OWASP
AppSec Europe
London 2nd-6th July 2018

Adding Privacy by Design in Secure Application Development

Sebastien Deleersnyder, Toreon

OWASP AppSec Europe
London 2nd-6th July 2018

TOREON

Sebastien Deleersnyder

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

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

Creating trust for a safer digital society

Security Governance
& Privacy

Security
Architecture

Ethical
Hacking

Application
Security

Industrial
Security & IOT

www.toreon.com

Agenda

- GDPR for developers
- Privacy by Design
- SDLC Introduction
- Embedding GDPR into the SDLC
- Q&A

GDPR

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

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

GDPR – 7 Principles

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

Legal

Privacy by Design

Information Security

DevOps

GDPR Obligations

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 minimization, 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.**

For which applications?

- Does the application collect, store or use personal data?

- Does the application collect, store or use sensitive personal data?

  (*Like racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, genetic data, biometric data, sex life or sexual orientation, past or spent criminal convictions)*

Design requirements

- Privacy impact assessments
- Review the security of your systems
- Review 3rd party data processors you interface with

Lifecycle requirements

- Minimize the amount of collected data.
- Minimize the amount of data shared with third parties.
- Where possible, pseudonymize personal data.
- Revisit contact forms, sign-up pages and customer-service entry points.
- Enable the regular deletion of data created through these processes.

User management

- Provide clear privacy- and data-sharing notices.
- Embed granular opt-ins throughout those notices..
- Separate consent for essential third-party data sharing from consent for analytics and advertising.

End of life

- Periodically remind users to review and refresh their privacy settings.
- Allow users to download and delete old data.
- Delete the data of users who have closed their accounts.
- Delete all user data when the app’s life comes to an end.

Privacy by Design

- Adopt a privacy-first best-practice framework: Privacy by Design (PbD)
- Anticipate, manage and prevent privacy issues during design.
- Mitigate privacy risks, by not creating them in the first place.

PbD

"Privacy by Design (PbD) refers to the philosophy and approach of embedding privacy into the design specifications of various technologies"

Ann Cavoukian, Information and Privacy Commissioner, Ontario

7 foundational principles

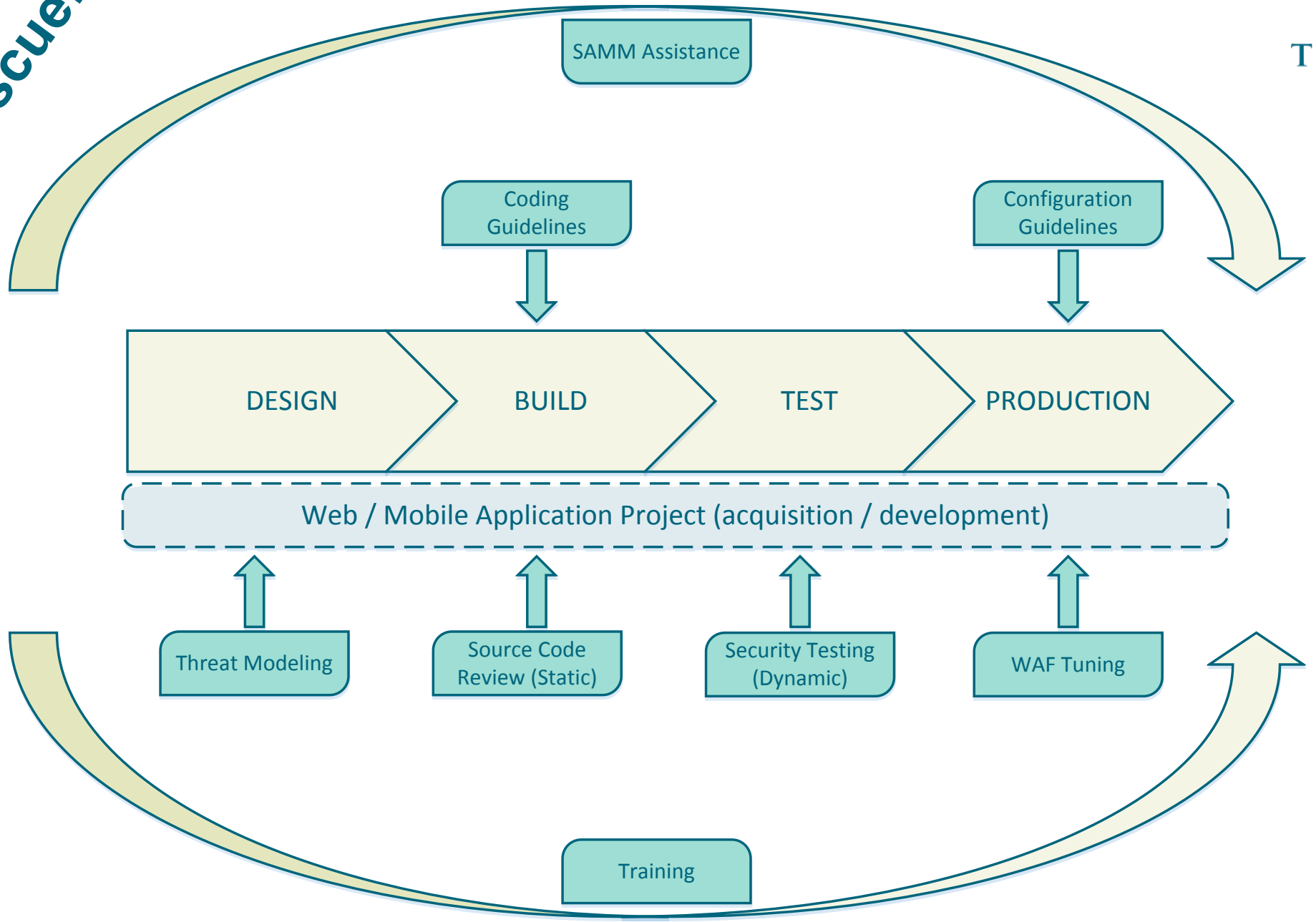
- Proactive, not reactive
- Privacy as default setting
- Embedded into design
- Full functionality
- End-to-end security
- Visibility and transparency
- Respect for user privacy

