.

The regulations are **important for the automotive industry** as they will apply, for example, to webshops, reservation platforms (e.g. testdrive, booking interfaces) and other eCommerce applications in the vehicle landscape. The extent to which the technical requirements are also to be implemented in the vehicle (e.g. the head unit) is left open by the law. Further questions arise for example with regards to websites or apps in mixed use scenarios (some parts subject to EEA while some are not) and if the entire service needs to meet EEA requirements (or only parts of it). Due to the broad interpretation of the requirements of the EAA and the national implementation laws based on it, it is urgently advisable for automotive companies to check their services with regard to the applicability of the regulations and start implementation as soon as possible to meet applicable timelines.

eCommerce and consumer protection

The requirements of the new **EU digital sales law** (applicable since 1 January 2022), the transposition laws to the Omnibus Directive (applicable since 28 May 2022) and the requirements for fair consumer contracts (some of which became applicable in the last years already) will keep automotive manufacturers on their toes also in 2025.

The new laws have a significant impact on automotive manufacturers, particularly in the area of connected vehicle services. They introduce new requirements specifically for digital products and services and can also apply to free services where for example personal data is provided in return for a "free" service. Warranty, termination and revocation rights are extended. Digital products will be subject to new support and update requirements to prolong their use for the duration of their typical usage which may exceed the general warranty rights and factually enhance them to several years. The regulations create a complex interplay between regulatory requirements, including in the area of UNECE R155 (over-the-air (OTA) update rules) and digital warranty rights, particularly where OTA updates will increasingly be used in future to rectify warranty-relevant defects in the vehicle. In addition, the constant integration of third-party services in vehicles increasingly raises the question of legal responsibility under warranty in the event of defects or malfunctions in digital products or products with digital elements. Manufacturers must clearly define the responsibilities contractually and in external communications in order to avoid unintentionally assuming liability for third-party services offered to customers in the future which are offered i.a. in the context of navigation services or media offerings. This network of obligations is complex and requires the involvement of various departments within the automotive's organization, such as IT security, product liability and product compliance, and sales. See our article on the new eCommerce and digital sales law and Connected Vehicle Services for more.



IT security and product security

Against the backdrop of the steadily increasing cyber threats, the topic will remain a top priority for car manufacturers in 2025, not least because of the constantly tightening legal requirements.

Manufacturers in scope had to implement the requirements of **UNECE Regulations** R155 (Cyber Management System for Vehicles) and R156 (Requirements for Updates of Vehicle Software / Systems), since 2024 via Regulation (EU) 2018 / 2144. They now need to obtain the corresponding official approvals, without which it will no longer be possible to sell vehicles in the EU in the future. The respective regulations are accompanied by corresponding industry standards which also need to be taken into account.

Until now, automotive manufacturers have not been directly subject to the strict IT security requirements of the Network Information Directive (NIS) and the **corresponding member state laws such as BSiG in Germany** (which incorporated aspects of the NIS Directive). However, as a result of the changes introduced by NIS-2 Directive and corresponding member state law automotive manufacturers will be subject to significantly more comprehensive technical and especially organizational requirements (including in the area of cyber governance, risk management and management liability), either as manufacturers or – depending on their service offering – as providers of certain regulated IT services.

Cyber Resilience Act (CRA) will introduce security requirements for a wide range of (connected) products with digital elements and networked software and supplements existing regulations with product related specifications (including the obligation to perform product-related cybersecurity risk assessments and documentation for products and third-party components). Similar to the AI Act and the Data Act, special regulations for the automotive environment are planned here, which will then take precedence over the CRA as a *lex specialis*. It is not yet clear exactly how the boundaries between the regulations will be drawn and which regulations will actually apply, for which function or product in the vehicle landscape (or not), as a more precise regulation by the EU is still pending. This is already creating certain uncertainties and questions in the implementation of the requirements in accordance with UNECE R155 (e.g. with regard to non- safety components of products or systems in the vehicle), which need to be clarified in a timely manner.

The revised **EU Product Liability Directive** has entered into force in December 2024 and enhances the liability of product manufacturers, importers and deployers for damage suffered by natural persons caused by defective products. This now also explicitly includes the liability for software and software-driven products and services which is now relevance for liability in the tech transformation in the automotive industry. The Directive follows a strict no-fault liability approach and includes comprehensive transparency and notification obligations, also in the online distribution of related products via platforms and market places including far reaching supplier and product screening requirements for platform and marketplace operators. For this reason, the specifications must always be observed in parallel as part of the implementation of the DSA in the platform environment (see details regarding DSA implementation above).

