Knowledge and skills for implementing personal data protection in a data-driven world.

Alignment of EXIN personal data protection certifications with ISO/IEC 27701 and the European General Data Protection Regulation (GDPR)

Organizations have more opportunities than ever to take advantage of data to improve products and services. Data has become a valuable asset that can give organizations an advantage over their competitors. However, the growing volume of data also creates vulnerabilities, particularly where the personal data of individuals is concerned. As a result, standards and regulations regarding data protection are increasingly crucial.

These regulations enable organizations to take advantage of new business opportunities and, at the same time, protect their customers and reduce their own compliance risk. Developing data and privacy protection skills and knowledge is no longer a 'nice to have'; it is a critical success factor for all types of organizations.

The General Data Protection Regulation (EU) 2016/679 ((GDPR) is a regulation created by the European Union in 2016 and implemented in 2018. GDPR focuses on "the protection of natural persons with regard to the processing of personal data and on the free movement of such data.". It aims to give individuals control over their (personal) data and to simplify the regulatory environment for international business by unifying the regulation within the EU. It replaces the previous Data Protection Directive 95/46/EC, and contains provisions and requirements related to the processing of personal data of individuals inside the European Economic Area (EEA). It applies to any enterprise established in the EEA or enterprises that are processing the personal information of data subjects inside the EEA (regardless of their location).

ISO/IEC 27701:2019 is a privacy extension to ISO/IEC 27001, which was released in August 2019. The goal of this extension is to enhance the existing Information Security Management System (ISMS) with additional requirements to establish, implement, maintain, and continually improve a Privacy Information Management System (PIMS). The standard outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage privacy controls and reduce the risk to personally identifiable information of individuals. The privacy controls outlined in the ISO/IEC 27701 standard are aligned with the GDPR. Also, industry efforts are underway to map ISO/IEC 27701 to other national and sub-national privacy laws, to support organizations in the development of a global privacy management system.

Standards and regulations are not enough in themselves; they require professionals with the right knowledge and skills to be able to apply them. EXIN's Data Protection and Privacy program covers the required knowledge of legislation and regulations relating to data protection and how this knowledge should be used to be compliant.

The certification program is based upon the GDPR and, as such, is also aligned to the ISO/IEC 27701 standard. The program contains certifications at different levels, from essential awareness to advanced specialist skills, leading ultimately to the EXIN Certified Data Protection Officer title. This paper contains a mapping of the EXIN Privacy & Data Protection program to both the GDPR and the ISO/IEC 27701 standard, to provide transparency on alignment.

Reference Matrix: EXIN Privacy and Data Protection Foundation

Exam Specifications	Literature Reference*	GDPR Reference	ISO/IEC 27701 Reference
1. Exam requirement: Privacy & Data Protection Fundamentals and Regulations			
1.1 Definitions	Chapter 1 Definitions and Historical Context	Recital 1 Data Protection as a Fundamental Right Recital 2 Respect of the Fundamental Rights and Freedoms Article 96 Relationship with previously concluded Agreements Article 97 Commission reports Articel 98 Review of other Union legal acts on data protection Article 99 Entry into force and application	no reference
1.2 Personal Data	Chapter 1 Definitions and Historical Context Chapter 2 Processing of Personal Data	Article 4.1(a) Personal data Article 4.10 Third party Article 9.1 Processing of special categories of personal data Article 17 Right to erasure ('right to be forgotten')	Subclause 7.2.2 Identify lawful basis Subclause 7.3.6 Access, correction and/or erasure
1.3 Legitimate Grounds and Purpose Limitation	Chapter 3 Legitimate Grounds and Purpose Limitation	Article 6.1 Processing shall be lawful only if and to the extent that ... Article 24 Responsibility of the controller	Subclause 7.2.2 Identify lawful basis
1.4 Further Requirements for Legitimate Processing of Personal Data	Chapter 3 Legitimate Grounds and Purpose Limitation	Article 5 Principles relating to processing of personal data Article 25 Data protection by design and by default Article 27 Representatives of controllers or processors not established in the Union Article 28 Processor Article 29 Processing under the authority of the controller or processor Article 30 Records of processing activities Article 31 Cooperation with the supervisory authority Article 32 Security of processing	Article 5 is referenced throughout the standard Subclause 5.2.1 Understanding the organization and its context
1.5 Rights of Data Subjects	Chapter 4 Rights of Data Subjects	Article 15 Right of access by the data subject Article 16 Right to rectification Article 17 Right to erasure ('right to be forgotten') Article 18 Right to restriction of processing Article 20 Right to data portability Article 21 Right to object Article 22 Automated individual decision-making, including profiling	Subclause 7.2.2 Identify lawful basis Subclause 7.3.2 Determining information for Personally Identifiable Information (PII) principles Subclause 7.3.6 Access, correction and/or erasure Subclause 7.3.9 Handling requests Subclause 7.3.10 Automated decision making Subclause 7.5.1 Identify basis for PII transfer between jurisdictions
1.6 Personal Data Breach and Related Procedures	Chapter 5 Personal Data Breaches and Related Procedures	Article 4(12) personal data breach Article 33 Notification of a personal data breach to the supervisory authority Article 34 Communication of a personal data breach to the data subject	Subclause 6.13.1.5 Response to information security incidents

