YOUR CHECKLIST FOR **GDPR** COMPLIANCE:

16 QUESTIONS

YOUR **TRAVEL BUSINESS** NEEDS TO BE ASKING **RIGHT NOW!**

On May 25, 2018, new General Data Protection Regulations (GDPR) approved by the EU Parliament takes effect. Designed to protect and empower EU citizens, GDPR unify laws that govern the handling of personal and financial information. It doesn't matter where your hotel or travel agency is located. If you process or store personally identifiable information (PII) such as name, date of birth, credit card, email, passport number and other sensitive data of any EU citizen, these regulations apply to you.

You can run from GDPR, but you can't hide. Those flagged for non-compliance after the deadline passes will be subject to significant penalties. These punishments are meant to hurt, with fines of up to 4% of annual global turnover or €20 million depending on the severity of the infraction.

If you're having trouble understanding GDPR or worried your organization isn't ready, have no fear. We've created this assessment to help you focus on the key takeaways of the regulations and what you need to do to ensure compliance.

Take the first step toward protecting your business's assets, customers and reputation by asking yourself the following 16 questions.

1

Do you have a method for handling credit cards and PII in a secure, GDPR, PCI-complaint format?

If your business manually executes transactions over the phone, by email, non-secure website or fax transmission, chances are you're not complaint.

2

Does your company have a Data Protection Officer (DPO) or need to appoint one?

GDPR mandates controllers or processors whose primary function involves processing operations must have a DPO in charge of monitoring compliance. A DPO can be an existing staff member or external service provider.

3

Do you have a clear and transparent policy about processing PII and acquiring consent?

Individuals have the right to not only approve access to their data but to also know exactly how you are using it and what you are using it for. Long, illegible terms and incomprehensible legalese must be replaced with simplified rules of consent presented in clear, easy to understand language.

4

Is your company equipped to detect a data breach and alert it to the authorities?

GDPR make it necessary to report a breach within 72 hours of becoming aware it has occurred. Lack of technological capabilities is not an excuse for letting an incident that threatens the PII of your customers go unnoticed.

5

Do you have a secure structure for data flow and storage of sensitive personal and financial information?

This includes ensuring data remains secure during transmissions within your system and to 3rd party partners and applications.

6

Are you able to control access to data and prevent unauthorized use?

You're business is accountable for who is able to enter systems and view information using appropriate credentials and authorization technology.

7

Do you understand the concept of Privacy By Design, and are you equipped to meet legal requirements established with GDPR?

This involves designing systems from the onset to protect data and and/or taking appropriate steps through technology and internal processes to keep data subjects safe.

8

Are you able to promptly comply with customer requests to account for their personal data and permanently delete it from your system?

GDPR grants customers the Right to Access as well as the Right to be Forgotten. If an individual requests records regarding their PII or for to be purged from your system, you must be able to comply in a timely manner.

9

Can your company account for and continually audit and asses all systems and processes for handling, transmitting and storing sensitive customer data?

"We didn't know" or "that doesn't belong to us" isn't a valid excuse. If you are using systems that aren't secure, or a member of your team is manually taking credit card payments, you're running the risk of GDPI penalties.

10

Do you have a secure system for transmitting and sharing relevant PII from your PMS or GDS with third-party companies?

You'll need to ensure a process for transferring personal data to vendors and applications that's validated to meet GDPR standards. If data shared with an outside entity is compromised, your business will also be held responsible.

11

Are you only collecting the information of customers that is absolutely essential?

Collection limitations state data must be obtained fairly and legally with the knowledge and consent of the individual.

12

Is PII you store accurate and complete?

New regulations make businesses responsible to ensure personal information is frequently periodically reviewed and kept up-to-date.

13

Is data you keep on file encrypted for an additional layer of safety?

You are required to protect the data you're storing whether it's on the Cloud, in your electronic systems, on a backup server, disks, USB or external hard drive.

14

If you're company generates aggregate data sets, are you sure the information is free of personal identifiers?

In an age of analytics and big data, GDPR raises the standards for ensuring collated statistical information can't be compromised to reveal the PII of individuals.

15

Are you prepared to take additional measures to acquire permission for controlling or processing data of individuals younger than 16-years-of-age?

Consent for handling the personal information of children must be granted by the parent or authorized legal guardian.

16

Have you established policies and procedures for proper data handling and conducting ongoing education and assessments?

You're required to provide the education and oversight to ensure your team is current on industry standards and best practices for keeping PII safe. GDPR is based on a set of principles rather than hard and fast rules to provide a framework for protecting the personal data of customers now and as technology and the risks continue to evolve.

Note: This list of questions is meant to serve as an unofficial self-assessment and make you aware of some of the most important aspects of GDPR. It is not endorsed or approved by any governing body nor is it meant to be a comprehensive or all-inclusive. For official GDPR information visit https://www.eugdpr.org

Follow us on

CAVEAU™
Your Personalized Card Vault