


*#EADPPCertification
WebinarSeries*

BOKS Domain D Action Plan – How

- EADPP Certification
- BOKS Domain D
- Q&A

EADPP

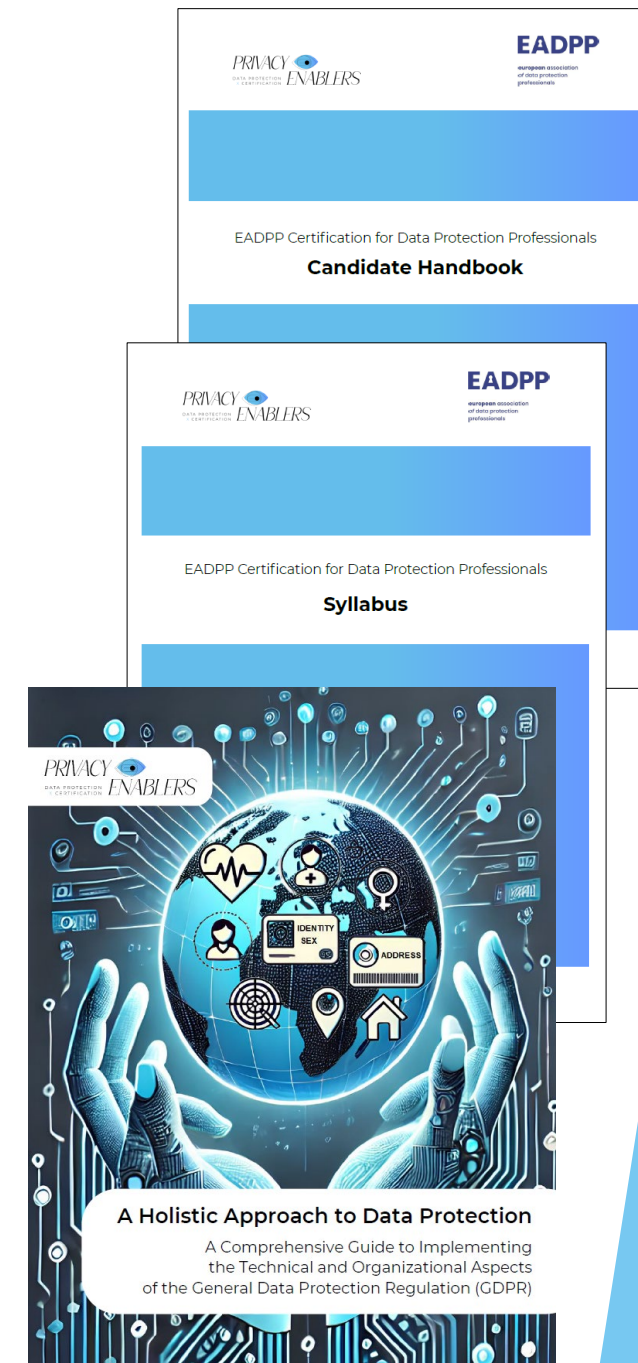
European association
of data protection
professionals

PRIVACY 
DATA PROTECTION
X CERTIFICATION **ENABLERS**

EADPP Certification for Data Protection Professionals

Aim, Content & Exam

- ▶ Providing a certification that focuses on **how data protection principles can be implemented**, beyond the legal aspects
 - ▶ Structured by a Body of Knowledge and Skills (BOKS) reflecting a holistic approach on data protection and privacy
- ▶ Becoming certified requires **passing the exam**
 - ▶ 40 single-option questions
 - ▶ **Exam package** includes (a.o.)
 - ▶ One online exam
 - ▶ Study book “A Holistic Approach to Data Protection”
- ▶ **Detailed information** can be found in the Syllabus and Candidate Handbook



Privacy Enablers Certification Platform




Username *

Password *

[Forgot username or password?](#)

Log in

Not registered yet? [Create an account](#)

 Application language

[Contact support](#)

Welcome to the Privacy Enablers Certification Platform!

Our platform is designed for seamless testing, training, and certification in the fields of data protection, privacy, and cybersecurity.

For any assistance, feel free to reach out to our support team at contact@privacyenablers.eu

BOKS Domain D: Action plan – How

Dominick De Boever

ISO27001 Lead Implementer – Data Protection Officer



Dominick is an experienced and certified professional in the field of information security, privacy and compliance. With a strong academic background, including a Master in Business Administration and Master of Science (Civil Engineering), he has specialised in IT security and data protection.

Dominick's certifications include EADPP Certified Data Protection Officer, CIPP/E, CIPM, CISM, ISO/IEC 27001 Lead Implementer and Prince2 Practitioner.



During his career, Dominick has led international programmes and projects focused on risk management, compliance and data security at large organisations such as BMW, Randstad, Securitas and Engie. He is an expert in implementing complex privacy and security frameworks such as GDPR, NIS2, TISAX and ISO27001.

