La boite à outils du GDPR

Compétences et connaissances indispensables pour le DPO

Georges Ataya, 23 octobre 2018

PEOPLE INVOLVED WITH THE GDPR COMPLIANCE

Data Subject

Primary Stakeholders

- Data protection Officer
- GDPR Compliance project manager
- Process Owner

Secondary Stakeholders

- Legal experts
- Chief information officer
- Chief information Security officer
- External Suppliers

BASED ON PROVEN FRAMEWORKS, BODIES OF KNOWLEDGE AND STANDARDS

Five domains of knowledge

D1. Compliance requirements

D2. Data Protection Management Requirements & Privacy Impact Assessment

D3. Compliance transformation

D4. Information security and data protection

D5. Compliance operations, monitoring and data breach management

D1. COMPLIANCE REQUIREMENTS

Identify applicable regulations to identify Data Protection requirements

D1. COMPLIANCE REQUIREMENTS

Domains of Knowledge	Learning Objectives
D101. GDPR application and scope	L101. To know when to apply the GDPR based on the Material, Personal and Territorial scope of the GDPR.
D102. Data processing principles	L102. To be able to list and explain each of the data processing principles: Lawfulness fairness and transparency of processing, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, accountability, conditions for consent, Processing of sensitive data.
D103. Data subject (DS) Rights	L103. To know in when the Data subject (DS) Rights are applicable and to be able to explain each of them: General modalities; Information and access to data; Rectification and erasure; Right to portability; Right to object; Right to not be subject to automated individual decision making/profiling
D104. Remedies for a data subject or a controller/processor and sanctions	L104. To be able to list all possible remedies for a data subject or a controller/processor and to be able to make the link between a possible infringement of the GDPR and the potential range of sanctions
D105. The obligations of the Controller	L105. To be able to list, apply and explain the obligations of the Controller
D106. The Processor interaction with the controller	L106. To know and explain how a Processor interacts with a controller, including the different obligations to appoint a processor and the sanction when it is made in compliance with the GDPR. To know and explain the interaction between a Processor and a sub-Processor, including the data processing agreement.
D107. Data Protection by Design and by Default	L107. To explain clearly the concept of Data Protection by Design and by Default
D108. Records of Processing Activities	L108. To know when a Records of Processing Activities need to be done and what are the essentials elements of it.
D109. DPO designation and the tasks of the DPO	L109. To know when a DPO need to be designated and to know and explain the position and tasks of the DPO
D110. Cross border data flows	L110. To know the different possibility for the Cross border data flows today and the road ahead, including to explain the international data transfers solutions such as adequacy decisions, appropriate safeguards or derogations
D111. Certification and the Codes of Conduct	L111. To know the existence of Certification mechanisms and Codes of Conduct mechanisms as well as the role of these mechanisms
D112. Data Protection Impact Assessment (DPIA)	L112. To know when a DPIA needs to be made and what are the content of it
D113. Supervisory Authorities (SA)	L113. To know and explain what is a Supervisory Authority (SA) in the GDPR and to be able to explain how the EU SAs are working together.
D114. Security and processing and Data breach management	L114. To understand the link between security and processing of personal data and to know what are the different actions to be taken when a Data breach occurs.
D115. Notices, Policies and Forms	L115. To understand and be able to create a privacy notice/policy, a consent policy/withdrawal, a Data breach notification form, and a complaint form
D116. Concept of Legitimate Interest	L116. To be able to explain the Concept of Legitimate Interest and the conditions for using it.