https://www.ipc.on.ca/resource/privacy-by-design/

PbD

- GDPR makes PbD and privacy by default legal requirements within the EU.
- Not only will you have to develop to PbD,
- But you will have to document your PbD development processes.
- That documentation must be made available to your DPA in the event of a data breach or a consumer complaint.

SDLC to the rescue!



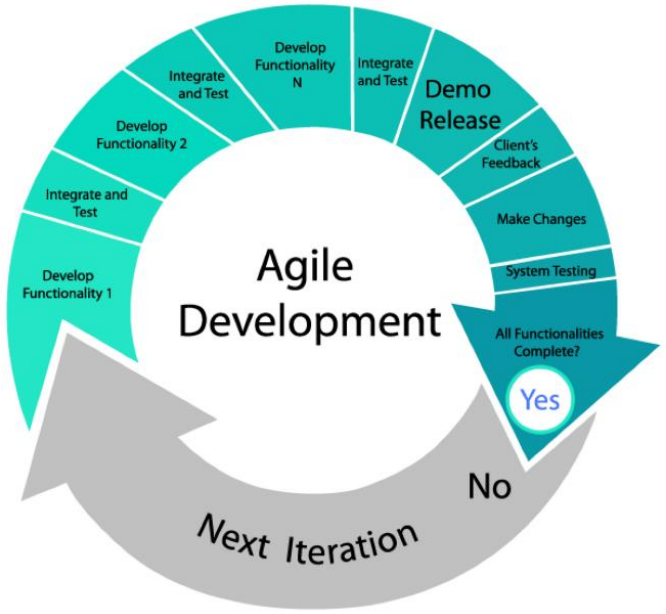
Mapping GDPR / SAMM (teaser)

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

https://www.toreon.com/application-security/embedding-gdpr-in-the-secure-development-lifecycle-sdlc/

