Information Security Best Practices and GDPR

Douglas Garrison - CISSP CCSP CISA PCI-QSA |
Security Consultant | Sirius
Objective

How do we use standard best practices in security to manage GDPR data securely and meet the compliance requirements?
What is Security?

What Security isn’t

- Compliance
- A Piece of Technology
- Risk Elimination

What Security is

- A Culture
- Risk Mitigation
- The Management of the People, Processes and Technology you have in a secure manner
- The Management of CIA
CIA – The Security Triad

**Confidentiality** - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

**Integrity** - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

**Availability** - Ensuring timely and reliable access to and use of information
What is GDPR?

The objective of the General Data Protection Regulation (GDPR) is to protect all European Union (EU) citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which its predecessor the 1995 Data Protection Directive 95/46/EC was established.
Key date and terms?

Approved: April 2016
Effective date: May 25th 2018

**Personal Data:** Any information related to a natural person or ‘Data Subject’, that can be used to directly or indirectly identify the person

**Data Controller:** entity that determines the purposes, conditions and means of the processing of personal data

**Data Processor:** entity that processes data on behalf of the Data Controller
Who is affected?

GDPR applies to all companies processing the Personal Data of subjects residing in the EU, regardless of the company’s location and regardless of whether the processing takes place in the EU. These rules apply to both Data Controllers and Data Processors of Personal Data; meaning cloud providers will not be exempt from GDPR enforcement.
Who should be involved?

Success with GDPR will be a joint project between Executives, Information Security, Information Technology and Legal. As with all security, compliance and privacy initiatives it is always better to build and maintain a proper security and privacy program rather than trying to chase compliance or laws - privacy and compliance are by-products of good security.
GDPR Requirement – Security of Processing and Privacy By Design

This is the implementation of Security Best Practices
Least Access\Least Privilege
Data Classification
Common Data Classification Labels

• Part of ISMS
  – ISO 2700X
  – NIST 800-53
  – NIST CSF
• Availability Requirements
• Encryption requirements
  – Data minimization
• Isolation and Storage
• Destruction requirements
• Movement
• Access controls
• Lifecycle
• Data subject rights
• Tools available
GDPR Requirement – Breach Notification

Security Best Practice = Breach Prevention - Breach Detection - Incident Response
GDPR Requirement – Vendor Management

Security Best Practice = Third Party Management
GDPR Requirement – Data Impact Assessments

Security Best Practice = Risk Management
GDPR Requirement – Right to Access – Data Portability - Right to be Forgotten

Security Best Practice = Data Classification and Management of CIA
Sirius Security and IBM

Providing consulting and integration services to help you establish and execute a security plan that fits your business.

Infrastructure
- Next-Generation Firewall
- Intrusion Detection & Prevention
- Micro-Segmentation
- Network Access Control
- IoT Security
- DDoS Protection
- Architecture & Design
- Remote Access

Data & Application
- Web Application Firewall
- Data Loss Prevention
- Secure Web Gateway
- Encryption
- Database
- Email
- Code Review/
  Application Scanning
- Data Classification

Intelligence & Analytics
- Security Information & Event Management
- User & Entity Behavior Analytics
- Network Analytics
- Sandboxing/Malware Analysis
- Threat Intelligence
- Digital Forensics/
  Incident Response
- Automation & Orchestration

Cloud
- Encryption
- Code Review/
  Application Scanning
- Threat Intelligence
- Automation & Orchestration

Threat & Vulnerability Management
- Endpoint Prevention,
  Detection & Response
- Vulnerability Management
- Patch & Configuration
  Management
- Penetration Testing
- Compromise Assessments
- Deception
- Security & Risk Monitoring

Identity & Access Management
- Core IAM Platform
- Multi-Factor, Risk-Based Authentication
- Single Sign-On
- Federation/Directory Integration
- Privileged Access Management
- Access Governance

Program Strategy & Operations
- Program Strategy & Development
- Governance, Risk & Compliance
- Third-Party Risk Management
- PCI QSA Services
- vCSO
- Security Awareness Training

AppScan Guardium
Qradar, i2 Resilient
MaaS360 BigFix
IG&A

www.siriuscom.com

10/19/2018
IBM Guardium

ANALYZE
Automatically discover critical data and uncover risk

PROTECT
Complete protection for sensitive data, including compliance automation

ADAPT
Seamlessly handle changes within your IT environment
IBM Resilient

**Security Module**
- Industry standard workflows (NIST, SANS)
- Threat intelligence feeds
- Organisational SOPs
- Community best practices

**Action Module**
- Automate processes
- Enrich incident details
- Gather forensics
- Enact mitigation

**Privacy Module**
- Global breach regulations
- Contractual obligations
- 3rd party requirements
- Organisational SOPs
- Privacy best practices

**Infrastructure Integration**
- Directory
- Endpoint forensics
- Threat intelligence
- Endpoint controls
- Network controls
References

• UK Information Commissioners Office (ICO)
• Center for Internet Security
• SANS
• NIST Special Publications
• Siriuscom.com
• IBM Guardium
• IBM Resilient
Questions?
Protect your data like your livelihood depends on it – because it does.

Thank You