How Automotive Companies Should Respond to GDPR, CCPA, and other International Privacy Laws

Brief Overview

Following a range of notable data breaches at organizations such as Equifax and Cambridge Analytica, international blocs, countries and even individual U.S. states are stepping up to the plate with data privacy protection laws. As cars are quickly becoming "vehicles" for data collection as well as traveling, companies in the auto industry will need to ensure that they are storing their customers' geolocational travel information, biometric data, and payment information in ways that achieve compliance with pertinent data security laws. This whitepaper will go over the key U.S. and international regulations governing data security for automobile companies, along with steps and considerations they should account

for to ensure compliance.

The General Data Protection Regulation ('GDPR'), the European Unionregulation on data protection and privacy, which came into force in May 2018, is one of the most robust data protection laws in the world to date. It is applicable to all individuals within the European Union (EU) and the European Economic Area (EEA). It further applies to organizations outside the EU if they offer goods or services to, or monitor the behavior of, persons within the EU.

In the absence of a comprehensive federal privacy law in the U.S., the California Consumer Privacy Act of 2018 ('CCPA') that will take effect on January 1, 2020 is considered one of the most significant legislative privacy developments in the country.[1] According to a global law firm DLA Piper, the United States has hundreds of privacy and data security laws among its 50 states and territories for safeguarding data, disposal of data, and appropriate use of Social Security numbers among other things.

An Overview of Data Protection Laws Around the World[2]

COUNTRIES	KEY DATA PROTECTION LEGISLATION	SECTORS AND ISSUES COVERED	OTHER IMPORTANT PRIVACY AND DATA PROTECTION LAWS (Not an exhaustive list)	REGULATION & ENFORCEMENT STRENGTH
Australia	The Federal Privacy Act 1988 (Cth) (Privacy Act); Australian Privacy Principles	Private sector entities with an annual turnover of at least AU$3 million, and all Commonwealth Government and Australian Capital Territory Government agencies.	Information Privacy Act 2014 (Australian Capital Territory); Information Act 2002 (Northern Territory); Privacy and Personal Information Protection Act 1998 (New South Wales); Information Privacy Act 2009 (Queensland); Personal Information Protection Act 2004 (Tasmania); and Privacy and Data Protection Act 2014 (Victoria); Assistance and Access Act; Consumer Data Right (Draft Bill)	Extremely Strong
Canada	Personal Information Protection and Electronic Documents Act ('PIPEDA')	Consumer and employee personal information practices of organizations that are deemed to be a 'federal work, undertaking or business' Organizations who collect, use and disclose personal information in the course of a commercial activity which takes place within a province Inter provincial and international collection, use and disclosure of personal information	Personal Information Protection Act ('PIPA Alberta') Personal Information Protection Act ('PIPA BC') Personal Information Protection and Identity Theft Prevention Act ('PIPITPA') (not yet in force) An Act Respecting the Protection of Personal Information in the Private Sector ('Quebec Privacy Act'), (collectively, 'Canadian Privacy Statutes')	Extremely Strong
People's Republic of China (PRC)	The PRC Cybersecurity Law is the first national-level law to address cybersecurity and data privacy protection. Rules relating to personal data protection and data can be found across various laws and regulations.	Businesses in the banking, healthcare or securities sectors may be subject to industry-specific data protection regulations; and employee personal data is covered under employment laws.	The Decision on Strengthening Online Information Protection, effective from December 28, 2012 (Decision); National Standard of Information Security Technology – Guideline for Personal Information Protection within Information System for Public and Commercial Services, effective from February 1, 2013 (Guideline); National Standard of Information Security Technology – Personal Information Security Specification, effective from May 1, 2018 (PIS Specification)	Strong
Russia	Data Protection Act No. 152 FZ dated 27 July 2006 (DPA)	All personal data operators	Information Technologies and Information Protection Act No. 149 FZ dated 27 July 2006; Some provisions are also found in the Russian Constitution, international treaties and other specific laws e.g. Russian Labour Code contains provisions on the protection of employees' personal data.	Reasonable
Thailand[3]	The Personal Data Protection Act, B.E. 2562 (2019) ("PDPA") published in the Government Gazette on 27 May 2019.	The PDPA has extraterritorial applicability. Thus, data controllers and data processors both in and outside of Thailand could be subject to the PDPA.	--	The effect of the new legislation is yet to be seen.
India	Privacy has been upheld as a fundamental right by the Supreme Court of India in Justice K.S.Puttaswamy (Retd.) v. Union of India [Writ Petition No. 494/ 2012]. The Information Technology Act, 2000 (the Act) contains specific provisions intended to protect electronic data. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules)	Applies to bodies corporate and persons located in India.	--	Limited
United States	Several sector-specific and medium-specific national privacy or data security laws Hundreds of privacy and data security laws across 50 states and territories California has more than 25 state privacy and data security laws, including the California Consumer Privacy Act of 2018 (CCPA), effective January 1, 2020	Applies to Financial institutions, telecommunications companies, personal health information, credit report information, children's information, telemarketing and direct marketing	A comprehensive national privacy law may be enacted to supersede and preempt state privacy laws in the future.	Extremely Strong

