认证备考指南

202403 版本

内容

1. 概述

EXIN Privacy & Data Protection Professional (PDPP.CH)

范围

EXIN Privacy & Data Protection Professional 认证验证考生具备以下方面的知识：

- 数据保护政策
- 隐私信息管理系统（PIMS）
- 控制者、处理者和数据保护官（DPO）的角色
- 数据保护影响评估（DPIA）
- 数据泄露，通知和事件响应

总结

EXIN Privacy & Data Protection Professional 旨在验证专业人员对欧盟隐私和数据保护法规及其国际效力的了解和理解，以及专业人员在日常专业实践中应用它的能力。

随着互联网信息爆炸式增长，每家公司都需要规划如何管理和保护个人隐私及其数据。出于相关理由，欧盟内部以及美国和许多其他地区都制定了许多新法律，以规范隐私和数据保护。

欧盟委员会已经发布了《通用数据保护条例》（GDPR），这意味着从 2018 年 5 月 25 日起，所有相关组织必须遵守其特定规则。该进阶层级的认证以 EXIN Privacy & Data Protection Foundation 考试所涵盖的主题为基础，重点落在制定并实施有关政策和程序以遵守现有和新的法规，推动对隐私和数据保护准则的应用和最佳实践，以及如何建立一个数据和隐私保护管理系统（DPMS）。

ISO/IEC 27000 系列中的标准，ISO/IEC 27701: 2019 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management – Requirements and Guidelines（国际标准 ISO/IEC 27701: 2019 安全技术 - 针对 ISO/IEC 27001 和 ISO/IEC 27002 在隐私信息管理的扩展 - 要求和指南）对于那些希望展现 GDPR 合规的企业是非常实用的。该 ISO 标准的内容将有助于组织在处理个人数据方面履行 GDPR 的义务。

GDPR 和 ISO 标准并非本认证的考试文献教材。即便如此，在第 4 部分的教材考点分布矩阵还是给出了认证的考试要求同考试文献教材、GDPR 和 ISO/IEC 27701: 2019 标准之间的关联，从而为本认证提供一个更广阔的视野。

背景

EXIN Privacy & Data Protection Professional 认证是 EXIN Privacy & Data Protection 认证项目的一部分。

目标群体

本进阶的认证尤其适用于以下群体：

- 数据保护官（DPO）/隐私官
- 法律/合规官
- 安全官
- 业务连续性经理
- 数据控制者
- 数据保护审计员（内审员和外审员）
- 隐私分析师
- 人力资源经理

认证要求

- 顺利通过 EXIN Privacy & Data Protection Professional 考试。
- 顺利完成 EXIN 授权的 EXIN Privacy & Data Protection Professional 培训，包括实践作业。

考试细节

考试类型：	单选题
题目数量：	40
通过分数：	65% (26/40 题)
是否开卷考试：	在考试过程中可以参考 GDPR。参加在线考试时，该文献将作为附录提供。参加纸质考试时，考生需要自行携带该文献。
是否记笔记：	否
是否允许携带电子设备/辅助设备：	否
考试时间：	120 分钟

EXIN 的考试规则和规定适用于本次考试。

布鲁姆级别

EXIN Privacy & Data Protection Professional 认证根据布鲁姆分类学修订版对考生进行布鲁姆 2 级、3 级和 4 级测试。

- 布鲁姆 2 级：理解——识记（1 级）之上的一级。理解表明考生能够理解呈现的内容，并能够评估如何将学习资料应用到实际的环境中。这类题目旨在证明考生能够整理，比较，阐释并选择跟事实和想法有关的正确描述。
- 布鲁姆 3 级：应用——表明考生有能力在与学习环境不同的情境下使用所学信息。这类题目旨在证明考生能够以不同的方式或新的方式应用所掌握的知识，实例，方法和规则，在新的情况下解决问题。这类题目通常包含一个简短的场景。
- 布鲁姆 4 级：分析——表明考生有能力将所学信息拆分并加以理解。布鲁姆级别主要通过实践作业进行测试。实践作业是为了证明考生能够辨明动机或原因，作出推断并找到支持归纳的证据，从而检查并拆分信息。