D2. Data Protection Management Requirements & Privacy Impact Assessment

Risk Assessment and Data Protection Impact Assessment exercises shape the transformation goals and mitigation plans

D2. Data Protection Management Requirements & Privacy Impact Assessment

Domains of Knowledge	Learning Objectives
D201. Definition of a Data Protection Management System	D201. To know and explain Data Protection Management System
D202. Data Protection Management System Lifecycle	D202. To be able to list and explain the different steps in the Data Protection Management System Lifecycle (initial assessment, design data protection management system, build, run, monitor, audit data protection management system)
D203. Framework development of Data Protection implementation (Toolkit)	D203. To be able to adopt or to develop a framework for Data Protection implementation (Toolkit)
D204. Translate business goals related to data protection into compliance goals	D204. To be able to determine business goals related to data protection and translate into compliance goals
D205. The 7. enablers for implementing and governing GDPR compliance	D205. To be able to identify the 7. enablers that are required for GDPR compliance
D206. Governance, Risk and Compliance (GRC)	D206. To understand the concept of Governance, Risk and Compliance (GRC)
D207. Risk Management concepts and practices	D207. To understand Risk Management concepts and practices (Risk Management principles and Risk Scenarios; Risk Response Priority Workflow; Information Risk Management Steps; Samples of detailed Risk Scenario Analysis)
D208. Performing a DPIA	D208. To be capable of performing a DPIA (Understand Data Protection Impact Assessments Context, Relevance, Detailed Walkthrough of the DPIA Process (Risks, Controls, Risks, and Decisions))
D209. Internal Controls and mitigations to major risks	D209. To be capable of recommending and describing relevant mitigations and internal controls to address major risks (including recommendations related to data subject rights, processing principles, breach handling, documentation requirements)
D210. Digital management domains	D210. Understand Digital management domains including Build/Implement/Acquire (GDPR Compliance transformation) and Deliver/Serve/Support (Data Protection operational Activities)
D211. Developing a management dashboard	D211. To be capable of developing a management dashboard with specific key performance and key goals indicators as well as maturity level.
D212. Specific practical cases on Data Protection in digital enterprises	D212. To be able to comment specific practical cases for example shadow IT and Internet of Things (IoT)

D3. COMPLIANCE TRANSFORMATION

Transformation through program and project management, process improvement and the implementation of adequate enablers to reach protection levels

D3. COMPLIANCE TRANSFORMATION

Domains of Knowledge	Learning Objectives
D301. Business and Digital strategy formulation	D301. To understand the concepts of Business and Digital strategy
D302. Translation of compliance Goals into Enterprise and technical target architecture	D302. To understand how to translate compliance goals into Enterprise and technical target architecture
D303. Compliance transformation dimensions	D303. To understand the concept of compliance transformation illustrated with four dimensions of a GDPR transformation
D304. Program and Project management and practices	D304. To understand the concepts of Program and Project management for a compliance transformation such as a GDPR compliance implementation
D305. Data Governance	D305. To understand Data Governance concepts and practices
D306. Business process and change management	D306. To understand the concepts of Business process management of Management of Change
D307. Data protection organization and competences	D307. To understand the data protection organization and competences

