GDPR Implications for the Travel Industry

Kishan Bhandarkar, Chief Architect, CTO Group

The Experiential Travel Paradigm

The travel and transportation services industry has grown by leaps and bounds in the last decade. The growth, simply put, is a reflection of the paradigm shift the industry has witnessed. It also brings to light how consumers and providers have leveraged technology to their advantage, making every experience more reliable and effortless. Not to mention, innovative.

For instance, services like 'Kayak' and 'Hipmunk' have today built a merchandised approach to travel, that simply puts everything under one roof; be it flights, hotels, car rentals or restaurants, to name a few. Add to it, the rise of services like 'Airbnb' and 'Uber' that have created unconventional marketplaces for travel services, unheard of before.

The Underlying Support Structure

A meticulous analysis or scrutiny, brings to the fore the significance of large data, especially in this industry. Upon close inspection, it is revealed that the intuitive services offered by brands to a potential customer in future, are simply a result of the data collected from an existing customer. For example, Uber, primarily depends on a user's location data to bridge the gap between the driver and the passenger, thereby enabling the most efficient connection. Similarly, a car rental company, in order to update the local inventory, will heavily rely on the customer's location data which helps them determine the time of the customer returning the vehicle. Thus, making it available for a prospect looking for a car, when required.

The Data-Driven Economy

The growth of industries and brands has paved the way for fierce but healthy competition among travel companies. Truth be told, data has emerged as the most significant component, enabling businesses to evolve through their features and capabilities. More so, companies have collected enormous amounts of data which cover both, an individual's personal as well as behavioural attributes. The data collected includes location data, browsing patterns, shopping behaviour, frequently visited sites and other such pertinent information.

While data, its importance and the source of information can act as a springboard in taking customer experience to the next level, it can also pose a threat.

Data posing a threat

Securing enormous amount of personal data, especially when it does not have any uniformity, is a big challenge. With the non-uniform approach of collating data and the constant threat of breach by unsavoury actors, several government entities have enacted or are contemplating the introduction of various laws, aimed at bringing a semblance towards securing personal data. These laws focus primarily around holding organisations accountable for lawful collection and processing of valuable data. One such law that has been in the news lately is General Data Protection Regulation (GDPR).

The GDPR is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU[1].

1. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

What are the Implications of GDPR for Travel Companies?

Compliance

With the enforcement of General Data Protection Regulation, any travel or transportation services provider collecting or processing data about an European Union(EU) subject, immediately becomes eligible for compliance. This means, travel organizations irrespective of the geography of incorporation, will need to adhere to the regulations and remain compliant as long as they continue to collect or process data on EU subjects.

As travel industry is inherently global in nature, travel organizations need to be extremely careful on this front due to the constant flux of travelers across the world.

Transparency

The GDPR compliance brings in a new level of transparency which previously was missing. Organizations collecting and processing the data of EU subjects are now required to gain explicit consent in unbundled and unambiguous terms from the data subjects. Additionally, organizations must communicate the intent for collecting the data and details of the data processors they share the data with, under the terms of the consent. It is further required by the regulation for all compliant organizations, to report any form of data breach within 72 hours of being detected to all the parties concerned.

Security

The GDPR explicitly promotes 'privacy by design' and hence, it becomes imperative for travel organizations to secure the access, storage and exchange of customer data across organizational boundaries. It also becomes important for them to carry out periodic security audits to ensure relevant controls are working as intended. These controls include tools, people and processes required to secure the data, both at rest and in motion.

Portability

The GDPR came into force as of 25th May 2018. Which means, travel companies can now expect requests from travelers for downloads of their own data as well as requests to delete the data previously collected. Revocation of consent is now plausible and hence, it is in the best interest of organizations to consolidate the customer data into a minimum set of replicas and keep it portable.

For example, a customer may request to see or download the data collected by a travel management company or an online travel agent (OTA) to either review or share as is with another travel partner. Providing such capabilities is now required as part of the GDPR compliance.

How Can Mindtree Help?

As a mature services organization, Mindtree understands the travel industry and is well-placed to implement relevant data strategies that bring you closer towards GDPR compliance. Here's how:

Minimize

With most enterprises engaged in collecting as many attributes of personal data as possible, due focus has to be applied on a succinct data minimization strategy. Mindtree can help you assess and consolidate your interfaces and channels, in order to minimize the overall customer data footprint. This in turn, improves the efficiency of controls and processes required to achieve the requirements of data portability.

