Data Privacy and Protection
GDPR Compliance for Databases

Walo Weber, Senior Sales Engineer
September, 2016
Agenda

• GDPR: who, what, why, when
• Requirements for databases
  – Discovery
  – Classification
  – Masking
  – Monitoring
  – Audit reporting
  – Incident response and notification
• Getting Started
GDPR: GENERAL DATA PROTECTION REGULATION
REGULATION (EU) 2016/679
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
GDPR: who, what, when

A regulation with teeth
Who is subject to the regulation:
Entities that collect (Controller) or routinely process (Processor) data subjects’ personal data – regardless of the company location.
Record keeping derogations are in place for entities with fewer than 250 employees

What is subject to the regulation: Data Subject’s personal data, that originated in or is based on activity occurring in EU member states. Personal data is everything that identifies an individual.
Both EU residents and visitors are protected – including visitors to EU based web sites and mobile site users

When will the regulation REALLY be enforced:
The Regulation shall apply from 25 May 2018
Six data loss breaches are currently reported each day – primarily in the US. There will be plenty of EU test cases.

What are the fine levels:
Violations of Articles: 8,11, 25 to 39, 42 and 43
€10m or up to 2% worldwide annual turnover of proceeding year, whichever is higher
Violations of Articles: 5,6,7,9,12-22, 44-49, 58, and member state laws adopted under Chapter IX
€20m or up to 4% worldwide annual turnover of proceeding year, whichever is higher
## GDPR: Primary Database Security Requirements

<table>
<thead>
<tr>
<th>Article</th>
<th>Requirement for Database Security</th>
<th>Imperva Database Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>Data protection by design and data protection by default</td>
<td>Data minimization&lt;br&gt;User access limits&lt;br&gt;Limit period of storage and accessibility</td>
</tr>
<tr>
<td>32</td>
<td>Security of processing</td>
<td><em>(a) pseudonymisation and encryption&lt;br&gt;(b) Ongoing protection&lt;br&gt;(d) Regular testing and verification</em></td>
</tr>
<tr>
<td>33 and 34</td>
<td>Data breach notification</td>
<td>72 hour notification following discovery of data breach</td>
</tr>
<tr>
<td>35</td>
<td>Data protection impact assessment</td>
<td>Assessment of the purpose, scope and risk associated with processing private data</td>
</tr>
<tr>
<td>44</td>
<td>Data transfers to third country or international organization</td>
<td>Permit transfers only to entities in compliances with regulation</td>
</tr>
</tbody>
</table>
Requirements for databases

Bank robbers target the money vault
Hackers target the databases
Map Requirements To An Data Audit and Protection Lifecycle

Discover
- Sensitive data

Classify
- Classify and minimize private data

Set Controls
- Access rights and policies

Audit & Secure
- Monitor, alert and block

Measure & Report
- Review, certify and investigate
Data Protection Assessment

**Discovery & Classification**

- Discover DBs and classify private information
  - Discover active DB services
  - Identify rogue DBs
  - Sample data, auto-identify private data
  - Determine what needs to be monitored

- Intellectual Property
- Credit Cards
- SSN
- Rogue
- PII

SecureSphere DAS
Data Minimization: Anonymization / Pseudonymisation

Mask Private Data In Test, Training, and Reporting Databases

1. Realistic fictional data maintains operational and statistical accuracy
2. Sensitive data is permanently removed
3. Security and compliance overhead are reduced

### BEFORE

<table>
<thead>
<tr>
<th>Name</th>
<th>SSN</th>
<th>Salary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Müller</td>
<td>756-2121-9812-22</td>
<td>77,000</td>
</tr>
<tr>
<td>Bohren</td>
<td>756-4321-3421-23</td>
<td>83,500</td>
</tr>
</tbody>
</table>

### AFTER

<table>
<thead>
<tr>
<th>Name</th>
<th>SSN</th>
<th>Salary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schmidt</td>
<td>756-5167-5273-09</td>
<td>79,250</td>
</tr>
<tr>
<td>Billeter</td>
<td>756-7044-0492-93</td>
<td>81,250</td>
</tr>
</tbody>
</table>

Locating and replacing *sensitive data* with *realistic, fully-functioning, fictional data*
Data Minimization - Database Access