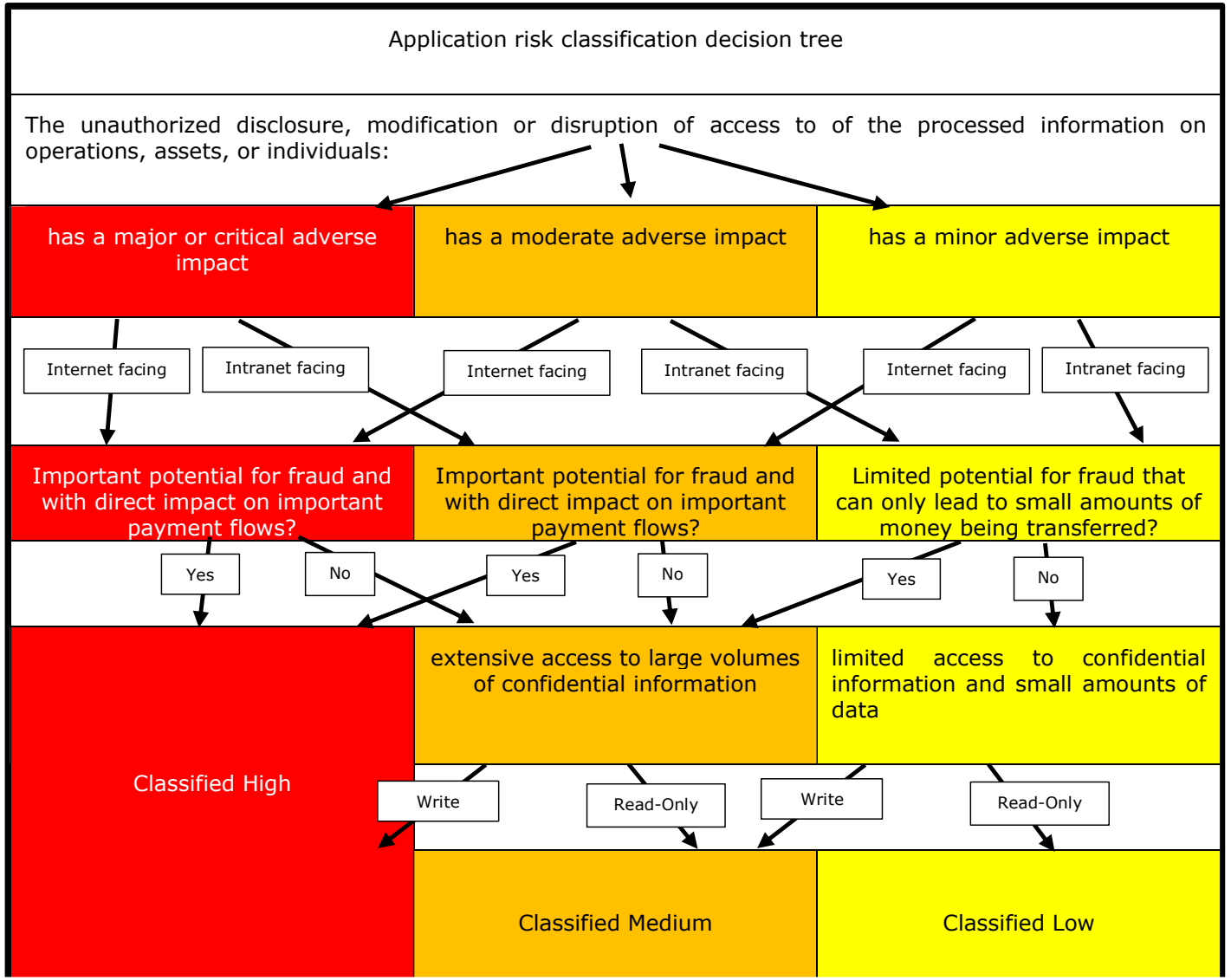
Integrate GDPR!

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



OWASP AppSec Europe
London 2nd-6th July 2018

Extend application security classification



Developer awareness training

- Raise overall awareness and understanding
- Learn defensive code techniques to developers
- Split over several brown bag sessions
- Extend with GDPR and privacy topics

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

Secure coding guidelines / Security requirements

- Add following topics:
  - GDPR security compliance requirements (opt-in, consent details, information portability…)
  - Consider extra security controls to protect privacy sensitive information
  - 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)

AppSec + Privacy Champions

- Security Champions are active members of a team that may help to make decisions about when to engage the Security Team
- Act as the "voice" of security for the given product or team
- Assist in the triage of security bugs for their team or area

- Consider combination with privacy champion role?
- Understands the privacy basics and organisation privacy context
- Identify potential privacy issues and involves the organisation DPO (if any)

Threat modeling

Diagram
- What are we building?

Identify threats
- What can go wrong?

Mitigate
- What are we doing to defend against threats?

