GDPR and Connected Car Data Privacy

The European Union's (EU) General Data Protection Regulation (GDPR) requires companies and organizations operating within the EU to strengthen their data protection and gives consumers control over how their data is used and shared. Similar regulations are making their way to the US and other countries as major automotive companies will soon possess huge amounts of consumer data from connected cars.

Communication

Consent

Access

Warnings

Erase Data

Profiling

Sensitive Data

Marketing

Data Transfer

As far back as the 1940's, librarians and researchers were aware that they would eventually collect huge amounts of information as society and technology continued to develop and evolve.

1940's

1997

In 1997 the term "big data" emerged and the dominant issue was data storage. This problem has largely been solved thanks to data storage scalability in the cloud.

98% of new vehicles will be connected to the Internet by 2020, and a subset of those vehicles will be enabled to transmit data to the cloud for advanced analytics.

2020

2030

Valuable revenue streams from connected car data could surpass $750 billion by 2030 providing automakers and ecosystem partners with valuable new business opportunities.

Automakers can leverage data and analytics to improve vehicle performance and services leading to enhanced consumer driving experiences and brand loyalty.

The more transparent companies can be about how they are using and protecting consumer data the more likely consumers will be to consent to sharing their data.

Four Tenants of Automotive Data Collection

Security

Ensure appropriate security measures are in place to protect personal data for the entire data lifecycle. This requires the adoption and adherence to reputable data practices that stretch across an organization. Organizations must look closely at data confidentiality, data integrity, and data availability.

Privacy

Data privacy is a branch of data security but needs to be treated as its own separate requirement due to its breadth. Data privacy concerns are focused on how data is handled, that proper consumer consent has been given, and that all regulatory obligations have been met.

Transparency

Organizations must establish a formal and lawful basis for collecting consumer personal data and be fully accountable at all times for answering what data was collected, why it was collected, where it was stored, who it was shared with, and when it was deleted.

Accountability

Take responsibility for what the organization does with data and ensuring compliance with applicable government regulations and standards for consumer data protection. Then, ensure the data collected is accurate before using it and taking actions to identify and erase incorrect or invalid data.

Corporate Headquarters 1191 Second Avenue | Suite 1900 | Seattle, WA 98101

Web www.airbiquity.com **Email** contact@airbiquity.com **Phone** +1 206 219 2700

Airbiquity®