info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

DATA PROTECTION LAW IN THE AUTOMOTIVE INDUSTRY:
The GM/OnStar Case and Global Data Protection Legal Frameworks
CCPA, EU GDPR, UK GDPR Comparative Analysis

1. Background and Facts of the Case

On 8 May 2026, California Attorney General Rob Bonta, together with District Attorneys from San Francisco, Los Angeles, Napa, and Sonoma County, and with the support of the California Privacy Protection Agency (CalPrivacy), announced a $12.75 million settlement against General Motors (GM) and OnStar[1]. The settlement resolves allegations of violations of the California Consumer Privacy Act (CCPA), the Unfair Competition Law, and the False Advertising Law, and is pending court approval.

The Data Involved and the Data Flow:
OnStar is a connected vehicle service offered by GM that provides navigation assistance and contacts emergency services in the event of an incident (e.g., an accident). During the provision of the service, the vehicle continuously collects and transmits telematics data. According to the investigation, between 2020 and 2024 GM sold the following data of hundreds of thousands of California users to two major data brokers, LexisNexis and Verisk[2]:

- Precise geolocation data (real-time GPS coordinates)
- Hard braking and rapid acceleration events
- Speed limit violations
- Seatbelt usage
- Late-night driving habits
- Trip duration and start/end times

The data brokers resold this data to auto insurers, which used the resulting risk scores to raise insurance premiums. GM monetized data collected in the course of providing the service without the knowledge or consent of consumers, and used it for purposes incompatible with those disclosed at the time of collection[1,2].

Terms of the Settlement:
Subject to court approval, the settlement includes the following obligations[3]:

- Payment of a $12.75 million civil penalty
- Five-year prohibition: GM may not sell driving data to consumer reporting agencies, including LexisNexis and Verisk
- Stored driving data must be deleted within 180 days, unless the consumer has provided express affirmative consent

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

- GM must request LexisNexis and Verisk to delete the data received from GM
- Development and maintenance of a robust privacy program, under which the risks of data collection through OnStar must be documented and mitigated
- Submission of annual privacy assessments to the Attorney General, the relevant District Attorneys, and CalPrivacy, for a period of four years

GM earned nearly $20 million in revenue nationwide from the data-sharing agreements at issue in the case.

The $12.75 million penalty is the largest fine ever imposed under the CCPA, significantly exceeding the previous record of $2.75 million assessed against Disney in February 2026[4,5]

2. The CCPA Legal Framework and the Precedential Value of the Case

2.1. Data Minimisation as the Legal Basis for the Penalty

The most significant legal novelty of the case is that it is the first CCPA enforcement action in which authorities have expressly applied the data minimisation principle[6]. The CCPA was supplemented in 2023 by the California Privacy Rights Act (CPRA) amendments, which introduced proportionality and data minimisation requirements. Under these provisions, the collection, use, retention, and sharing of personal data must be reasonably necessary and proportionate to the purpose of collection, or to another disclosed and compatible purpose.

In the GM case, the authorities found that:

- GM retained data that was no longer necessary for the operation of OnStar
- GM subsequently sold the retained data for commercial purposes, contrary to the original collection purpose
- Consumers were not given adequate notice that their data was being sold to data brokers
- GM did not provide an opt-out mechanism prior to the sale of data

2.2. The Special Sensitivity of Location Data

The authority specifically highlighted in its announcement that vehicle location data reveals highly sensitive personal information: a person's home, workplace, their children's school, place of worship, and medical facilities[1]. The CCPA classifies precise geolocation data as sensitive personal information, subject to stricter processing rules.

2.3. Structural vs. Procedural Enforcement

Another notable feature of the case is the speed and structural nature of the enforcement. California did not merely impose a financial penalty but also prescribed immediate, operationally binding behavioural obligations. The five-year data sales prohibition, the deletion obligation, and the mandatory privacy programme will take effect shortly after court approval in contrast to European enforcement processes, where decisions can be mired in years of administrative and judicial proceedings.[7]

The effectiveness of enforcement depends not only on the size of the fine but also on mandatory behavioural obligations and their immediate enforceability. California leads most EU Member States in this regard

3. EU GDPR: The European Regulatory Model

3.1. Principles and Regulatory Architecture

The General Data Protection Regulation (GDPR), which has applied across the European Union since 25 May 2018, constitutes one of the most comprehensive data protection frameworks in the world[8]. Its key principles include data minimisation, purpose limitation, storage limitation and transparency.