D4. INFORMATION SECURITY AND DATA PROTECTION

Build the Data protection secure platform, architecture and methods

D4. INFORMATION SECURITY AND DATA PROTECTION

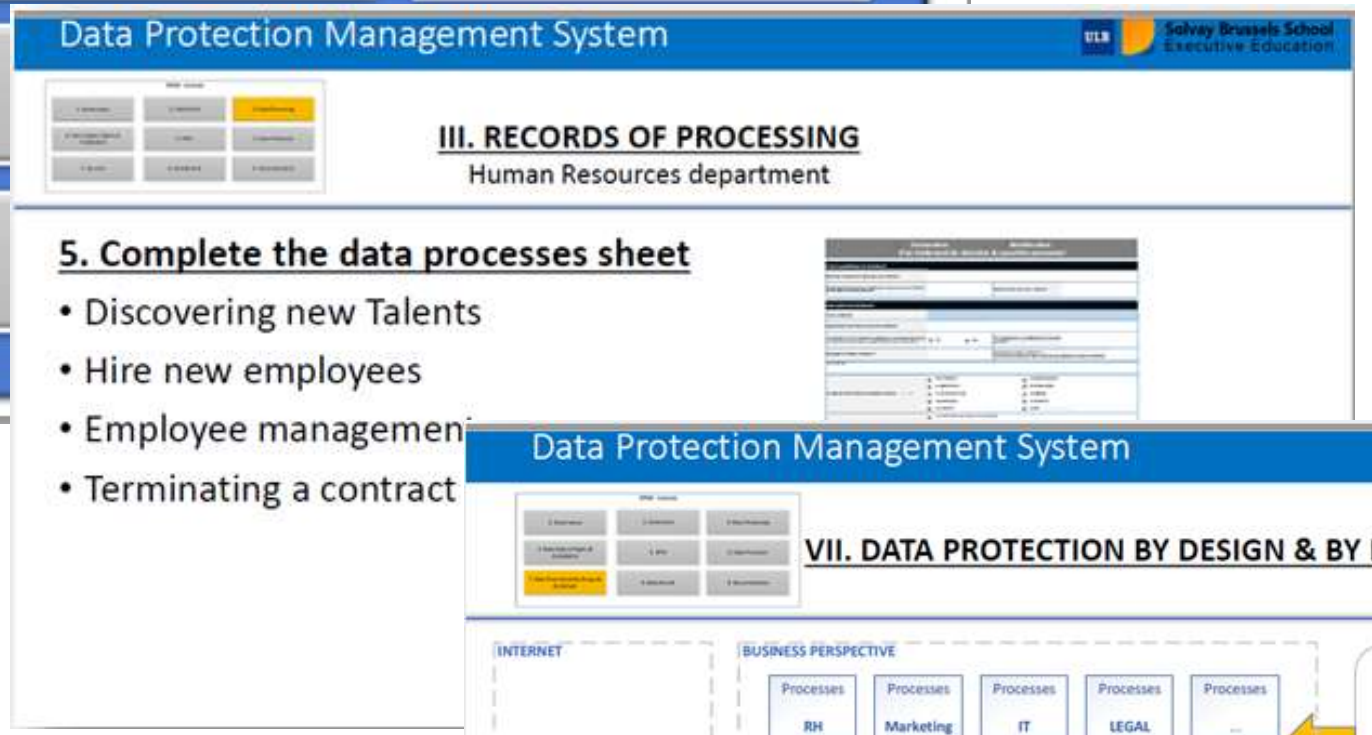
Domains of Knowledge	Learning Objectives
D401. Information Security objectives to support GDPR Compliance	D401. To understand Information Security objectives and their link to GDPR Compliance and Data Protection risks
D402. Security Architectural components and related threats and vulnerabilities	D402. To understand Security Architectural components and related threats and vulnerabilities
D403. High-level information security mitigation objectives	D403. To understand the concept of Internal controls and identify high-level information security mitigations
D404. Information Security Management System (ISMS) and the role of the CISO	D404. To understand the Information Security Management System (ISMS) and the role of the CISO
D405. Privacy Threats and vulnerabilities in a digital world	D405. To understand Privacy issues in a digital world taking into consideration ecommerce threats and technology and social media vulnerabilities
D406. Data Protection technology	D406. To understand Data Protection techniques and their impact on increasing compliance
D407. Practical cases for Data Protection technologies	D407. To be able to comment specific practical cases for example ‘GDPR accountability versus consent’ and ‘Privacy by default in a Geolocation’