培训

培训时长

本培训课程时长建议 21 小时。该时长包括学员实践作业、考试准备和短暂休息。该时长不包括家庭作业、备考的准备工作和午餐休息时间。

建议个人学习时间

112 小时（4 ECTS），根据现有知识的掌握情况可能有所不同。

培训机构

您可通过 EXIN 官网 www.exin.com 查找该认证的授权培训机构。

2. 考试要求

考试要求详见考试说明。下表列出模块主题（考试要求）和副主题（考试规范）。

考试要求	考试规范	权重
1. 数据保护政策		**10%**
	1.1 组织内数据保护和隐私政策的目的	5%
	1.2 基于设计和默认的数据保护	5%
2. 隐私信息管理系统（PIMS）		**32.5%**
	2.1 隐私信息管理系统（PIMS）基础	12.5%
	2.2 隐私信息管理系统（PIMS）的益处	10%
	2.3 隐私信息管理系统（PIMS）的关联	10%
3. 控制者、处理者和数据保护官（DPO）的角色		**17.5%**
	3.1 控制者和处理者的角色	10%
	3.2 DPO 的角色和职责	7.5%
4. 数据保护影响评估（DPIA）		**27.5%**
	4.1 数据保护影响评估（DPIA）的标准	15%
	4.2 数据保护影响评估（DPIA）的步骤	12.5%
5. 数据泄露、通知和事件响应		**12.5%**
	5.1 GDPR 有关个人数据泄露方面的要求	2.5%
	5.2 对通知的要求	10%
	合计	**100%**

考试规范

1 数据保护政策

1.1 组织内数据保护和隐私政策的目的

考生能够...

1.1.1 说明组织遵守数据保护法规所需的政策和程序。

1.1.2 说明政策的内容。

1.2 基于设计和默认的数据保护

考生能够...

1.2.1 说明基于设计和默认的数据保护的概念。

1.2.2 描述基于设计和默认的数据保护的七项原则。

1.2.3 说明基于设计和默认的隐私的相关原则如何落实。

2 隐私信息管理系统（PIMS）

2.1 隐私信息管理系统（PIMS）基础

考生能够...

2.1.1 解释 ISO/IEC 27701 标准中使用的不同术语（内部问题和外部问题、相关方）。

2.1.2 列举实施 PIMS 时必须考虑的媒体。

2.1.3 定义什么是适用性声明（SoA）。

2.1.4 说明 PIMS 中文档的作用。

2.1.5 说明 PIMS 中管理评审的作用。

2.2 隐私信息管理系统（PIMS）的益处

考生能够...

2.2.1 说明 PIMS 中的审计目标。

2.2.2 说明如何根据适当的当地规则和合同要求确定 PIMS 的具体要求。

2.2.3 说明 PIMS 和审计如何帮助证实合乎相关的标准和法规。

2.2.4 说明 PIMS 如何有助于供应商筛选。

2.3 隐私信息管理系统（PIMS）的关联

考生能够...

2.3.1 说明隐私信息管理系统（PIMS）与信息安全管理系统（ISMS）之间的区别。

2.3.2 说明对信息安全恰当安排的数据保护原则与 ISO/IEC 27701 标准之间的关系。

2.3.3 说明 ISO/IEC 27002 标准对于实施 PIMS 的有用性。

2.3.4 说明如何应用 PIMS 的控制措施。

3 控制者、处理者和数据保护官（DPO）的角色

3.1 控制者和处理者的角色

考生能够...

3.1.1 行使控制者的职责。

3.1.2 行使处理者的职责。

3.1.3 说明在特定情况下控制者和处理者之间的关系。

3.2 DPO 的角色和职责

考生能够...

