OWASP AppSec EU Belfast

8th to 12th of May 2017

Waterfront Conference Center

Embedding GDPR into the SDLC

Sebastien Deleersnyder
Siebe De Roovere

Toreon

Who is Who?

Sebastien
Deleersnyder

TOREON

Siebe
De Roovere

- 5 years developer experience
- 15+ years information security experience
- Application security consultant Toreon

- Belgian OWASP chapter founder
- OWASP volunteer
- www.owasp.org

- 4 years Governance, Risk, Compliance (GRC) Information Security experience
  - Information Security (ISO27001 implementor)
  - Privacy (certified DPO)
- GRC security consultant at Toreon

- IAPP (international association of privacy professionals) member.
- https://iapp.org/

Agenda

- GDPR Introduction
- SDLC/SAMM Introduction
- Embedding GDPR into the SDLC
- Conclusions & Next Steps
- Q&A

GDPR

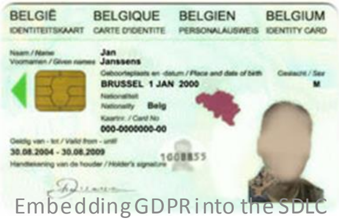
- General Data Protection **Regulation**
  - Directly applicable within EU + UK
  - 25th of may 2018

- Goals
  - Unification of Privacy Legislation
  - Improve **protection of personal data** and data subject rights

What is Personal Data?

Personal data is all information related to an identified or identifiable person ("data subject").

Card number, IP address, biometric, user id, email address, employee mobile phone traffic data, surf history, employee mailbox, …

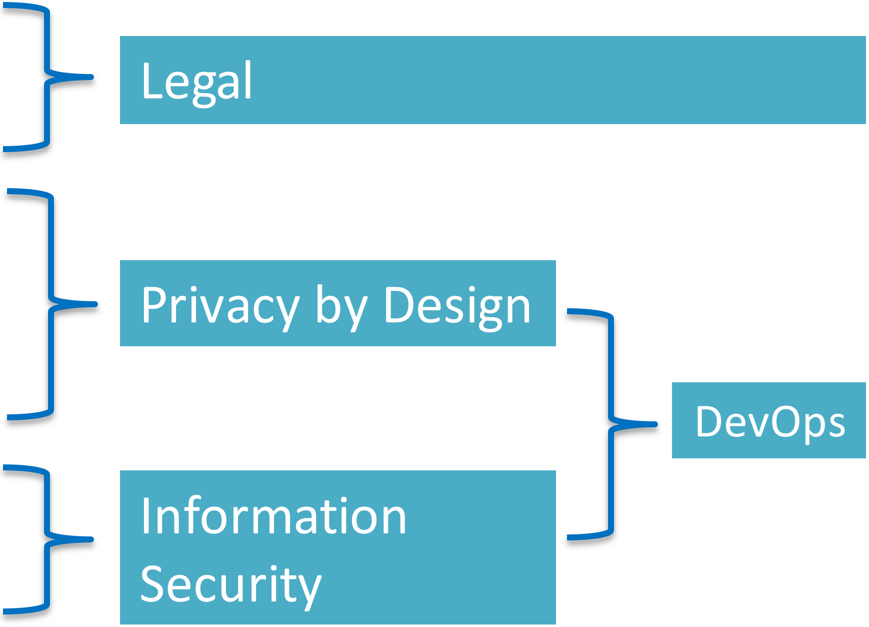


BELGIË IDENTITEITSKAART BELGIQUE CARTE D'IDENTITE BELGIEN PERSONALAUSWEIS BELGIUM IDENTITY CARD

Naam / Name Jan
Voornamen / Given names Janssens
Geboorteplaats en -datum / Place and date of birth BRUSSEL 1 JAN 2000
Geslacht / Sex M
Nationaliteit Nationality Belg
Kaartnr. / Card No 000-0000000-00
Geldig van - tot / Valid from - until 30.08.2004 - 30.08.2009
Handtekening van de houder / Holder's signature
1008855

GDPR – 7 Principles

- Justification
- Transparency
- Finality
- Proportionality
- Accuracy
- **Confidentiality**
- **Accountability**