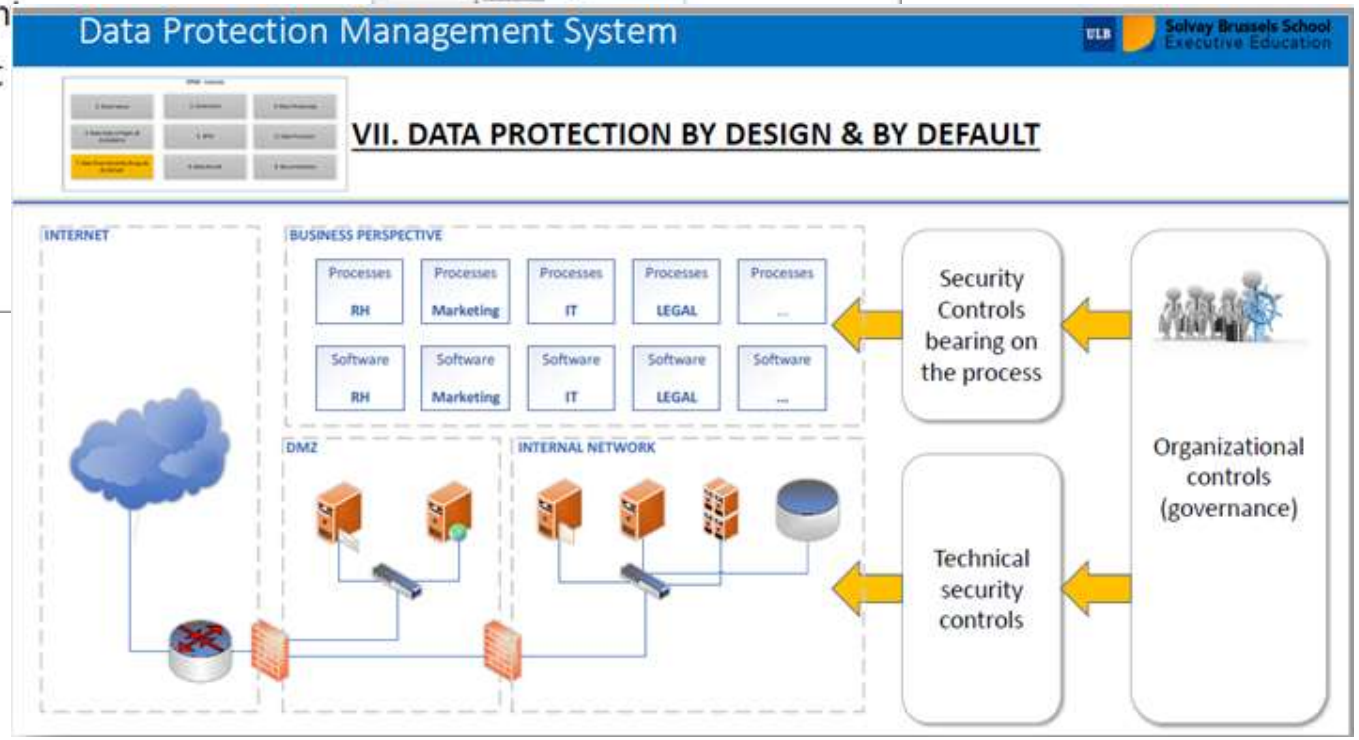
D5. COMPLIANCE OPERATIONS, MONITORING AND DATA BREACH MANAGEMENT

Compliance operations, Response management, breach handling activities, monitoring and assurance

D5. COMPLIANCE OPERATIONS, MONITORING AND DATA BREACH MANAGEMENT

Domains of Knowledge	Learning Objectives
D501. Service management	D501. To understand the Concepts and practices of Service management
D502. Incident management	D502. To understand Incident management practices
D503. Incident response plan	D503. To be capable of developing an incident response plan
D504. GDPR requirements for breach management	D504. To understand the GDPR requirements for breach management and be able to translate those into necessary enablers
D505. Personal Data Breach Handling process, organisation and tools	D505. To be capable to implement a Personal Data Breach Handling process, organisation and tools
D506. Compliance operations	D506. To be able to manage compliance operations
D507. Monitoring plan, Assurance and Maturity evaluation	D507. To be able to develop a monitoring plan and to conduct an assurance review of the maturity of Compliance activities





Program in European Data Protection

Started in 2016 as a research project with the ITMA asbl core team and the Belgian Privacy commission. Positioned today as a European leader in GDPR education. The body of knowledge is packaged to support a professional certification based on the ISO17024 standard.