He has extensive experience in lighting awareness campaigns and in training teams worldwide. With his strong leadership and communication skills, Dominick works effectively with both technical and non-technical teams to achieve business goals.

Overview

1. Risk management
2. Privacy metrics
3. Data Processing Impact Assessment (DPIA)
4. Business continuity
5. Data protection by design and by default
6. Management platforms
7. Conclusion

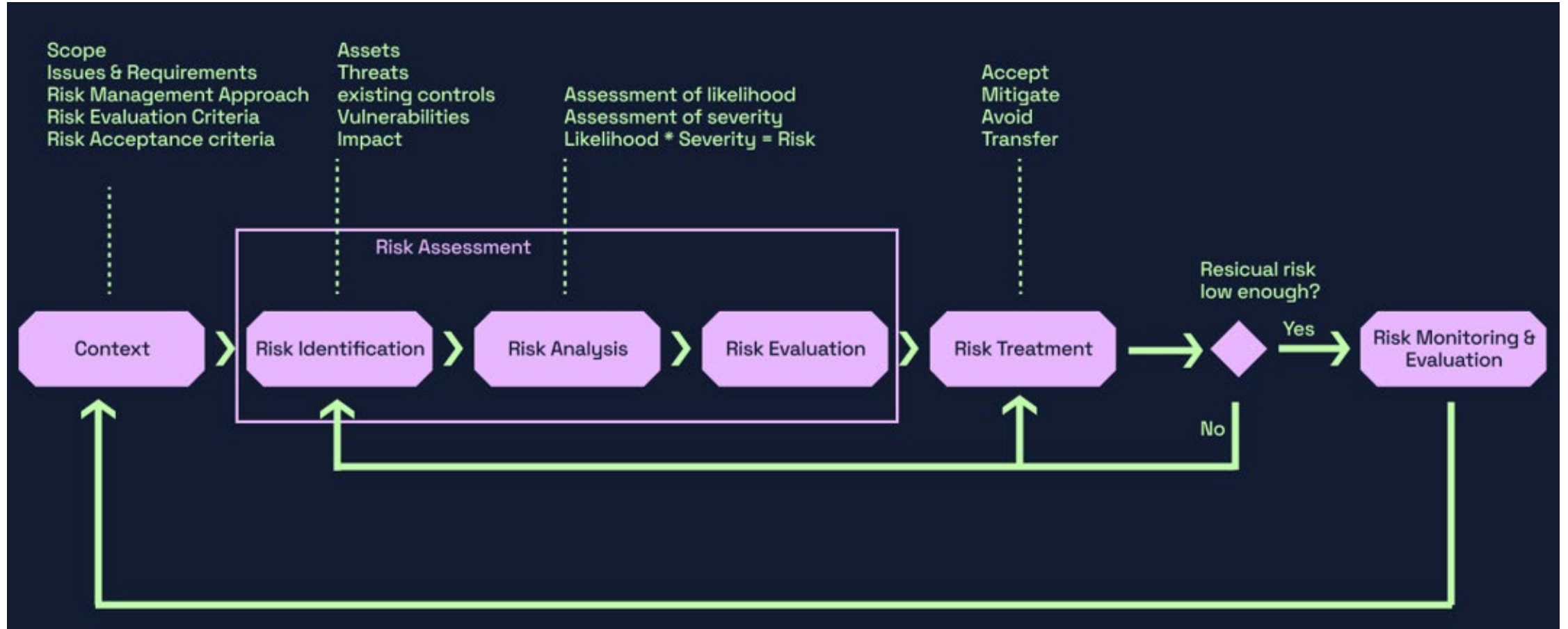
1. Risk management

- ▶ Risk **assessment** techniques
 - ▶ Risk = Impact x Probability
 - ▶ Risk = Vulnerability x Threat
- ▶ **Data protection risk** vs. **enterprise risk** 
- ▶ Build a **risk register** to manage risk
- ▶ Risk management **process** 
- ▶ Growing importance of **third-party** risk management
 - ▶ Compensating controls
 - ▶ Data breaches
 - ▶ Vendor questionnaires



Risk management process

(Courtesy GRC Lab)



2. Privacy metrics

- ▶ Quantitative and qualitative assessments that privacy leaders use to measure, manage, and improve the privacy programme and to establish transparency and trust
- ▶ Audiences: BoD, execs, BUs, employees, Privacy Team, IT, externals, etc.
- ▶ Measurement points:
 - ▶ Awareness
 - ▶ DSARs
 - ▶ DPAs and third-party audits
 - ▶ Accountability (policies, PIAs, TIAs, Privacy Stewards throughout the organisation, etc.)
 - ▶ Quality of RoPA
 - ▶ Translation of privacy risks to ERM: Can be KRIs
- ▶ Both activity-based as well as outcome-focused
- ▶ Facilitate risk management and mitigation