Legal

Privacy by Design

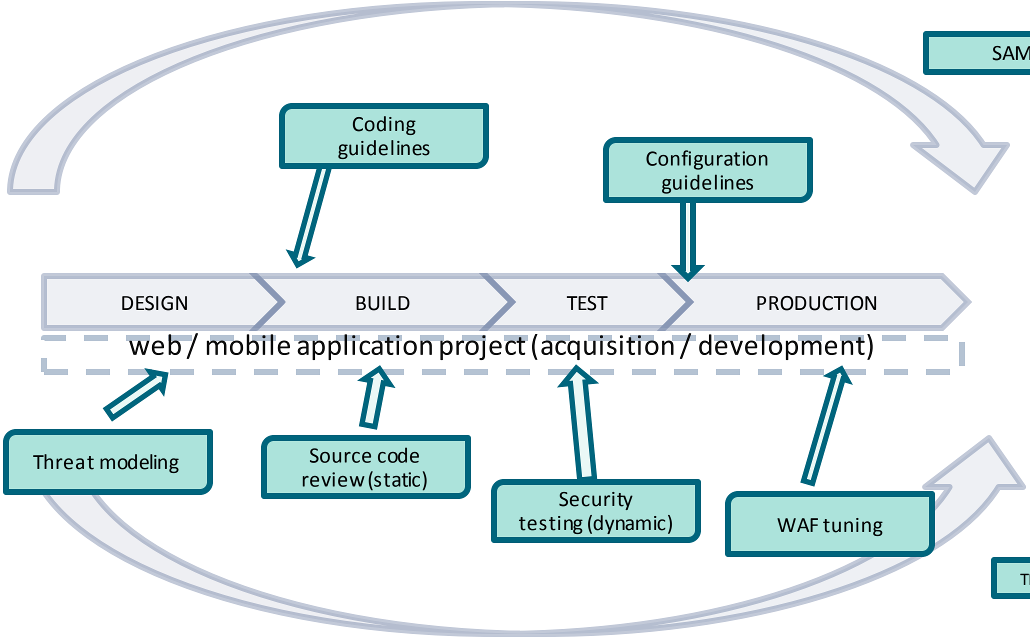
Information Security

DevOps

GDPR Secure Development

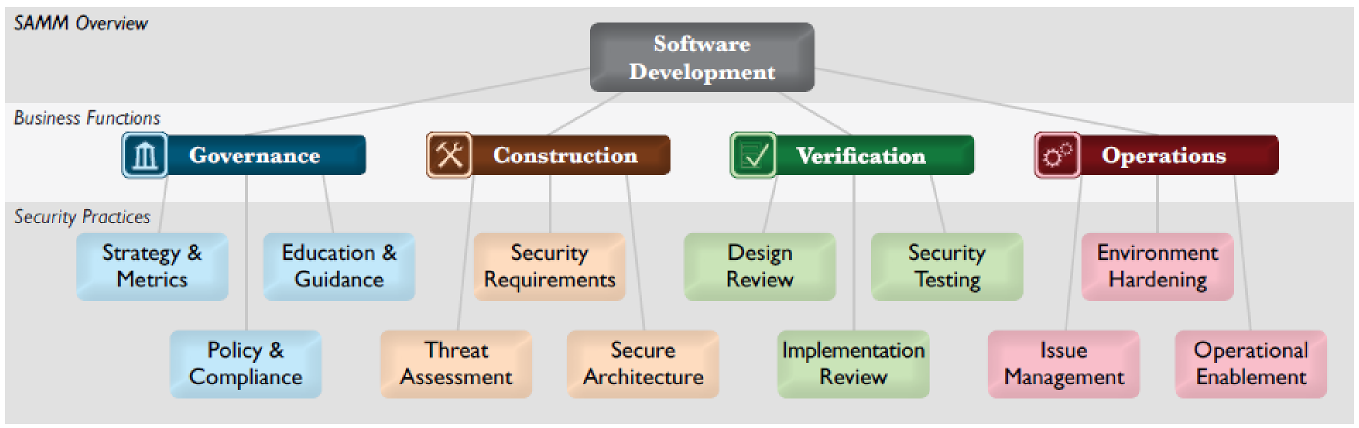
GDPR Article	GDPR Content
25. Privacy by Design & Default	**implement appropriate technical and organizational measures**, such as pseudonymisation, **which are designed to implement data-protection principles**, such as data minimisation, **in an effective manner and to integrate the necessary safeguards into the processing** in order to meet the requirements of this Regulation and protect the rights of data subjects. The controller shall implement appropriate technical and organizational measures for ensuring that, **by default, only personal data which are necessary for each specific purpose of the processing are processed**. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.
32. Security of Processing	Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well **as the risk of varying likelihood and severity** for the rights and freedoms of natural persons the controller and the processor shall **implement appropriate technical and organizational measures** to ensure **a level of security appropriate to the risk**
35. DPIA's	Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, **is likely to result in a high risk to the rights and freedoms of natural persons**, the controller shall, prior to the processing, **carry out an assessment of the impact on the protection of personal data.**

SDLC


SAMM
Coding guidelines
Configuration guidelines
DESIGN
BUILD
TEST
PRODUCTION
web / mobile application project (acquisition / development)
Threat modeling
Source code review (static)
Security testing (dynamic)
WAF tuning
TRAINING