Solvay.edu/gdpr

Coms.Solvay.edu/gdpr-modules

Georges ATAYA

Case discussion

Prereading and preparation work

Prereading and preparation work

S1 - Information Security Management

B2 - Business Transformation

A3 - Building Expert Opinion

G3 - IT Risk and Legal concerns

Up to fifteen specialised modules

Senior subject matter experts

Solvay Brussels School
Economics & Management

European Program in Data Protection
Next edition starting on March 22

Solvay.edu/gdpr

coms.solvay.edu/gdpr-modules-alumni-2018

Solvay Executive Education

Solvay Brussels School
Executive Education

DPO CIRCLE

IT MANAGEMENT Academy

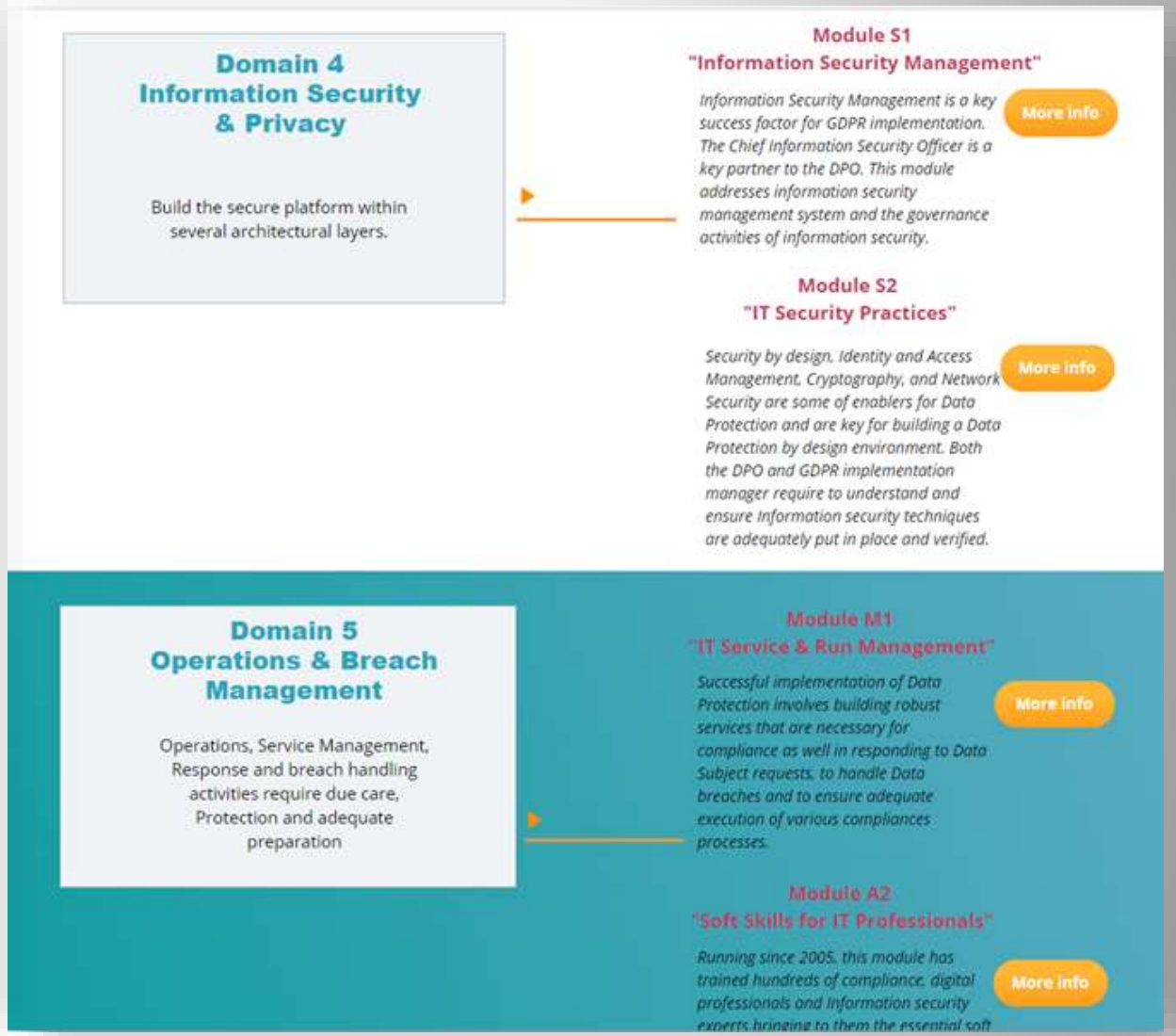
Extended Education for DPO professionals