User Rights Analysis

Scan for granted user rights
- Eliminate unwarranted access
- Ensure business need-to-know
- Reduce risk of data breaches

Users ➔ Roles ➔ Privileges ➔ Objects

- SELECT
- UPDATE
- DELETE
- INSERT
Private Data Audit and Privileged User Activity Monitoring

**Activity Auditing**
- Collect and record database activity details
  - Satisfy compliance requirements
  - Conduct forensic analysis

**Privileged User Monitoring**
- Monitor privileged users
  - Enforce separation of duties
  - See all activity including local server access
  - Block if needed
A global electronic payment processor:
- DBAs around the world
- Building a new datacenter in Germany
- Needed to control access to EU/German PII and perform PII discovery

SecureSphere DAM/DBF:
- Prevent access to German PII to DBAs outside of the country

SecureSphere DAS:
- PII Discovery and Classification
Database Security

Alerting
Alert in real time on suspicious behavior
- Quickly identify attacks
- Prevent data theft

Blocking
Monitor database access
- Prevent unauthorized database access
- Secure sensitive data

Security Policy
Dynamic Profile

Network User, DBAs, Sys Admin

UPDATE orders set client 'first

Unusual Activity

Allow

Block

Dashboard
SYSLOG
Email

© 2016 Imperva, Inc. All rights reserved. Confidential
Measuring & Reporting

Reporting

Enterprise class reporting framework
- Analyze threats
- Accelerate compliance

Analytics

Examine detailed audit logs, interactive dashboard views, and reports
- Accelerate forensic analysis
- Simplify compliance

GDPR, PCI, BDSG, PDA...
Custom
Getting Started

Step 1: Account for 100% of the private data located in all databases and data marts
Visit imperva.com for GDPR information and tips

September 01, 2016

GDPR Compliance: How to get the ball rolling today?

The General Data Protection Regulation (GDPR) impacts every business in the European Union (EU) or doing business in the EU even if their headquarters are outside EU borders. The GDPR enforcement starts May 2018, giving ample time for enterprises to plan and implement the right controls. There are many elements in the GDPR directive. We recommend that enterprises put a plan in place to achieve certain milestones before the deadline, in order to avoid fines and possibly earn some goodwill from the EU. Compliance experts at Imperva have worked on the following framework to help customers navigate the data security and compliance technology requirements for compliance with the GDPR.

Stage 1: 0-6 months

Discover and inventory – of known and unknown data repositories and sensitive data
Data Protection Reference Architecture

Data → Assets

Machine Learning / User Behaviour Analysis

Cloud Access Security Broker

Managed & Unmanaged Devices

SaaS

Legitimate Traffic

Spammers

Hackers

DDoS

DDoS Mitigation

Cloud WAF

Web Servers

IaaS/PaaS

IMPERVA COUNTERBREACH

IMPERVA SECURESPHERE

WAF

Fraud & Business Logic Attacks

DAM & FAM

Auditing & Access Control
User Rights Management

Camouflage - Data Masking
Obfuscate Sensitive Data

Please refer to the full document for detailed information on each component.
CounterBreach: Enterprise Threat Intelligence Solution

Visibility into unusual data access patterns:
- Data theft
- Account abuse
- Data mishandling
- Suspicious activity

Behavior Analysis
anomaly detection engine

Internal Resources:
Databases & File Servers

External Resources:
Cloud Apps

Compromised
Careless
Malicious
Privileged
Data Breach Notification
Will you be ready if you wait?

• Within 72 hours of discovery
  – 2% of revenue or €10M fine for non-compliance
• Headline portrayal option
  – Denial or responsive and responsible

Be Ready – stop the breach
Avoid the fines and headlines
Meet Imperva at it-sa congress in Nürnberg

**it-sa – The IT Security Expo and Congress**

- Trends & innovations in the IT security sector
  18 – 20 October 2016
  Exhibition Centre Nuremberg
- Visit the Imperva Booth at Stand 412 and talk to Imperva experts and our partners
- Presentations in Forum Blue
  Schutz Ihrer unternehmenskritischen Daten und Applikationen
  - ob in der Cloud oder On-Premise
  18.10.2016, 15.45 and 20.10.2016, 11.15
- Get your free pass at
  https://www.imperva.com/Company/EventsIT_SA