3.2.1 根据 GDPR 说明何时任命一个 DPO 是强制性的。

3.2.2 扮演 DPO 的角色。

3.2.3 说明 DPO 与监管机构的关系。

4 数据保护影响评估（DPIA）

4.1 数据保护影响评估（DPIA）的标准

考生能够...

4.1.1 依据相应标准来实施 DPIA。

4.1.2 描述 DPIA 的目标和产出。

4.2 数据保护影响评估（DPIA）的步骤

考生能够...

4.2.1 描述 DPIA 的步骤。

4.2.2 在特定情况下执行 DPIA。

5 数据泄露、通知和事故响应

5.1 GDPR 有关个人数据泄露方面的要求

考生能够...

5.1.1 依据 GDPR 评估是否发生了数据泄露事故。

5.2 对通知的要求

考生能够...

5.2.1 通知监管机构个人数据泄露事故。

5.2.2 向通知数据主体通告有关的个人数据泄露事故。

5.2.3 描述 GDPR 存档义务的有关要素。

3. 考试术语表

本章节包含了考生应熟知的术语和缩写。

请注意单独学习术语并不能满足考试要求。学员必须了解其概念，并且能够举例说明。

英文	中文
appropriate technical and organizational measures	适当的技术和组织措施
audit	审计
authenticity	真实性
availability	可用性
awareness	意识
bring your own device (BYOD)	自携设备（BYOD）
certification (bodies)	认证（机构）
cloud computing	云计算
codes of conduct	行为守则
collecting personal data	收集个人数据
commission reports	委员会报告
complaint	投诉
compliance	合规
consent • child's consent • conditions for consent • explicit consent	同意 • 儿童的同意 • 同意的条件 • 明确同意
consistency mechanism	一致性机制
controller	控制者
cross-border processing	跨境处理
data accuracy	数据准确性
data breach	数据泄露
data classification system	数据分类系统
data lifecycle management (DLM)	数据生命周期管理（DLM）
data mapping	数据映射
data portability	数据可携性
data protection	数据保护
data protection authority (DPA)	数据保护局（DPA）
data protection by default / privacy by default	默认的数据保护/默认的隐私
data protection by design / privacy by design	基于设计的数据保护/隐私预设
data protection impact assessment (DPIA)	数据保护影响评估（DPIA）
data protection officer (DPO)	数据保护官（DPO）
data protection policy	数据保护政策
data protection program	数据保护计划
data protection provisions	数据保护条款
data subject	数据主体
data subject access (facilities)	数据主体查阅（设施）
data transfer	数据传输

declaration of consent	同意声明
delegated acts and implementing acts • committee procedure	授权法案与执行法案 • 委员会程序
documentation obligation	存档义务
EU types of legal act	欧盟法规类型
European Data Protection Board	欧洲数据保护委员会
European Data Protection Supervisor (EDPS)	欧洲数据保护主管（EDPS）
European Economic Area (EEA)	欧洲经济区（EEA）
European Union legal acts on data protection	欧盟数据保护法案
General Data Protection Regulation (GDPR)	通用数据保护条例（GDPR）
governing body	管理机构
group of undertakings	企业集团
incident response	事故响应
independent supervisory authorities	独立监管机构
• activity reports • competence • establishment • powers • tasks	• 活动报告 • 能力 • 设立机构 • 权力 • 任务
Information Security Management System (ISMS)	信息安全管理系统（ISMS）
information society service	信息社会服务
international organization	国际组织
internet of things (IoT)	物联网（IoT）
joint controllers	联合控制者
judicial remedy	司法救济
lawfulness of processing	处理合法性
legitimate basis (GDPR Recital 40)	合法基础（GDPR 第 40 条声明）
legitimate ground (GDPR Article 17(1c), Article 18(1d), Article 21(1))	合法事由（GDPR 第 17（1c）条，第 18（1d）条，第 21（1）条）
legitimate interest	合法权益
liability	责任
main establishment	主要机构
material scope	适用范围
non-repudiation	不可抵赖性
opinion of the board	董事会意见
personal data	个人数据
personal data breach	个人数据泄露
personal data relating to criminal convictions and offences	有关刑事定罪和犯罪的个人数据
policy (rules)	政策（规则）