Tooling & Metric frameworks

- ▶ Key is shifting from manual processes to automated follow-up with Automated Privacy Governance Controls and Processes
 - ▶ Privacy Mailbox & Privacy Intranet
 - ▶ Privacy module on enterprise software
 - ▶ E.g., Setting up FAQs on privacy
 - ▶ Privacy GRC Tools
 - ▶ Privacy software tools
 - ▶ E.g., Tools for tracking DSR requests/fulfillment, retention, policy management and violation
- ▶ Standards & Norms:
 - ▶ NIST Privacy Framework v2
 - ▶ ISO 27001, 27018, 27701
 - ▶ GDPR, LGPD, COPPA

3. Data Processing Impact Assessment (DPIA)

- ▶ Understand the requirements (GDPR, COPPA, etc.)
- ▶ Create your own DPIA framework:
 - ▶ Identify & describe data processing activities
 - ▶ Evaluate risks & focus on risk-based approach
 - ▶ Suggest mitigating measures
- ▶ Engage relevant stakeholders early
 - ▶ Foster a collaborative approach
 - ▶ Promote culture of accountability
 - ▶ Stimulate responsibility for data protection throughout the organisation
- ▶ Document
- ▶ Evaluate
- ▶ Implement continuous monitoring

4. Business continuity

- ▶ Integrating DRP into BCP
- ▶ Essential element of CIA triad →
- ▶ Determine business continuity requirements
 - ▶ RTO (Recovery Time Objective)
 - ▶ RPO (Recovery Point Objective)
- ▶ Elaborate a comprehensive Business Continuity Plan (BCP) that is 100% available when all systems are down
- ▶ Test and rehearse at least annually



Business Continuity Plan (BCP) cycle



5. Data protection by design and by default

- ▶ Requirement for all data controllers
- ▶ Applies to companies of all sizes
- ▶ Integrate data protection from the design stage of systems, processes, and services
 - ▶ Proactively embedding data protection compliance before initiating any processing activity, ensuring privacy considerations from inception to the entire data lifecycle

Checklists

Data protection by default	Data protection by design	End-to-end security
<ul style="list-style-type: none">▪ Is our DP policy up-to-date?▪ Have we trained our people?▪ Have we conducted a DPIA where needed?▪ Have we evaluated the necessity of the data processing?▪ Data minimization & purpose limitation?▪ Data retention?	<ul style="list-style-type: none">▪ Can users revise their privacy settings?▪ Can users opt-in/opt-out?▪ Do we have a process for data erasure?▪ Can we pseudonymize / anonymize data?	<ul style="list-style-type: none">▪ Are security policies drawn up and translated into procedures?▪ How is our access control set up?▪ How about remote working protocols?▪ Is encryption properly applied?▪ Is there a DRP?▪ Is there vulnerability testing?▪ Do we have a security certification?

6. Management platforms

▶ Considerations:

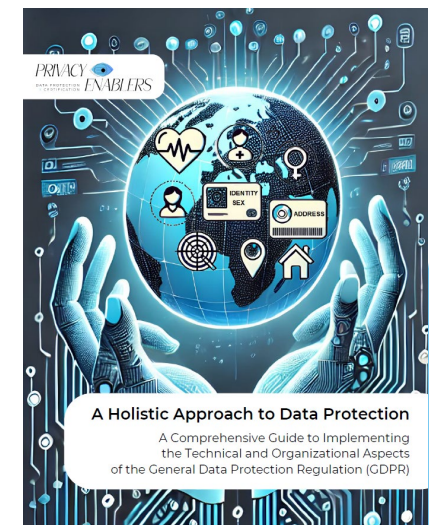
- ▶ Integration with other tools (e.g., GRC)
- ▶ Automation level (integration with IT systems)
- ▶ U.S. vs. Europe-based vendors
- ▶ Price

▶ Legislative framework:

- ▶ GDPR and country-specific implementations (e.g., BDSG in Germany)
- ▶ CCPA (California)
- ▶ PIPL (China)
- ▶ LGPD (Brazil)
- ▶ COPPA (Canada)

Conclusion

- ▶ Using a risk-based approach is a strong starting point
 - ▶ Use metrics that link privacy management and risk mitigation
 - ▶ Assess the impact of any initiatives on rights and freedoms of data subjects
 - ▶ Develop and test an adequate Business Continuity Plan (BCP)
 - ▶ When designing new processes, always use the minimal set of personal data and protect them adequately (PBDD)
-
- ▶ **Study Book** outlines several hints and handles for effective implementation



Q&A

- ▶ Questions?
- ▶ Comments?



Planning upcoming webinar

- ▶ **BOKS Domain E:** Privacy Culture – Human Perspective
 - ▶ Tuesday, 15 April 2025 at 11am CEST
 - ▶ Registration link: <https://events.teams.microsoft.com/event/2692e836-b8a7-4a72-b797-7c6601c038ce@8b75739f-c4ad-49d3-baaa-74bbf671c99a>