Validate
- Validate steps 1-3 / Report

- Extend with privacy threats
- Apply privacy mitigations (e.g. minimization / pseudonymization)
- Apply encryption (risk based)

GDPR Risk Patterns

Example pattern:

Threat (from data subject perspective)	**Impossible to exercise right to information** - "Data subject cannot exercise his rights which makes it possible for data subjects to file a complaint at local Data Protection Authority which might lead to administrative fines. Data subject = person of whom personal data is processed"
Weakness	**No export functionality** – “No exportability functionality (for users or admins) which would allow the user to (directly or indirectly via an admin) export his personal data in a clear, readable format and transport it towards another data controller.”
GDPR	**Transparency** - Right to Data Portability - Art. 12/13/14/20
Control	"All data gathered from a user should be **exportable**. This does not include derivate fields that were created by the organization, such as customer segmentation fields. Provide or develop the means that will contribute to answer data portability requests, such as **download tools or Application Programming Interfaces (API)**. They should guarantee that personal data are transmitted in a structured, commonly used and machine-readable format, and they should be encouraged to ensure the interoperability of the data format provided in the exercise of a data portability request. See also - http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 (Guidelines on the right to "data portability" by WP29)

Next step is to convert the Control to a SCRUM User Story

3rd parties

- Explicitly evaluate risk from third-party components
- Check dependencies

- Extend with GDPR due diligence on processors
- Data processing agreements
- Verify that data is not transferred out of Europe

Security testing

- Include GDPR checks (manual or automated)
- Include GDPR checks in security reviews/reporting
- Assure pseudonymisation and/or anonymization of test data
- Minimize or remove production data from test environments
- Consider/review privacy scanning tools (e.g. scan for cookies, tags, forms and policies)

Incident management

- Include GDPR impact assessment early in the incident management process
- Identify/document breach indicators to assure timely follow-up (for DPA notification)
- Forward / trigger on privacy or security related alerts/logs (automate with WAF, SIEM)

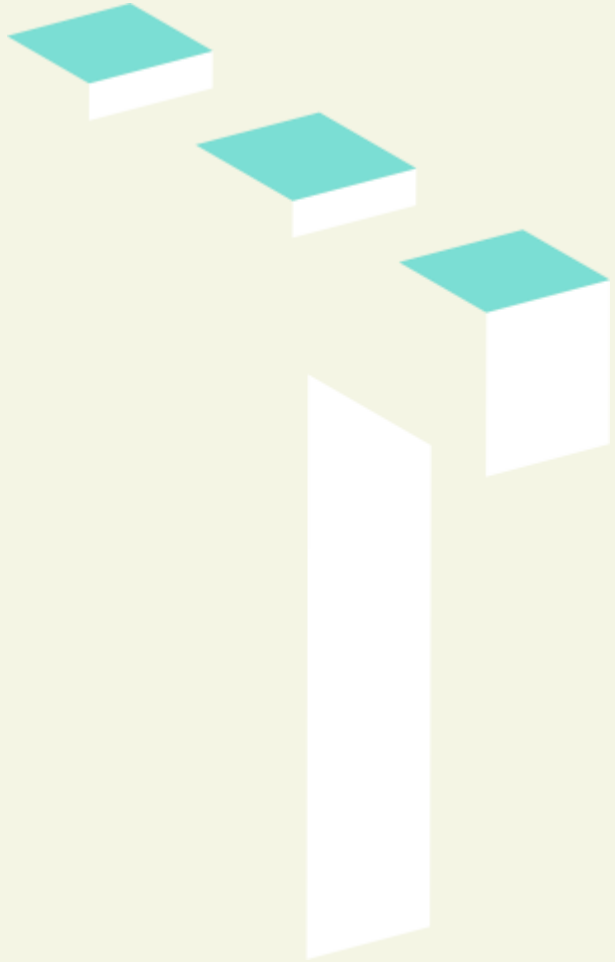
Advantages

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

Key Success Factors

- Extend your appsec “community” with DPO & legal allies.
- Turn your DPO into an SDLC advocate
- Integrate privacy and security in your developer/company culture


Q&A



Get in touch

OWASP: seba@owasp.org
Toreon: seba@toreon.com
Twitter: @SebaDele

@Toreon_BE
http://www.linkedin.com/company/toreon