principles relation to processing of personal data (GDPR Article 5)	处理个人数据的有关原则（GDPR 第 5 条）
• accountability • accuracy • confidentiality • data minimization • fairness • integrity • lawfulness • purpose limitation • storage limitation • transparency	• 可问责 • 准确 • 保密 • 数据最小化 • 公平 • 完整 • 合法 • 目的限制 • 存储限制 • 透明
prior consultation	事前协商
privacy	隐私
privacy analysis	隐私分析
privacy information management system (PIMS)	隐私信息管理系统（PIMS）
privacy officer	隐私官
processing (of personal data)	（个人数据）处理
processing agreement	处理协议
processing situations	处理场景
• data protection rules of churches and religious associations • employment • for archiving purposes in the public interest • for scientific or historical research purposes • for statistical purposes • freedom of expression and information • National Identification Number • obligations of secrecy • public access to official documents	• 教会和宗教协会的数据保护规则 • 雇佣 • 出于公共利益下的归档目的 • 出于科学或历史研究的目的 • 出于统计目的 • 言论与信息自由 • 身份证号 • 保密义务 • 官方文件的公共查阅
processor	处理者
profiling	特征分析
proportionality, the principle of	相称性原则
pseudonymization	假名化
quality cycle	品质管控循环
recipient	接收者
relevant and reasoned objection	相关和合理的反对
repealed	废除
representative	代表
restriction of processing	处理限制
retention period	存留期

rights of the data subject • 'right to be forgotten' • automated individual decision-making • data portability • information and access • modalities • notification obligation • rectification and erasure • restriction of processing • right to compensation • right to objection • transparency	数据主体的权利 • "被遗忘的权利" • 自动化的个体决策 • 数据可携性 • 告知与查阅 • 方式 • 通知义务 • 修正和删除 • 处理限制 • 赔偿权 • 反对权 • 透明
risk management	风险管理
rules of procedure	程序规则
security breach	安全漏洞
security incident	安全事故
service provider	服务提供商
seven principles for privacy by design	基于设计的隐私预设七项原则
Social [media], Mobile [technology], [advanced] Analytics, Cloud, and [Internet of] Things (SMACT)	社交【媒体】、移动【技术】、【高级】分析、云、物【联网】(SMACT)
special categories of personal data	个人数据的特殊类别
• biometric data • data concerning health • genetic data • political opinions • racial or ethnic origin • religious or philosophical beliefs • sex life or sexual orientation • trade union membership	• 生物特征数据 • 有关健康的数据 • 遗传数据 • 政治观点 • 种族或民族起源 • 宗教或哲学信仰 • 性生活或性取向 • 工会会员
subsidiarity, the principle of	辅助性原则
supervisory authority	监管机构
supervisory authority concerned	有关监管机构
suspension of proceedings	处理暂停
territorial scope	地域范围
third party	第三方
threat	威胁
transfer of personal data to third countries and to international organizations	向第三国和国际组织传输个人数据
• adequacy decision • appropriate safeguards • binding corporate rules (BCR) • derogations • disclosures • international protection of personal data	• 充分性决定 • 适当的保障措施 • 约束性企业规则 (BCR) • 克减 • 披露 • 个人数据的国际保护
unified communications and collaboration (UCC)	统一通信与协作 (UCC)
vulnerability	漏洞

4. 文献

考试文献教材

以下文献包含了考试要求掌握的知识。

A. [英] IT Governance 隐私小组 著 刘合翔 译
欧盟通用数据保护-GDPR 合规实践
清华大学出版社有限公司（第二版，2021）
ISBN: 9787302594796（印刷版）

B. Alan Shipman & Steve Watkins
ISO/IEC 27701:2019: An introduction to privacy information management
IT Governance Publishing（2020）
ISBN: 9781787781993（印刷版）
ISBN: 9781787782013（电子书）

