COMPLIANCE PARTNERS

GDPR FAQ

Find here the answers to some common questions about data protection!

1

What is GDPR, and why is it important for businesses?

GDPR, or the General Data Protection Regulation, is a comprehensive data privacy and protection law in the European Union. It's crucial for businesses as it establishes guidelines for the lawful and transparent processing of personal data. Compliance helps build trust with customers, avoids hefty fines, and ensures ethical handling of sensitive information.

2

Who does GDPR apply to?

GDPR applies to any organization that processes personal data of individuals within the EU, regardless of the organization's location. This includes businesses, nonprofits, and government agencies that collect, store, or process personal information of EU residents.

COMPLIANCE
PARTNERS

3

What rights do individuals have under GDPR?

Individuals, or data subjects, have several rights under GDPR, including the right to access their data, the right to be forgotten (data erasure), the right to data portability, and the right to know about and consent to the processing of their personal information.

4

What steps can businesses take to ensure GDPR compliance?

Businesses can ensure GDPR compliance by implementing robust cybersecurity measures, conducting regular risk assessments, obtaining clear consent for data processing, appointing a Data Protection Officer (DPO) if necessary, and staying informed about changes in regulations.

COMPLIANCE
PARTNERS

5

How can businesses prepare for a data breach in line with GDPR?

Preparedness for a data breach involves having an incident response plan in place, promptly notifying the relevant supervisory authority and affected individuals, conducting thorough investigations, and implementing measures to mitigate the impact. Businesses should also regularly test and update their breach response procedures.

6

What is a Data Protection Impact Assessment (DPIA), and when is it required under GDPR?

A DPIA is a systematic evaluation of the potential impact of a data processing operation on the protection of personal data. It is required under GDPR when a type of processing is likely to result in a high risk to individuals' rights and freedoms, such as large-scale processing of sensitive data.