Reference Matrix: EXIN Privacy and Data Protection Foundation

Exam Specifications	Literature Reference*	GDPR Reference	ISO/IEC 27701 Reference
2. Exam requirement: Organizing Data Protection			
2.1 Importance of Data Protection for the Organization	Chapter 2 Processing of Personal Data Chapter 3 Legitimate Grounds and Purpose Limitation Chapter 5 Personal Data Breaches and Related Procedures Chapter 6 Importance of Data Protection for the Organization Chapter 7 Supervisory Authorities	Article 7 Conditions for consent Article 8 Conditions applicable to child's consent in relation to information society services Article 13 Information to be provided where personal data are collected from the data subject Article 25(1) Implement appropriate technical and organisational measures Article 30 Records of processing activities Article 83 General conditions for imposing administrative fines	Subclause 6.11.2.1 Secure development policy Subclause 6.11.2.5 Secure systems engineering principles Subclause 7.2.3 Determine when and how consent is to be obtained Subclause 7.2.4 Obtain and record consent Subclause 7.2.5 Privacy impact assessment Subclause 7.2.8 Records related to processing PII Subclause 7.3.2 Determining information for PII principles Subclause 7.3.6 Access, correction and/or erasure Subclause 7.3.10 Automated decision making Subclause 7.5 PII sharing, transfer and disclosure Subclause 8.2.6 Records related to processing PII Subclause 8.5.2 Countries and international organizations to which PII can be transferred Subclause 8.5.3 Records of PII disclosure requests
2.2 Supervisory Authority	Chapter 7 Supervisory Authorities	Article 33 Notification of a personal data breach to the supervisory authority Article 34 Communication of a personal data breach to the data subject Article 36 Prior consultation	Subclause 5.2.2 Understanding the needs and expectations of interested parties Subclause 6.13.1.1 responsibilities and procedures Subclause 6.13.1.5 response to information security incidents Subclause 7.2.5 Countries and international organizations to which PII can be transferred
2.3 Personal Data Transfer to Third Countries	Chapter 7 Supervisory Authorities	Article 29 Processing under the authority of the controller or processor Article 30 Records of processing activities Article 45 Transfers on the basis of an adequacy decision	Subclause 7.2.8 Records related to processing PII Subclause 7.5 PII sharing, transfer and disclosure Subclause 8.2.2 Organization's purposes Subclause 8.2.6 Records related to processing PII
2.4 Binding Corporate Rules and Data Protection in Contracts	Chapter 7 Supervisory Authorities	Article 24 Responsibility of the controller Article 28 Processor Article 47 Binding corporate rules	Subclause 5.2.1 Understanding the organisation and its context Subclause 6.12.1.2 Addressing security with supllier relationships Subclause 7.2.6 Contracts with PII processors Subclause 7.2.8 Records relating to processing PII Subclause 7.5.1 Identify basis for PII transfer between jurisdictions Subclause 8.5 PII sharing, transfer, and disclosure.

Reference Matrix: EXIN Privacy and Data Protection Foundation

Exam Specifications	Literature Reference*	GDPR Reference	ISO/IEC 27701 Reference
3. Exam requirement: Practice of Data Protection			
3.1 Data Protection by Design and by Default Related to Information Security	Chapter 7 Supervisory Authorities, Chapter 8 Quality Aspects	Article 25 Data protection by design and by default	Subclause 6.11.2.1 Secure development policy Subclause 6.11.2.5 Secure systems engineering principles Subclause 7.4.2 Limit processing Section B.8.4 Privacy by design and privacy by default
3.2 Data Protection Impact Assessment (DPIA)	Chapter 8 Quality Aspects	Article 35 Data protection impact assessment	Subclause 5.2.2 Understanding the needs and expectations of interested parties Subclause 7.2.5 Privacy impact assessment Subclause 8.2.1 Customer agreement
3.3 Practice-related Applications of the Use of Data, Marketing and Social Media	Chapter 4 Rights of Data Subjects, Chapter 8 Quality Aspects	no reference	Section B.8.2.3 Marketing and advertising use

Reference Matrix: EXIN Privacy and Data Protection Practitioner

Exam Specifications	Literature Reference**	GDPR Reference	ISO/IEC 27701 Reference
1. Exam requirement: Data Protection Policies			
1.1 Purpose of the Data Protection and Privacy Policies within an Organization	A, Chapter 1 Privacy Compliance Frameworks A, Chapter 16 Transitioning and Demonstrating Compliance	no reference	no reference
1.1 Purpose of the Data Protection and Privacy Policies within an Organization	A, Chapter 5 Requirements for Data Protection Impact Assessments	Article 25 Data protection by design and by default	Subclause 6.11.2.1 Secure development policy Subclause 6.11.2.5 Secure systems engineering principles Subclause 7.4.2 Limit processing Section B.8.4 Privacy by design and privacy by default
2. Exam requirements: Managing and Organizing Data Protection			
2.1 Phases of the Data Protection Management System (DPMS)	A, Chapter 12 Controllers and Processors A, Chapter 14 Incident Response Management and Reporting B, Chapter 2 Data Protection and Privacy Management System	no reference	no reference