可选教材

C. European Commission
General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
Regulation of the European Parliament and the Council of the European Union.
布鲁塞尔，2016 年 4 月 6 日

D. Article 29 Data Protection Working Party
Guidelines on Data Protection Officers ('DPOs'), wp 243rev.01，2017 年 4 月 5 日

E. Article 29 Data Protection Working Party
Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248，2017 年 4 月 4 日

F. A. Cavoukian
Privacy by Design - The 7 Foundational Principles
Information & Privacy Commissioner，安大略省，加拿大
https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

G. ISO/IEC 27701:2019 (EN)
Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management – Requirements and Guidelines
瑞士，ISO/IEC（2019）
https://www.iso.org/home.html

备注

可选教材仅作为参考和深度学习使用。

由于考试文献中已充分提供了有关《通用数据保护条例》（GDPR）的知识，因此《通用数据保护条例》原文（文献 C）未列入首要的考试文献。考生应熟悉其他文献中对 GDPR 的引用。

教材考点分布矩阵

考试要求	考试规范	教材参考章节	GDPR 对应章节	ISO/IEC 27701 对应章节
1. 数据保护政策				
	1.1 组织内数据保护和隐私政策的目的	A，第 1 章、第 16 章	*无引述*	*无引述*
	1.2 基于设计和默认的数据保护	A，第 5 章	第 25 条	B 部分 8.4 节、第 6.11.2.1 款、第 6.11.2.5 款、第 7.4.2 款
2. 管理和组织数据保护（PIMS）				
	2.1 隐私信息管理系统（PIMS）基础	B，第 1 章、第 2 章、第 3 章、第 4 章	*无引述*	*全文*
	2.2 隐私信息管理系统（PIMS）的益处	B，第 2 章、第 3 章、第 4 章、第 5 章	*无引述*	*全文*
	2.3 隐私信息管理系统（PIMS）的关联	B，第 3 章、第 4 章、第 5 章、第 6 章	*无引述*	*全文*
3. 控制者、处理者和数据保护官（DPO）的角色				
	3.1 控制者和处理者的角色	A，第 12 章	第 24 条、第 26 条、第 27 条、第 28 条、第 29 条	第 5.2.1 款、第 6.3.1.1 款、第 6.12.1.2 款、第 6.15.1.1 款、第 7.2.6 款、第 7.2.7 款、第 8.2.1 款、第 8.2.4 款、第 8.2.5 款、第 8.5.4 款、第 8.5.6 款、第 8.5.7 款、第 8.5.8 款
	3.2 DPO 的角色和职责	A，第 2 章	第 37 条、第 38 条、第 39 条	第 6.3.1.1 款、第 6.4.2.2 款、第 6.10.2.4 款

4. 数据保护影响评估（DPIA）				
	4.1 数据保护影响评估（DPIA）的标准	A，第 5 章、第 6 章、第 7 章、第 8 章	第 35 条	第 5.2.2 款、第 7.2.5 款、第 8.2.1 款
	4.2 数据保护影响评估（DPIA）的步骤	A，第 5 章、第 7 章、第 8 章	*无引述*	第 5.2.2 款、第 7.2.5 款、第 8.2.1 款
5. 数据泄露、通知和事故响应				
	5.1GDPR 有关个人数据泄露方面的要求	A，第 3 章，第 14 章	第 4(12)条、第 33 条、第 34 条	第 6.13.1.1 款、第 6.13.1.5 款
	5.2 对通知的要求	A，第 14 章	第 33 条、第 34 条	第 6.13.1.1 款、第 6.13.1.5 款

联系 EXIN

www.exinchina.cn

info.china@exin.com

WeChat ID: EXINCH