

YOUR DATA, YOUR RIGHTS: NAVIGATING PRIVACY LAWS IN THE DIGITAL WORLD

DEPARTMENT OF AVIATION INFORMATION SECURITY UPDATE

Data privacy is more important than ever in today's highly digital aviation industry. From online booking systems to digital passenger records, airlines, airports, and related service providers collect, process, and store a vast amount of personal information. Whether it's flight information, passport data, or travel preferences, passengers entrust aviation companies with sensitive data, and it is crucial to understand the privacy laws that protect it.

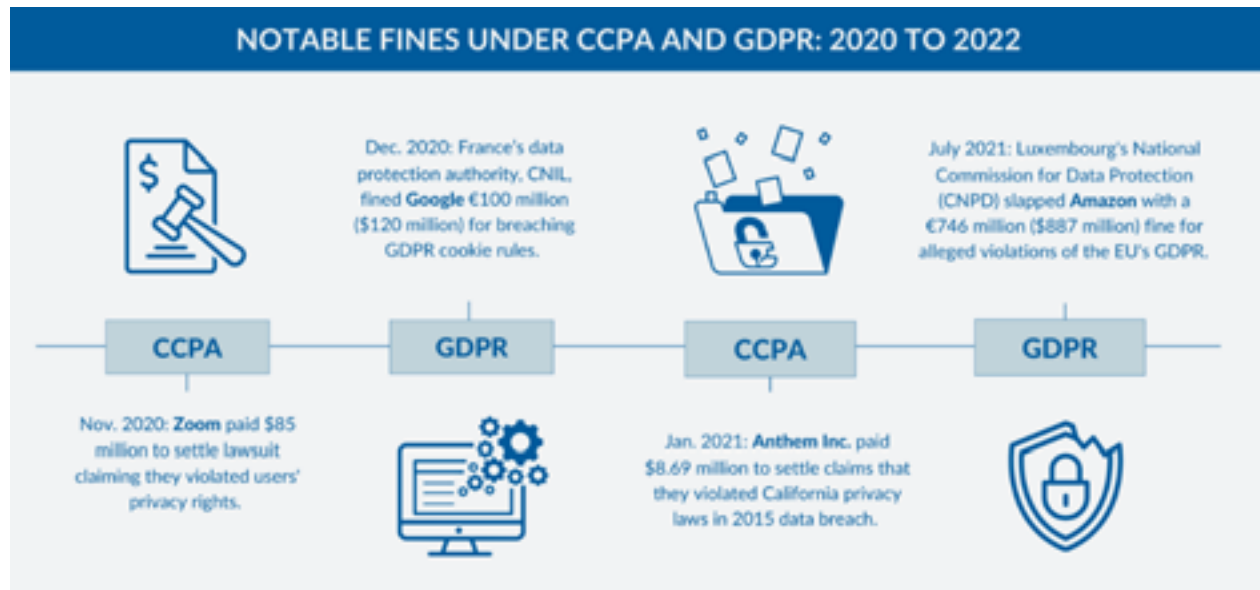
In regions like the European Union, the General Data Protection Regulation (GDPR) gives passengers the right to know how their personal information is used, stored, and shared. Similar laws, like the California Consumer Privacy Act (CCPA) in the United States, allow passengers to access and control their data, ensuring greater transparency. These regulations empower passengers by allowing them to request data access, make corrections, or delete their information.

CCPA		GDPR
JANUARY 1, 2020 Enforcement begins July 1, 2020	WHEN DOES THE LAW GO INTO EFFECT?	MAY 25, 2018 Enforcement in effect
FOR-PROFIT COMPANIES THAT: <ul style="list-style-type: none">• Collect personal data on 50K+ California residents• Have annual revenues of over \$25 million• Earn 50%+ of annual revenue from California residents' data	WHAT ORGANIZATIONS ARE IN SCOPE?	ANY ORGANIZATION THAT: <ul style="list-style-type: none">• Operates inside or outside the European Union (EU) and offers goods or services to customers or businesses in the union
<ul style="list-style-type: none">• Business, service providers, third parties, and California consumers	WHO IS AFFECTED?	<ul style="list-style-type: none">• EU citizens, businesses, controller, processor, and data subjects
<ul style="list-style-type: none">• Personal data that is sold for monetary or other value considerations (releasing, disclosing, transferring, or even renting of the data)	WHAT DATA IS WITHIN SCOPE?	<ul style="list-style-type: none">• Personal data of any type
<ul style="list-style-type: none">• Up to \$7,500 per violation with no ceiling on the number of violations• \$100-\$750 per consumer per incident for statutory damages related to breaches	WHAT ARE THE FINES OF NONCOMPLIANCE?	<ul style="list-style-type: none">• Up to 20 million euros or 4% of total global turnover from the prior fiscal year for the most severe violations• Up to 10 million euros or 2% of the worldwide annual revenue of the prior fiscal year for less severe violations

In aviation, data privacy concerns range from the personal details passengers provide when booking a flight to the biometric data used in modern boarding processes. Companies must stay transparent about how this information is used and give the passengers control over their data. Passengers must know their rights and the privacy policies of the airlines and airports they engage with to ensure their data is managed responsibly.

Staying Compliant: What You Need to Know About Data Privacy Regulations

Staying compliant with data privacy regulations is critical for aviation companies. Stringent global privacy laws like GDPR, the CCPA, and others challenge airlines and airports to protect vast amounts of passenger data. Non-compliance can result in hefty fines, loss of customer trust, and reputational damage, making data privacy a top priority.



To ensure compliance, aviation companies must implement robust data privacy practices. This begins with conducting regular data audits to assess what passenger information is collected, how it's stored, and how it's shared. Whether handling passport numbers, flight details, or credit card information, aviation companies must ensure this data is protected and used lawfully.

Airlines and airports should have clear privacy policies that explain how passenger data is collected and used, and these policies must be communicated effectively to passengers. Additionally, obtaining proper consent for collecting personal data is key to compliance. Whether it's collecting data for loyalty programs or biometric boarding systems, passengers should be informed and given the option to opt in or out.

Cybersecurity is also critical for safeguarding passenger data. Airlines and airports must invest in modern security measures to prevent data breaches and comply with timely breach reporting regulations. The aviation industry must stay vigilant and proactive in protecting passenger privacy to build trust and comply with evolving global data privacy laws.

By adhering to these practices, PHL can protect passengers' personal data, avoid penalties, and foster a reputation of trustworthiness in an increasingly digital world.