3.2. The GM Case Through the Lens of EU GDPR

If the GM/OnStar case were assessed under the EU GDPR, the following violations would arise:

Absence of Legal Basis

The legal basis for selling data to data brokers would have been questionable under the EU GDPR. The original purpose of processing (navigation, emergency assistance) does not support the sale of data to third parties. Under the GDPR, the compatibility assessment must take into account the link between the purposes, the context in which the data was collected, the nature and sensitivity of the data, and the possible consequences for data subjects[9].

Special Categories of Data

Article 9 of the GDPR provides special protection for health data, data revealing religious beliefs, and other sensitive categories. Geolocation data that reveals a person's place of worship, healthcare provider, or political activities may qualify as special category data under GDPR interpretive practice. The European Data Protection Board (EDPB) guidance indicates that

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

precise location data deserves special treatment, particularly where it enables sensitive inferences to be drawn.

Data Protection Impact Assessment

Processing of personal data on this scale, in a systematic and large-scale manner, particularly involving sensitive data, would have required a mandatory data protection impact assessment (DPIA) under EU GDPR. Failure to carry out the DPIA constitutes an independent infringement.

3.3. Sanctioning Framework and Enforcement Challenges

The EU GDPR provides for two tiers of maximum fines depending on the severity of the infringement: for violations of basic provisions, up to EUR 10 million or 2% of global annual turnover (whichever is higher); for violations of the core principles of processing, data subject rights, and data transfer rules, up to EUR 20 million or 4% of global annual turnover (whichever is higher). In the case of GM, this maximum could theoretically amount to billions of euros if the turnover-based measure were applied.
However, one critically debated weakness of the EU GDPR enforcement system is the so-called 'one-stop-shop' mechanism and the lead supervisory authority model. In several major cases, particularly those involving Meta handled by the Irish Data Protection Commission (DPC), it took years before an enforceable decision was reached.

The EU GDPR's theoretical maximum sanction far exceeds the California fine, but in terms of the speed of practical enforcement and its direct operational impact, California currently proves stronger

3.4. CCPA vs. EU GDPR

CCPA (Kalifornia)

Jogalap modellje: Not a legal-basis model (unlike GDPR); opt-out right for sales and sharing; opt-in required for sensitive data and minors
Data Minimisation: Expressly required since 2023 (CPRA amendment); proportionality test for collection, use, retention, and sharing
Maximum Fine: $2,500 per negligent violation; $7,500 per intentional violation or violation involving a minor, cumulative per person and per transaction (in the GM case: $12.75M)
Enforcement: Joint jurisdiction of AG + CalPrivacy; swift settlements; operational obligations (prohibitions, deletion deadlines, compliance programme) immediately enforceable
Location Data Protection: Sensitive personal information; opt-in consent required for sale/sharing; particularly sensitive inferences (home, workplace, religion, health)

Data Brokers: Consumer opt-out right against sale; data brokers subject to registration and deletion obligations under CPRA; downstream liability throughout the entire chain

EU GDPR:

Jogalap modellje: Opt-in based: lawful basis required for all processing
Data Minimisation: Principle since 2018 (Article 5)
Maximum Fine: EUR 20M or 4% of turnover
Enforcement: National DPAs, slower process
Location Data Protection: Potentially special category, DPIA mandatory
Data Brokers: Joint controller / processor liability

4. UK GDPR - The Post-Brexit British Regulatory Model

4.1. The Specific Position of the UK GDPR

The United Kingdom has operated its own data protection regime since 1 January 2021. The UK GDPR is based on the text of the EU GDPR but incorporated into UK law and supplemented by the Data Protection Act 2018 (DPA 2018). The Information Commissioner's Office (ICO) supervises the application of the regime.
While the principles of the UK GDPR align with those of the EU GDPR, differences have emerged or are emerging in a number of areas:

- The Data (Use and Access) Act 2025 modernises the UK data protection regime, introducing a more flexible and business-friendly approach[10].
- The aim of the UK government is to reduce the rigidity of the EU GDPR while maintaining the adequacy relationship with the EU (the UK adequacy decision remains in force).