As illustrated in the chart above, several countries around the world are in the process of passing significant privacy laws and some others have firm data protection legislation already in place.

Australia regulates data privacy and protection through a combination of federal, state and territory laws. The Federal Privacy Act 1988 (Cth) and its Australian Privacy Principles (APPs) take under its purview private sector entities with an annual turnover of at least AU$3 million ($2.1 million), and all Commonwealth Government and Australian Capital Territory Government agencies.[4] The United States has an extremely strong US privacy law, however, it is a complex mix of national privacy laws and regulations that address particular issues or sectors. There are also state laws that further address privacy and security of personal information, and federal and state prohibitions against unfair or deceptive business practices. Canada has 28 federal, provincial and territorial privacy statutes that govern the protection of personal information in the private, public and health sectors.[5] PRC, Russia, Thailand, and India are some of the other countries on the chart with varied strengths of data privacy laws and geographical reach.

How Does This Impact the Auto Industry?

In the sphere of mobility, data is the nucleus of the continuing evolution of automotive technology. With the market shifting from driver controlled to completely autonomous driverless cars there has been a steep rise in collection, usage, and disclosure of vast amounts of information about the car and its passengers.

Just an hour of driving an autonomous car will churn out 4,000 GB of data per day

According to Intel, an hour of driving could churn out 4,000 GB of data per day

most of which would be personal data.[6] Thus, data has been deemed the next oil.

To safeguard this huge expanse of personal information the car manufacturers and service providers are now required by law to conform to the GDPR.

Liability and consequences of non-compliance:

'Controllers' and 'processors' who process personal data on behalf of controllers and under the direction of controllers are responsible for complying with the obligations under the GDPR as are 'businesses' pursuant to the CCPA.

Under the GDPR, data subjects can bring an action against processors and claim damages for "material or immaterial damage" suffered as a result of an infringement of the processor obligations. In case of misuse of personal information, a service provider is liable for civil penalties under the CCPA.[7]

In case of breach of regulation under the GDPR, the manufacturer can be fined up to €10 million ($11.3 million), or 2% of the car manufacturers' total worldwide annual turnover, whichever is higher.[8]

In April 2019, the Czech Data Protection Authority (UOOU) imposed a fine of €1,165 ($1,325) on a rental car company. One of the rental cars was being tracked via GPS by the renting company even though there was no information provided on the fact that the car was being tracked to the person who had rented the car. This was in violation of Art. 5 (1) (a) GDPR, which provides that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').[9]

In 2018, the Austrian Data Protection Authority imposed a fine of €300 ($341) on a private car owner for unlawful use of a dashcam. It was a camera recording the use of a car from the driver's point of view, which is illegal under the General Data Protection Regulation (DSGVO).[10]

It should be noted that according to the GDPR data generated in a vehicle is the property of the driver. This clarification of ownership puts a significant data privacy compliance burden on car manufacturers, rental car companies and fleet operators.