OWASP SAMM

- For each of the Business Functions, 3 Security Practices are defined
- The Security Practices cover areas relevant to software security assurance
- Each one is a ‘silo’ for improvement



Mapping GDPR / SAMM

SAMM Domains		GDPR Articles
SM	Strategy & Metrics	5, 24, 32, 33
PC	Policy & Compliance	7, 24, 32, (12-21)
EG	Education & Guidance	37, 39
TA	Threat Assessment	25, 35
SR	Security Requirements	24, 28, 32
SA	Secure Architecture	25
DR	Design Review	24, 25, 30, 32
IR	Implementation Review	24, 25, 32
ST	Security Testing	24, 25, 32
IM	Issue Management	33, 34, 39
EH	Environment Hardening	25, 33
OE	Operational Enablement	32, 33

SM – Strategy & Metrics

SAMM		GDPR
SM 1	• Estimate overall business risk profile • Build and maintain assurance program roadmap	• Include privacy/GDPR within Entreprise Risk Management • Create a GDPR implementation Roadmap and involve DPO
SM 2	• Classify data and applications based on risks • Establish and measure per classification security goals	• Create a Personal Data Inventory (Records of Processing), integrate this with an application security classification scheme. • DPIA threshold questionnaire • Define personal data risks within applications
SM 3	• Conduct periodic industry-wide cost comparisons • Collect metrics for historic security spenditure	• /

PC – Policy & Compliance

SAMM		GDPR
PC 1	• Identify and monitor external compliance drivers • Build and maintain compliance guidelines	• GDPR is an external compliance driver • Build and maintain GDPR policies and processes and integrate GDPR into existing Info. Sec. and operational policies, processes and guidelines.
PC 2	• Build policies and standards for security and compliance • Establish project audit experience	• Build and maintain GDPR policies and processes and integrate GDPR into existing Info. Sec. and operational policies, processes and guidelines. • DPO should monitor GDPR compliance within the organization.
PC 3	• Create compliance gates for projects • Adopt solution for audit data collection	• DPO should monitor and approve security of new developed applications at different timeframes in the project

EG – Education & Guidance

SAMM		GDPR
EG 1	• Conduct technical security awareness training • Build and maintain technical guidelines	• Include GDPR requirements (opt-in, consent details, information portability…) in secure coding guidelines
EG 2	• Conduct role-specific application security training • Utilize security coaches to enhance projects teams	• The DPO should raise GDPR awareness within the organization.
EG 3	• Create formal application security support portal • Establish role-based examination and certification	• The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and implementation practices .

TA – Threat Assessment

SAMM		GDPR
TA 1	- Build and maintain application specific threat models - Develop attacker profile from software architecture	- Include DPIA threshold analysis in threat modeling phase. If appropriate perform a full DPIA.
TA 2	- Build and maintain abuse-case models per project - Adopt a weighting system for measurement of threats	- /
TA 3	- Explicitly evaluate risk from third-party components - Elaborate threat models with compensating controls	- Conduct due diligence on processors

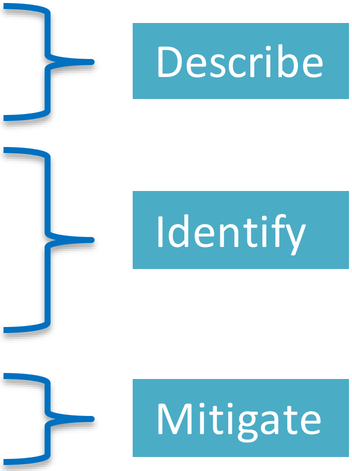
Data Protection Impact Assessment (DPIA)

- Methodology for identifying and mitigating compliance nonconformities and personal data risks.
- A DPIA should contain at least:

  - Description of processing and purposes
  - Legitimate interests pursued by controller
  - List of recipients & processors of personal data

  - Proportionality Assessment
  - Assessment Data Subject Rights
  - Foreseen measures to control security & compliance risks
  - Identification and quantification of risks

  - Additional security & compliance risk mitigating measures
  - Timeframes to implement additional controls



Describe

Identify

Mitigate

SR – Security Requirements

SAMM		GDPR
SR 1	• Derive security requirements from business functionality • Evaluate security and compliance guidance for requirements	• Add GDPR security compliance requirements (opt-in, consent details, information portability…) • Consider extra security controls to protect privacy sensitive information
SR 2	• Build an access control matrix for resources and capabilities • Specify security requirements based on known risks	• Apply least privilege, need to know and segregation of duties principles • Create audit trail of data access • Apply data retention requirements • Consider encryption of data (stored or in transit)
SR 3	• Build security requirements into supplier agreements • Expand audit program for security requirements	• Have data processing agreement in place with suppliers (and include security requirements at the same time). • Verify that data is not transferred out of Europe

