GDPR Compliance Assessment
Spirent SecurityLabs

The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years—we’re here to make sure you’re prepared.

Index
1. Summary
2. Spirent Security Labs Solutions
   2.1. Article 25: Data protection by design and by default
   2.2. Article 32: GDPR Security of processing
   2.3. Article 33: Notification of a personal data breach to supervisory authority
       Article 34: Communication of a personal data breach to the data subject
   2.4. Article 35: GDPR Data protection impact assessment
3. About Us
   3.1. Team Credentials and Certifications
   3.2. Media and Publications
GDPR Compliance Assessment
Spirent SecurityLabs

1. Summary
Our team of experienced security experts will assess and help your organization achieve GDPR compliance to improve overall security and data protection. GDPR Assessment will assess network, applications & software for security of personal data and assesses organization’s Cyber Incidence response readiness.

GDPR Security Requirements:
• Section 1: General Obligations
  - Article 25: Data protection by design and by default
• Section 2: Security of personal data
  - Article 32: GDPR Security of processing
  - Article 33: Notification of a personal data breach to the supervisory authority
  - Article 34: Communication of a personal data breach to the data subject
• Section 3: Data protection impact assessment and prior consultation
  - Article 35: Data protection impact assessment

2. Spirent Security Labs Solutions

2.1 Article 25: Data protection by design and by default.
Data privacy by design—appropriate organizational and technical measures to ensure personal data security and privacy are embedded into the complete lifecycle of an organization’s products, services and procedures.
Data privacy by default—(a) only necessary personal data is collected, stored, or processed and (b) personal data is not accessible to an indefinite number of people.

Spirent SecurityLabs Solution: Security and Privacy Risk Assessment
• Identify critical data collection sources
• Review appropriate safeguards to protect personal data privacy in collection, processing, and storage
• Review limits and conditions on collection and usage of personal data
• Review of authorization rules for personal data usage and disclosures

2.2 Article 32: GDPR Security of processing.
• Encryption and pseudonymisation of personal data
• The ability to restore personal data availability in the event of a security incident or technical issue in a timely manner
• Ensuring ongoing confidentiality, integrity, and availability (the tenets of InfoSec) of data processing systems and services
• Establishing a process for regular security testing and assessment of the effectiveness of security practices and solutions in place

Spirent SecurityLabs Solution:
• Network and Application Assessment
  - Assessment of network and applications and any related hosts in critical areas such as:
    - Improper user data validation
      • Insecure cryptographic storage
      • Insecure communications
      • Improper error handling
      • Improper access control
      • Broken authentication and session management
    - Data policy compliance
    - Insecure Server Configuration
    - Default System Passwords
    - Unpatched systems
    - Known Vulnerabilities & Exploits
    - Insecure Firewall Configuration
    - Information Leakage
• Cryptographic Review
  - Thorough assessment of cryptographic hash functions, public-key cryptography, digital signature algorithms, key storage, authentication, authorization, communications protocols being used for data encryption and integrity.

• Database Security Review
  - Identify weaknesses and misconfigurations the data structures, logic, organization, storage formats, optimization and exposure and encryption of critical and sensitive data.

• Data Recovery Plan Review
  - Review of organization’s personal data recovery plan to ensure data recovery in a timely manner in an event of security incident or technical issue. This audit will focus on reviewing key components of the data recovery plan such as safeguarding data privacy, corporate assets and customer data while minimizing disruption to core business activities.

2.3 Article 33: Notification of a personal data breach to supervisory authority.

Data Controllers must notify the appropriate supervisory authority within 72 hours of becoming aware of a personal data breach. Notification, at a minimum, must describe the nature and consequences of the data breach, type and approximate number of affected Data Subjects and data records, remedial actions taken or proposed, and the name and contact information of person who can provide additional information.

Article 34: Communication of a personal data breach to the data subject.

If a data breach risks the rights and freedoms of the affected Data Subjects, then the Data Controller must, without undue delay, notify each affected person.

Spirent SecurityLabs Solution:
- Incident Response Readiness Assessment
  Unfortunately, in today’s world being compromised is not a matter of if but a matter of when. Swift reaction to signs of compromise and the correctness of the response can drastically limit the scope of the compromise.
  - Review of incidence response plan to ensure timely detection, reporting of incident, triaging, and responding in timely manner to the affected data subjects and appropriate supervisory authority.
  - Review network, system IDS, IPS, firewall and router logging process for signs of anomalous activity and communication to ensure regular event logging and monitoring activity.

2.4 Article 35: GDPR Data protection impact assessment.

Data Controllers must perform a Data Protection Impact Assessment (DPIA) whenever a new processing operation is proposed.

Spirent SecurityLabs Solution:
Penetration testing services provides Data Controller a threat model on the security impact of the newly proposed processing operation. Penetration test showcases the impact on the data compromise and exfiltration in an event of a successful security breach.
About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent’s customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information, visit: www.spirent.com

3 About Us

3.1 Team Credentials and Certifications.

- OSCP (Offensive Security Certified Professional)
- GXPN (GIAC Certified exploit researcher and advanced penetration tester) - License 478
- GPEN (GIAC Penetration Tester) - License 7854
- GICSP (Global Industrial Cyber Security Professional)
- NSA ISAM (NSA InfoSec Assessment Methodology Certification)
- CISSP (Certified Information Systems Security Professional) - License 376542, 434007
- CCENT (Cisco Certified Entry Networking Technician)
- CEH (Certified Ethical Hacker)
- CREST (CRT-PEN)
- Security+, Server+
- UCP (Unix Certified Programmer)
- MS Computer Science
- MS Electrical Engineering
- BS Computer Science
- BS Mechanical Engineering

3.2 Media and Publications.

- Spirent SecurityLabs Website: http://www.spirent.com/Global-Services/SecurityLabs
- Twitter: @SpirentSecurity
- Spirent Security Channel: https://www.youtube.com/channel/UCj4pLd3dUdl4p5w1Gcv-hmQ

Contact Us

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

www.spirent.com

© 2018 Spirent Communications, Inc. All of the company names and/or brand names and/or product names and/or logos referred to in this document, in particular the name “Spirent” and its logo device, are either registered trademarks or trademarks pending registration in accordance with relevant national laws. All rights reserved. Specifications subject to change without notice.

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

US Government & Defense
info@spirentfederal.com | spirentfederal.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

Rev B | 08/18