What Should the Car Manufacturers Do?

- **Protect against data thefts and privacy leaks:** The car manufacturers must design products and services with privacy and security in mind to protect the customers from cyber-attacks, data loss and privacy leaks. Auto industries must ensure that data from a connected vehicle does not fall in the hands of the new owner of the car. Identity thefts and data privacy breaches in second-hand vehicles are not unusual. Even a single hack has the potential to cause grave harm. In February 2018, a cyber-attack on a contractor's data servers compromised the personal information of over 28,700 Porsche customers in Japan.[11] Robust processes must be established to prevent data from being lost, corrupted or leaked and any breach should be notified to the right authorities within 72 hours of detection. Under the GDPR data processors must notify the controller of any data breach without undue delay. Individuals must also be informed at the earliest if the breach poses a substantial risk to the individuals' rights and freedoms. To facilitate decision-making on these aspects there should be an investigation and internal reporting procedure in place.

In February 2018, a cyber-attack on a contractor's data servers compromised the personal information of over 28,700 Porsche customers

in Japan.

- **Maintain transparency:** The vehicle owners should be clearly informed about their data and the ways in which the manufacturer can access it. The companies must maintain transparency with regard to the data collected, the purpose behind taking the data, and allow the owners to restrict such access if needed.
- **Take express consent:** GDPR requires the data controllers to process personal information lawfully with the subject's express consent.
- **Effectuate written contract with service providers:** There should be a detailed contract between controllers and processors of data, laying out the mandate given to processors and other terms of the controller-processor relationship. Similarly, under the CCPA personal information should not be disclosed to service providers without a written contract.
- **Extend right to portability and erasure to customers:** The law also requires companies to extend the 'right to portability' and the 'right to erasure' to the customers. This means customers should be able to transfer information between services and delete personally identifiable information when needed.
- **Maintain data activity log:** Some of the other obligations imposed on processors under the GDPR state that they must keep a record of data processing activities, implement appropriate technical and organisational measures, undertake data protection impact assessments prior to the processing, and appoint a Data Protection Officer.

To avoid any regulation breaches, it would be in the best interest of all businesses with a global footprint to have a defined roadmap for data protection and data privacy compliance.

LegalEase Solutions offers corporate legal departments and law firms innovative support with regulatory compliance, Contract Lifecycle Management, legal analytics, and legal research and writing. Our team is designed to function as an extension to your legal practice/department, providing you the capabilities and resources to stay up to date with your needs. If you have a project you need a

hand with, feel free to reach out to us at contact@legaleasesolutions.com. Our team is happy to assist.

[1] Comparing privacy laws: GDPR vs CCPA by Data Guidance: https://www.dataguidance.com/rep-ccpavgdpr/

[2] Data sourced from https://www.dlapiperdataprotection.com/

[3] https://www.bakermckenzie.com/en/insight/publications/2019/05/thailand-personal-data-protection-act

[4] https://www.dlapiperdataprotection.com/?t=law&c=AU

[5] https://www.dlapiperdataprotection.com/?t=law&c=CA

[6] https://www.networkworld.com/article/3147892/one-autonomous-car-will-use-4000-gb-of-dataday.html

[7] https://www.dataguidance.com/rep-ccpavgdpr/

[8] https://www.automotive-iq.com/autonomous-drive/articles/mobility-and-the-gdpr-an-important-but-uneasy-partnership

[9] http://www.enforcementtracker.com/

[10] https://www.derstandard.de/story/2000092017999/erst-vier-strafen-wegen-dsgvo-seit-mai