SA – Security Architecture

SAMM		GDPR
SA 1	• Maintain list of recommended software frameworks • Explicitly apply security principles to design	• Apply privacy by design principles. • Apply minimization / pseudonymization if possible (risk based approach, comply or explain) • Apply encryption (risk based approach, comply or explain)
SA 2	• Identify and promote security services and infrastructure • Identify security design patterns from architecture	• /
SA 3	• Establish formal reference architectures and platforms • Validate usage of frameworks, patterns, and platforms	• /

DR – Design Review

SAMM		GDPR
DR 1	• Identify software attack surface • Analyze design against known security requirements	• Review design against GDPR controls decided during previous phases.
DR 2	• Inspect for complete provision of security mechanisms • Deploy design review service for project teams	• /
DR 3	• Develop data-flow diagrams for sensitive resources • Establish release gates for design review	• /

IR – Implementation Review

SAMM		GDPR
CR 1	• Create review checklists from known security requirements • Perform point-review of high-risk code	• Include GDPR checks in security reviews/reporting
CR 2	• Utilize automated code analysis tools • Integrate code analysis into development process	• /
CR 3	• Customize code analysis for application-specific concerns • Establish release gates for code review	• /

ST – Security Testing

SAMM		GDPR
ST 1	• Derive test cases from known security requirements • Conduct penetration testing on software releases	• Include GDPR checks in security reviews/reporting • Assure pseudonymisation and/or anonymization of test data • Minimize or remove production data from test environments
ST 2	• Utilize automated security testing tools • Integrate security testing into development process	• Consider/review privacy scanning tools (e.g. IAAP OneTrust that scans for cookies, tags, forms and policies)
ST 3	• Employ application-specific security testing automation • Establish release gates for security testing	• /

VM- Vulnerability Management

SAMM		GDPR
VM1	- Define contact point for data breaches - Create informal security response team	- DPO should be notified of all Data Breaches
VM2	- Establish consistent incident response process - Adapt a security issue disclosure process	- Organization must be able to identify data breaches - Data Protection Authorities and affected Data subjects must be notified
VM3	- Conduct root-cause analysis for incidents - Collect per-incident metrics	- /

EH – Environment Hardening

SAMM		GDPR
EH 1	• Maintain operational environment specification • Identify and install critical security upgrades and patches	• /
EH 2	• Establish routine patch management process • Monitor baseline environment configuration status	• Privacy by default (most privacy friendly setting should be the default setting)
EH 3	• Identify and deploy relevant operations protection tools • Expand audit program for environment configuration	• Forward / trigger on privacy or security related alerts/logs (automate with WAF, SIEM)

OE – Operational Enablement

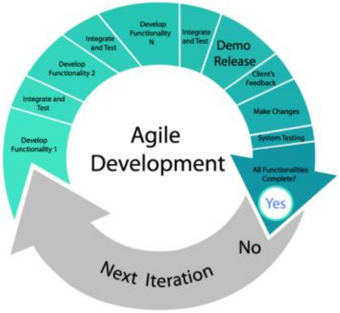
SAMM		GDPR
OE1	• Capture critical security information for deployment • Document procedures for typical application alerts	• Identify/document breach indicators to assure timely followup (for DPA notification)
OE2	• Create per-release change management procedures • Maintain formal operational security guides	• Include GDPR considerations in the operational security guides to demonstrate compliance!
OE3	• Expand audit program for operational information • Perform code signing for application components	• /

Use Case

- Project ongoing with customer
- Combined SAMM, GDPR & PCI assessment
- Integrated approach
- Security group & champions in the development teams
- Anonymized questionnaire will be shared with the SAMM project

Integrate GDPR!

- Do not “bold on” extra compliance activities
- Integrate compliance in appsec / infosec activities
- Add “GDPR epics and stories” to product backlog & include in sprints.



Advantages

- GDPR and SDLC re-inforce each other
- (ab)use GDPR to start SDLC (business case)
- Improve SDLC by including GDPR activities
- SDLC “deliverables” with GDPR demonstrate compliance

Key Success Factors

- Extend your appsec “community” with DPO & legal allies.
- Turn your DPO into an SDLC advocate

Next steps

- Share the mappings with the OWASP SAMM project
- Improve GDPR / SAMM activity mappings at OWASP Summit
- Feedback & improvements will be included!

http://owaspsummit.org/

Q & A

That’s all folks

OWASP: seba@owasp.org

Toreon: seba@toreon.com / siebe.deroovere@toreon.com