In addition, the EU Representative Actions Directive makes it easier for interest groups to enforce claims by affected consumers, which further increases the risk of collective enforcement and mass consumer actions which may give rise to more comprehensive enforcement activities in particular related to data breaches as have been seen in 2024 in the automotive industry on several occassions.

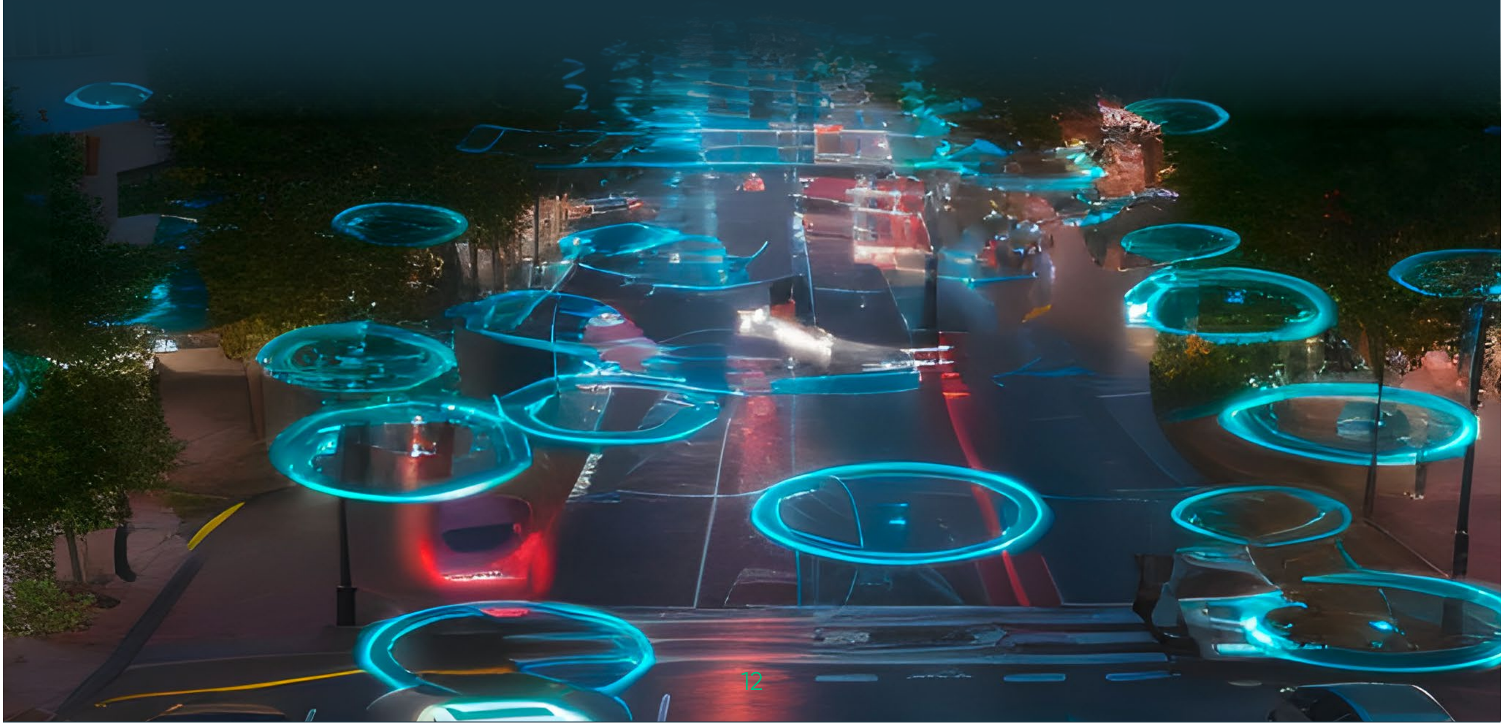
TaylorWessing

Telecommunications regulation

Connected vehicle manufacturers and service providers will continue to focus on **telecommunications law** in 2025. The legal framework (in Germany, the TKG (*Telekommunikationsgesetz*)/ TDDDG), has failed to clarify when connected vehicle services fall within the scope of application of telecommunication law standards. Statements by the competent authorities indicate that connected vehicle services are not always subject to the strict provisions of telecommunications law, especially if they are closely related to functions of the vehicle and do not constitute an additional telecommunication or telecommunication-supported service offered by the car manufacturer for a fee (services such as car WiFi). Being in scope brings a significant compliance burden so automobile manufacturers need to pay close attention to what the regulators are saying.