4.2. Assessment of the GM Case Under UK GDPR

The following assessment can be given under the UK GDPR:

Purpose Limitation and Data Minimisation
Article 5 of the UK GDPR also enshrines the principles of data minimisation and purpose limitation. The GM case, the sale for insurance purposes of data collected for a navigation service, would constitute a clear purpose limitation violation under the UK GDPR as well. Under ICO guidance, the use of data must be assessed in accordance with the reasonable expectations of the data subject[11].
Location Data and Sensitive Inferences

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

Based on Morrisons v Various Claimants and other UK judgments, the ICO is increasingly taking into account the inferences that can be drawn from data when assessing its sensitivity. Location data collected from autonomous and connected vehicles, which may reveal lifestyle, religious practice, and health status, can be considered data warranting special attention under the UK GDPR.

The ICO's Enforcement Capacity

The UK's data protection authority (ICO) initially indicated an intention to impose a GDPR fine of £183.39 million in relation to British Airways' 2018 data breach; however, in the final decision issued in October 2020, the fine was reduced to £20 million. One reason for the reduction was the impact of the COVID-19 pandemic on British Airways' financial situation[12]. The ICO's fining policy is less aggressive than that of certain EU Member States with Ireland being an exception, as the Irish DPC has been more restrained, whereas Luxembourg, the Netherlands, and France have been more active. Nevertheless, the ICO's strategic priorities include examination of data processing related to AI and connected technologies.

4.3. UK GDPR Specific Considerations

UK GDPR:

Legal Basis: UK GDPR + DPA 2018
Supervisory Authority: ICO (single authority)
Maximum Fine: £17.5M or 4% of turnover
Reform Direction: More flexible, business-friendly (2025 reform)
Data Brokers: Ugyanaz, mint EU GDPR

EU GDPR:

Legal Basis: EU GDPR (rendelet)
Supervisory Authority: National DPAs + EDPB
Maximum Fine: EUR 20M or 4% of turnover
Reform Direction: Stricter, fundamental rights-focused
Data Brokers Joint controller / processor system

5. Three-System Comparison and Sectoral Conclusions

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

5.1. Convergent Principles, Divergent Enforcement

It is striking that all three legal frameworks (the CCPA, the EU GDPR, and the UK GDPR) share the same core principles: purpose limitation, data minimisation, storage limitation, transparency, and the protection of data subject rights.
The difference lies not in the principles themselves, but in the mechanisms and speed of their enforcement.
California's strength lies in its direct, swift, and operationally binding enforcement. The EU GDPR's strength lies in its deterrent maximum sanctions and the consistency of its substantive law. The UK GDPR's strength lies in its unified supervisory authority and flexible law application, while its weakness is the uncertainty generated by the ongoing reform and its relatively restrained enforcement.

5.2. The Connected Vehicle Sector as a Test Environment

The connected vehicle case is particularly significant because this sector sits at the intersection of virtually every data protection principle:

- Large-scale, automated data collection (IoT)
- Sensitive data (location, behaviour, health inferences)
- Complex data flows (OEM → data broker → insurer)
- Asymmetric information (consumers were unaware of data sales)
- Cross-border data transfers

The GM/OnStar case sets a precedent not only in the automotive industry, but also in the fields of IoT, health technology, mobility platforms, AI-based profiling, and fintech.

5.3. Sector-Specific Considerations for Businesses

Based on the comparison of the three legal frameworks, the following priorities can be identified for regulatory risk management:

Purpose Limitation and Data Minimisation
A baseline requirement in all three systems. The GM case demonstrates that the 'collect now, use later' model, long applied by the tech industry as a proven business practice, is increasingly a source of legal risk. Businesses must define specific, documented purposes prior to collection and align their retention periods accordingly.

Location Data and Sensitive Profiling
Precise geolocation data requires heightened attention in all three systems. Under the EU GDPR and UK GDPR, a DPIA is mandatory where processing involves sensitive data or large-scale profiling. The CCPA requires opt-in consent for the sale of sensitive personal information.
Data Broker Relationships

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

The GM case highlights that the entire data broker chain carries legal risk. Under the EU GDPR and UK GDPR, joint controller agreements are mandatory, and processor contracts do not provide exemption from liability where the controller itself lacks a valid legal basis.