DPO and GDPR implementation professionals require extended knowledge and practice. We are delighted to give access to our **Alumni of the Program in European Data Protection** to extended education that both created and sustained the reputation of **Sol School** in domains like **Digital Transformation**, **Technology Implementation**, **Security, Risk Management, Compliance and Auditing**, and much more.

Benefit from our spec

S1 – Information Security Management	G1 – The CIO Foundation	M1 – Applications Build and Management	B1 – Enterprise Strategy and Architecture	A Po
S2 – IT Security Practices	G2 – IT Governance Workshop	M2 – IT Services and Run Management	B2 – Business Transformation	A2 – Soft Skills for IT professionals
S3 – Cybersecurity Workshop	G3 – IT Risk and Legal concerns	M3 – IT Sourcing Management	B3 – Digital Agility and Innovation	A3 – Building Expert Opinion

Coms.Solvay.edu/gdpr-modules



Solvay.edu/gdpr

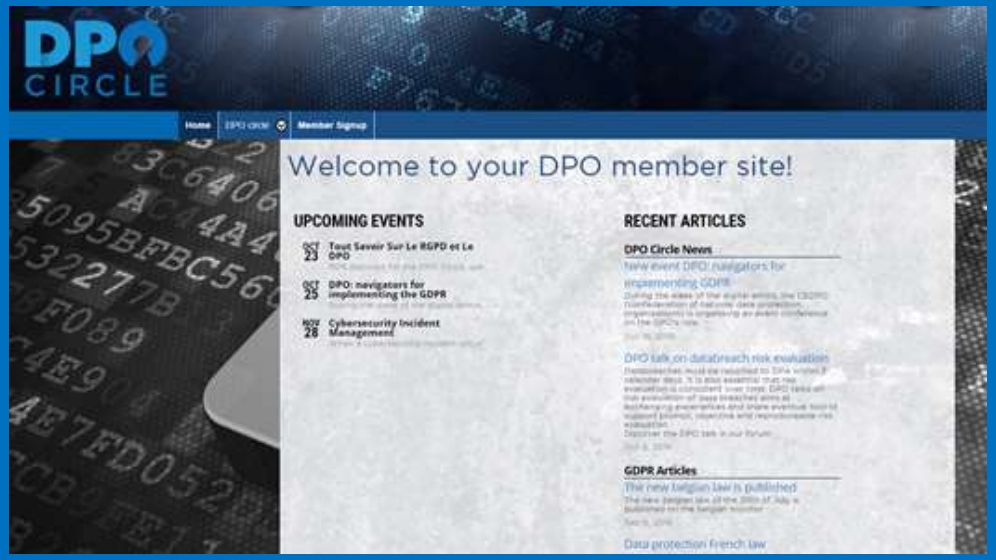
Coms.Solvay.edu/gdpr-modules


GDPRPRO
DPOASASERVICE
gdprpro.com

DPO and GDPR professionals

Association belge des professionnels du RGPD.

Rejoignez gratuitement les membres et participer aux différentes réunions et tables rondes sur différents sujets relatifs à la protection des données.



DPOCIRCLE.EU

DPO CIRCLE TALKS

Experience sharing, advocacy and development of toolbox,
Up to two round table meeting in a month

Conferences with the involvement of Data Protection authorities (Belgian ADP, EU EDPS) and Secretary of state

Annual Conference in Genval 2018

300 members

MERCI POUR VOTRE PRESENCE

Questions?

DPO CIRCLE

GDPRPRO.com

ICT CONTROL
Your Trusted Advisor

ULB Solvay Brussels School Executive Education