Centralize

Data centralization is among the most common design strategies, to address GDPR compliance. Currently, enterprises have a lot of redundancies with regards to data collection. Data ownership and stewardship strategies are not clearly defined and data boundaries blend into each other. Mindtree excels in creating a centralized customer data repository, to host and serve customer personally identifiable information (PII) and their related interactions. Additionally, storing confidential data in a secure zone within the data platform also helps in minimizing the attack surface in the event of a breach.

Abstract

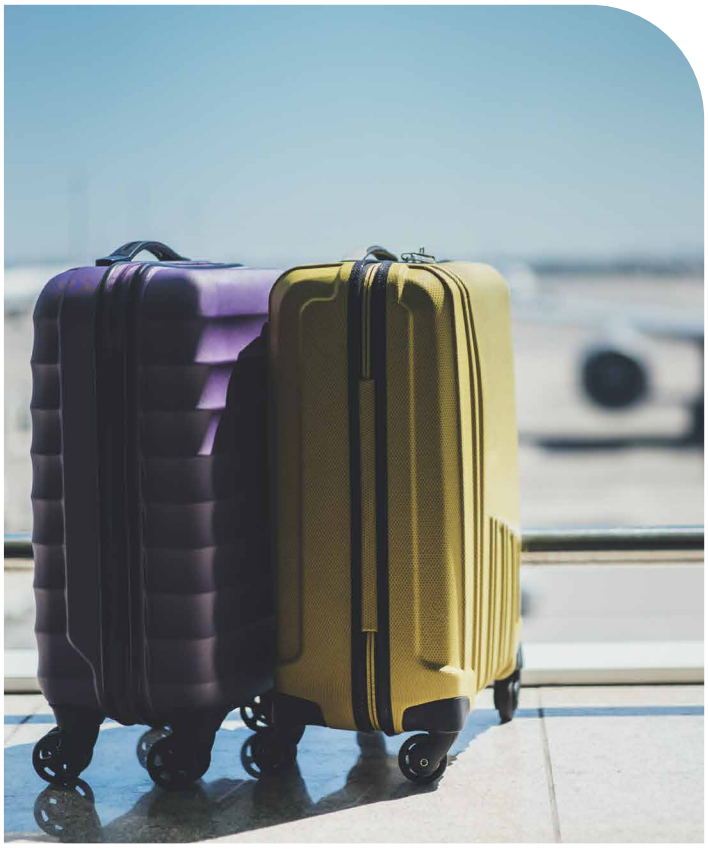
Data abstraction is particularly effective when sharing information with partners and external third parties for processing.

In the travel industry, airlines, travel agents, hotel chains or car rentals exchange a lot of traveler data over their partnership or loyalty programs. Strategies like implementing the usage of pseudonyms, surrogate keys, data masking and field level encryption can significantly improve the aspects of data protection when sharing confidential data with other travel companies like airlines, travel agents, and more. Additionally, GDPR actively encourages organizations to process data in a pseudo-anonymized form and relaxes enforcement on such processing to some extent. Mindtree can help to implement the best of breed, industry-standard security practices to mask confidential data within the enterprise boundary.

Secure

Data security being at the core of any enterprise data strategy, should influence all aspects of data platform design, including but not limited to, data at rest and data in motion. Therefore, data protection should be addressed at multiple layers including all enterprise databases, networks and storage hosting confidential customer information. Mindtree excels in implementing industry best practices like block-level encryption for storage, Transparent Data Encryption (TDE) for databases, OAuth/SAML token-based authentication and authorization strategies for APIs and transport layer security for enterprise endpoints.

In a nutshell, the above strategies should provide adequate levels of compliance when implemented correctly. Nonetheless, data security and governance policies / processes, must be constantly reviewed to continually ensure adequate levels of coverage and protection for confidential customer information.



Join us on a journey of data protection. Welcome to possible!

About the Author: Kishan Bhandarkar is the Chief Architect, CTO Group at Mindtree. He is a full-stack architect with over 18 years experience in the Technology space across industries. He is well versed in digital technology stacks such as Bigdata, Cloud, Web and Mobile with special focus on Blockchain-based solution architectures and enterprise integration techniques.