

GDPR Compliance

GDPR Compliance: Protecting Personal Data in Europe



The General Data Protection Regulation (GDPR) is a comprehensive data protection law that gives individuals greater control over their personal data and imposes strict obligations on organizations that collect and process personal data of EU residents.

Key Principles of GDPR

- Lawfulness, fairness, and transparency: Data processing must have a legal basis and be transparent to data subjects.
- Purpose limitation: Data should be collected for specified, explicit, and legitimate purposes.
- Data minimization: Only the necessary data should be collected.
- Accuracy: Data must be accurate and kept up-to-date.
- Storage limitation: Data should be kept only for as long as necessary.
- Integrity and confidentiality: Data must be processed in a manner that ensures security.
- Accountability: Organizations are responsible for compliance.

Key Obligations for Organizations

- Data Protection Impact Assessment (DPIA): For high-risk processing activities.
- Data Subject Rights: Individuals have the right to access, rectify, erase, restrict, and object to processing, as well as data portability.
- Data Breaches: Must be reported to the supervisory authority within 72 hours.
- Privacy by Design and Default: Data protection should be integrated into systems and processes from the outset.
- Appointing a Data Protection Officer (DPO): In certain cases.
- International Data Transfers: Specific rules for transferring data outside the EU.

Penalties for Non-Compliance

Non-compliance with the GDPR can result in significant fines, up to €20 million or 4% of global annual revenue.

Challenges of GDPR Compliance

- Complex and Extensive: The GDPR is a complex regulation with numerous requirements.
- Evolving Landscape: The regulatory environment is constantly changing.
- Technological Challenges: Implementing technical measures to protect data can be challenging.
- Balancing Privacy and Business Needs: Striking the right balance can be difficult.

Best Practices for GDPR Compliance

- Conduct a Gap Analysis: Assess your current practices against GDPR requirements.
- Implement Data Protection by Design and Default: Integrate privacy into your systems and processes.
- Train Employees: Raise awareness of data protection obligations.
- Appoint a DPO (if necessary): Ensure you have the right resources.
- Monitor and Review: Continuously assess and improve your compliance efforts.



Cybersecurity Compliance Services

Learn More

GLBA DORA FCRA NIST
ISO 27001
GDPR
HIPAA SOX
PCI DSS
SOC2 AI ACT CCPA

The banner features a dark blue background with a world map. On the right, a shield-shaped graphic is composed of a network of glowing blue lines and dots. Various regulatory standards are labeled around the shield: GLBA, DORA, FCRA, NIST, ISO 27001, GDPR, HIPAA, SOX, PCI DSS, SOC2, AI ACT, and CCPA.

What's Next?

- ✓ Learn more about [ImmuniWeb Compliance Services](#).
- ✓ Read ImmuniWeb [Cyber Law and Cybercrime Investigation Blog](#).
- ✓ Join ImmuniWeb at the upcoming [Webinars](#) and [Events](#).
- ✓ Follow ImmuniWeb on [LinkedIn](#), [X \(Twitter\)](#), and [Telegram](#).
- ✓ Subscribe to ImmuniWeb [Newsletter](#).
- ✓ Try ImmuniWeb [Community Edition](#) Free Security Tests.
- ✓ See the benefits of ImmuniWeb [Partner Program](#).



The award-winning ImmuniWeb® AI Platform helps over 1,000 customers from over 50 countries to test, secure and protect their web and mobile applications, cloud and network infrastructure, to prevent supply chain attacks and data breaches, and to comply with regulatory requirements.



[API Penetration Testing](#)



[Continuous Automated Red Teaming](#)



[Dark Web Monitoring](#)



[Phishing Websites Takedown](#)



[API Security Scanning](#)














[Continuous Breach and Attack Simulation](#)



[Digital Brand Protection](#)



[Red Teaming Exercise](#)

- | | | | |
|---|--|---|---|
|  Attack Surface Management |  Continuous Penetration Testing |  Mobile Penetration Testing |  Third-Party Risk Management |
|  Cloud Penetration Testing |  Cyber Threat Intelligence |  Mobile Security Scanning |  Web Penetration Testing |
|  Cloud Security Posture Management |  Cybersecurity Compliance |  Network Security Assessment |  Web Security Scanning |

One Platform. All Needs.
www.immuniweb.com

.....
This document is provided "as is" without any warranty of any kind for informational purposes only.