Reference Matrix: EXIN Privacy and Data Protection Practitioner

Exam Specifications	Literature Reference**	GDPR Reference	ISO/IEC 27701 Reference
3. Exam requirements: Roles of the Controller, Processor and Data Protection Officer (DPO)			
3.1 Roles of the Controller and Processor	A, Chapter 12 Controllers and Processors	Article 24 Responsibility of the controller Article 26 Joint controllers Article 27 Representatives of controllers or processors not established in the Union Article 28 Processor Article 29 Processing under the authority of the controller or processor	Subclause 5.2.1 Understanding the organization and its context Subclause 8.5.8 Change of subcontractor to process PII Subclause 6.3.1.1 Information security roles and responsibilities Subclause 6.12.1.2 Addressing security within supplier releationships Subclause 6.15.1.1 Identification of applicable legislation and contractual requirements Subclause 7.2.6 Contracts with PII processors Subclause 7.2.7 Joint PII controller Subclause 8.2.1 Customer agreement Subclause 8.2.4 Infringing instruction Subclause 8.2.5 Customer obligations Subclause 8.5.4 Notification of PII disclosure requests Subclause 8.5.6 Disclosure of subcontractors used to process PII Subclause 8.5.7 Engagement of a subcontractor to process PII
3.2 Roles of the Controller and Processor	A, Chapter 2 Role of the Data Protection Officer	Article 37 Designation of the data protection officer Article 38 Position of the data protection officer Article 39 Tasks of the data protection officer	Subclause 6.3.1.1 Information security roles and responsibilities Subclause 6.4.2.2 Information security awareness, education and training Subclause 6.10.2.4 Confidentiality and non-disclosure agreements Subclause 6.3.1.1 Information security roles and responsibilities Subclause 6.4.2.2 Information security awareness, education and training Subclause 6.10.2.4 Confidentiality and non-disclosure agreements

Reference Matrix: EXIN Privacy and Data Protection Practitioner

Exam Specifications	Literature Reference**	GDPR Reference	ISO/IEC 27701 Reference
4. Exam requirement: Data Protection Impact Assessment (DPIA)			
4.1 Criteria for a DPIA	A, Chapter 5 Requirements for Data Protection Impact Assessments A, Chapter 6 Risk Management and DPIAs A, Chapter 7 Data Mapping A, Chapter 8 Conducting DPIAs	Article 35 Data protection impact assessment	Subclause 5.2.2 Understandiong the needs and exectations of interested parties Subclause 7.2.5 Privacy impact assessment Subclause 8.2.1 Customer agreement
4.2 Steps of a DPIA	A, Chapter 5 Requirements for Data Protection A, Chapter 7 Data Mapping A, Chapter 8 Conducting DPIAs	no reference	Subclause 5.2.2 Understandiong the needs and exectations of interested parties Subclause 7.2.5 Privacy impact assessment Subclause 8.2.1 Customer agreement
5. Exam requirements: Data Breaches, Notification and Incident Response			
5.1 GDPR Requirements with Regard to Personal Data Breaches	A, Chapter 3 Common Data Security Failures A, Chapter 14 Incident Response Management and Reporting	Article 4(12) personal data breach Article 33 Notification of a personal data breach to the supervisory authority Article 34 Communication of a personal data breach to the data subject	Subclause 6.13.1.1 Responsibilities Subclause 6.13.1.5 Response to information security incidents
5.2 Requirements for Notification	A, Chapter 14 Incident Response Management and Reporting	Article 33 Notification of a personal data breach to the supervisory authority Article 34 Communication of a personal data breach to the data subject	Subclause 6.13.1.1 Responsibilities Subclause 6.13.1.5 Response to information security incidents

* A.L. Besemer, Whitepaper: EXIN Privacy & Data Protection Foundation. Free download from www.exin.com

** A. IT Governance Privacy Team, EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (second edition, 2017), ISBN 978-1-84928-9450 (paperback), ISBN 978-1-84928-9474 (e-book)

B. Kyriazoglou, J., Data Protection and Privacy Management System. Data Protection and Privacy Guide – Vol. I, bookboon.com (first edition, 2016), ISBN 978-87-403-1540-0

Summary

As ‘digital’ becomes the norm, the resulting data explosion means that standards and regulations are increasingly crucial to ensure that the personal data of individuals is protected. The GDPR and the ISO/IEC 27701 standard lead the way internationally in setting the standard. Professionals require the right skills to apply these standards and regulations.

The EXIN Privacy & Data Protection program allows professionals to develop these skills and gain an independent, internationally recognized certification, which is aligned to both he GDPR and the ISO / IEC 27701 standard.

For more information, see: www.exin.com/qualification-program/exin-privacy-and-data-protection.