It is not sufficient to review internal data processing practices: the entire chain of data broker and third-party contracts must be assessed from a legal and compliance perspective

6. Conclusions and Recommendations

6.1. The Symbolic and Normative Significance of the GM Case

The GM/OnStar case is not merely a regulatory failure of one company: it is a symbolic milestone in the development of data protection law. It carries three messages for global businesses: data minimisation has finally become a genuinely enforceable principle; sensitive data, particularly location data, carries heightened risk and heightened protection obligations; and enforcement is strongest where authorities are proactive, swift, and capable of imposing structural obligations.

6.2. Regulatory Convergence and Divergence

The principles of the three systems examined (CCPA, EU GDPR, UK GDPR) are substantially convergent. For a globally operating business, this means it is advisable to apply a single, highest-level standard that satisfies the requirements of all three systems. The GDPR principles are generally the most stringent procedurally (mandatory legal basis, DPIA, DPO), while the operationally binding obligations of the CCPA deletion deadlines, prohibitions achieve an immediate and verifiable impact.

6.3. Recommendations for Businesses

We recommend the following for businesses involved in connected products, mobility services, telematics, IoT data, or AI-based profiling:

- Conduct a complete data flow mapping (data mapping), including data transferred to third parties
- Review retention periods: in the GM case, the legal issue was precisely unnecessary retention
- Assess the alignment between collection purposes and actual use
- Verify the legal compliance of data broker contracts
- Conduct a DPIA (EU/UK) or, for California, a risk assessment when processing sensitive data

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

- Update consumer notices to make clear who receives the data and for what purpose
- Establish opt-in processes for the sale of sensitive data and data transfers to brokers
- Monitor regulatory developments: the CCPA, EU GDPR, and UK GDPR are all continuously evolving

6.4. Outlook

The GM case is expected to have a ripple effect. Supervisory authorities in other Member States (particularly the more active European DPAs such as the Dutch AP, the French CNIL, or the Luxembourg CNPD) may bring similar cases against automotive manufacturers and IoT service providers operating within their jurisdictions. The European Data Protection Board is also examining data protection issues related to connected vehicles, which could lead to unified EU guidance.

Data protection is no longer merely a compliance matter: it has become a strategic risk management priority, the neglect of which, as the GM case demonstrates, carries direct financial and reputational consequences.

Data protection can become a competitive advantage: businesses that make data minimisation and transparency an integral part of their business model not only reduce their legal risks but also build consumer trust, which translates into a long-term market advantage.

This analysis is for informational purposes only and does not constitute legal advice

Sources

1. California Office of the Attorney General. (8 May 2026). *"When It Comes to Data Privacy, Consumers Must Be in the Driver's Seat: Attorney General Bonta, Partners Secure $12.75 Million General Motors Privacy Settlement*
2. Los Angeles County District Attorney's Office. (8 May 2026). *"General Motors to Pay $12.75M to Settle California Consumer Protection Lawsuit Alleging Data Privacy Violations."*
3. White & Case LLP. (May 2026). *"California announces landmark US $12.75 million CCPA settlement with General Motors, the largest settlement to date."*
4. Hunton Andrews Kurth LLP. (May 2026). *"California AG Announces Record $12.75M Settlement with GM over CCPA Data Minimization and Purpose Limitation Violations."*
5. California Office of the Attorney General. (11 February 2026). *"California Won't Let It Go: Attorney General Bonta Announces $2.75 Million Settlement with Disney, Largest CCPA Settlement in California History."*

6. Akin Gump Strauss Hauer & Feld LLP. (May 2026). *"California Announces Largest CCPA Penalty to Date and First Data Minimization Enforcement Action."*
7. Clark Hill PLC. (May 2026). *"GM OnStar $12.75M CCPA Settlement Signals Compliance Shift."*
8. European Parliament and the Council. (27 April 2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR).* EUR-Lex CELEX: 32016R0679.
9. Privado AI. (May–June 2026). *"Largest CCPA Settlement Yet: What GM's $12.75M penalty changes about US privacy enforcement."*
10. Information Commissioner's Office (ICO). (2025). *"The Data Use and Access Act 2025 (DUAA) – what does it mean for organisations?"*
11. Information Commissioner's Office (ICO). *UK General Data Protection Regulation (UK GDPR) – official guidance.*
12. Penalty notice Section 155, Data Protection Act. British Airways plc (case ref.: COM0783542)