Law enforcement

Another development that will continue to concern connected car manufacturers in 2025 is the noticeable increase in requests they receive for data from **law enforcement authorities** in the context of criminal prosecutions. These have been increasing since the introduction of new rules in the TDDDG (q.v. § 21 ff. TDDDG). Businesses need to have processes and policies in place to ensure they deal with these requests appropriately.



International aspects

The strict requirements of the **GDPR for international data transfers** have presented global automotive manufacturers with major challenges since the CJEU ruling in the Schrems II case and the publication of the new EU Standard Contractual Clauses (SCCs). The growing number of correspondingly strict data protection laws in other countries of the world (including Brazil, Korea, etc.) further complicate the transfer of vehicle data in international corporate groups and joint ventures which also has far reaching effects on international collaboration based on data gathered in several parts of the world in the field of global R&D. Read more about the latest on international data transfers here. Even though the introduction of the Data Privacy Framework for data transfer to the US has eased the tension for OEMs in the EU a bit, international data transfers under GDPR remain a difficult topic. Data protection authorities have so far kept a low profile on data transfers to China. This may change soon, as the authorities are currwently dealing with with submissions of interest groups wich may likely put Chinese car manufacturers into the focus of authority practice.

Most recently, **China** has increasingly come to the attention of carmakers for another reason, not only as one of the most important sales markets, but also as one with strict requirements for the handling and export of vehicle data. The Chinese provisions on Car Data Security apply to a wide range of players in the automotive industry, from car manufacturers and suppliers to insurers, when they have to deal with relevant data. Unlike the GDPR, the scope of the regulations is not limited to the processing of personal data and includes the mere processing of data in the vehicle (without access by the OEM). These regulations are supplemented by a variety of new requirements, including those under the Personal Information Protection Law and other laws relating to cybersecurity and data localization.

As in many other industries, the question for connected vehicle businesses is what will emerge as the ‘gold standard’ privacy and data governance regime going forward. The GDPR could be overtaken. Data Act sets a new standard which is currently explored by business in the industry while it is unclear whether it has the potential to become a guideline for vehicle data access also in other markets. In terms of privacy regulations, China’s framework appears to go significantly beyond the European law requirements. It poses considerable practical and legal challenges for automotive manufacturers with business in China, especially since the actual requirements have not yet been fully specified by the authorities involved and impacted manufacturers will be kept busy during 2025. Read more on the changes in Chinese law and the consequences for automotive manufacturers.

Setting off in the right direction … also in 2025

Automotive manufacturers of connected vehicles and other stakeholders in the industry will be faced with major legal compliance challenges – also in 2025. Not only is a raft of new requirements coming in, but important questions remain unresolved which will likely require the intervention of regulators and the courts.

Key steps to be taken include:

Step 1

Analyze product and service portfolio to understand where the new laws will apply (and where not)

Step 2

Define requirements according to the new laws including by when they have to be met

Step 3

Make a plan on how to technically implement the requirements in a timely manner together with business teams, management as well as the legal & compliance team

Step 4

Get started - the timeline is short!

As is so often the case, preparation for compliance and early involvement of legal advisors (whether internal and / or external) is the key to ensuring the journey goes in the right direction from the start.

How we support our clients

With our team of automotive experts from all specialist areas we support our clients in implementing the obligations resulting from the new legal framework for companies in the automotive & mobility industry. We work with clients to analyze their business models, products and distribution channels to determine where, when and how existing concepts need to be adapted to the new requirements. We work with our clients to find practical solutions to best integrate the often complex regulatory requirements into existing concepts. We develop corresponding specifications in joint workshops, in which the company's specialist departments can also be involved, in order to jointly search for practical implementation options.

We would be pleased to support you and your team in this exciting project!

Feel free to contact us

Thomas Kahl
Co-Head Industry Group Automotive
Partner
Certified Specialist lawyer for Informationtechnology

t.kahl@taylorwessing.com

Dajin Lie
Salary Partner

d.lie@taylorwessing.com

TaylorWessing

2000+ people
1100+ lawyers
300+ partners
29 offices
17 jurisdictions

Austria	Klagenfurt | Vienna
Belgium	Brussels
China	Beijing | Hong Kong | Shanghai
Czech Republic	Brno | Prague
France	Paris
Germany	Berlin | Düsseldorf | Frankfurt | Hamburg | Munich
Hungary	Budapest
Netherlands	Amsterdam | Eindhoven
Poland	Warsaw
Republic of Ireland	Dublin
Slovakia	Bratislava
South Korea	Seoul*
UAE	Dubai
Ukraine	Kyiv
United Kingdom	Cambridge | Liverpool | London | London TechFocus
USA	New York | Silicon Valley

* In association with DR & AJU LLC