认证备考指南

202308 版本

内容

1.概述

EXIN Privacy & Data Protection Foundation (PDPF.CH)

范围

EXIN Privacy & Data Protection Foundation (PDPF) 认证旨在验证专业人员是否掌握和理解有关个人数据保护、欧盟规则以及数据保护法规方面的知识。

总结

无论个人数据在何处采集、存储、使用及最终删除和销毁，都将产生隐私问题。通过《通用数据保护条例》（GDPR），欧盟理事会试图强化和统一欧盟（EU）境内所有个体的数据保护。该条例将对处理欧盟个人数据的每个组织造成影响。EXIN Privacy & Data Protection Foundation 认证涵盖与 GDPR 相关的主要主题。

ISO/IEC 27000 系列中的新标准：ISO/IEC 27701:2019 安全技术-ISO/IEC27001 和 ISO/IEC 27002 在隐私信息管理方面的扩展，其要求与指南对想要展现 GDPR 合规的组织会有帮助。新 ISO 标准的内容有助于组织履行其在处理个人数据方面的 GDPR 义务。

GDPR 和 ISO 标准都不是考试文献教材。但是，本材料第 4 章的考点引述表展现了考试要求、参考文献、GDPR 和 ISO/IEC 27701:2019 标准之间的关联，从而为本认证提供了一个更开阔的视野。

背景

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

目标群体

需要掌握数据保护和欧洲在 GDPR 中定义的法律要求的所有企业雇员。这项认证专门面向：

- 数据保护官（DPO）
- 合规官
- 安全官
- 人事专员
- 流程和项目经理

认证要求

- 顺利通过 EXIN Privacy & Data Protection Foundation 考试。

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：	否
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：	60 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 Foundation 认证根据布鲁姆分类学修订版对考生进行布鲁姆 1 级和 2 级测试。

- 布鲁姆 1 级：记忆——依靠对信息的回忆。需要考生吸收、记住、识别和回忆。
- 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。

培训

培训时长

本培训课程时长建议 14 小时。该时长包括学员分组作业、考试准备和短暂休息。该时长不包括午餐休息、家庭作业以及考试的时间。

建议个人学习量

56 小时（2 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（考试明细）。

考试要求	考试规范	权重
1.隐私和数据保护基础和法规		**47.5%**
	1.1 定义	7.5%
	1.2 个人数据	17.5%
	1.3 合法依据与目的限制	5%
	1.4 合法处理个人数据的进一步要求	5%
	1.5 数据主体权利	2.5%
	1.6 个人数据泄露和相关程序	10%
2.组织数据保护		**35%**
	2.1 数据保护对组织的重要性	12.5%
	2.2 监管机构[1]	7.5%
	2.3 个人数据传输到第三国	7.5%
	2.4 企业约束性规则（BCR）与合同中的数据保护	7.5%
3.数据保护实践		**17.5%**
	3.1 与信息安全相关的，基于设计的和默认的数据保护	5%
	3.2 数据保护影响评估（DPIA）	5%
	3.3 使用中的个人数据	7.5%
	合计	**100%**

[1] 在引入 GDPR 前，数据保护局是负责执行数据保护法规的国家主管部门。在 GDPR 中，数据保护局称为“*监管机构*“。

考试规范

1 隐私和数据保护基础和法规

1.1 定义

考生能够...

1.1.1 定义隐私。
1.1.2 将隐私与个人数据和数据保护相关联。
1.1.3 描述欧盟和成员国法律背景。

1.2 个人数据

考生能够...

1.2.1 根据 GDPR 定义个人数据。
1.2.2 区分个人数据和特殊类别数据（例如敏感个人数据）。
1.2.3 描述数据主体关于个人数据的权利。
1.2.4 定义属于 GDPR 范围内的个人数据处理。
1.2.5 列出 GDPR 中的角色、职责和利益相关者。

1.3 合法依据和目的限制

考生能够...

1.3.1 列出处理的六大合法依据。
1.3.2 描述目的限制的概念。
1.3.3 描述相称性和辅助性原则。

1.4 合法处理个人数据的进一步要求

考生能够...

1.4.1 描述合法数据处理的要求。
1.4.2 描述个人数据处理的目的。
1.4.3 说明个人数据处理相关原则。

1.5 数据主体权利

考生能够...

1.5.1 描述数据可携权和检查权。
1.5.2 描述被遗忘权。

1.6 个人数据泄露和相关程序

考生能够...

1.6.1 描述个人数据泄露的概念。
1.6.2 说明发生个人数据泄露时的应对程序。
1.6.3 举例说明个人数据泄露类别。
1.6.4 描述安全泄露（事件）与个人数据泄露的区别。
1.6.5 列出个人数据泄露时需通知的相关利益相关者。

2 组织数据保护

2.1 数据保护对组织的重要性

考生能够...

2.1.1 列出不同管理类别（GDPR 第 28 和 30 条）。
2.1.2 指出遵守 GDPR 需采取的活动。
2.1.3 定义基于设计的和默认的数据保护。
2.1.4 举例说明个人数据泄露事件。
2.1.5 描述 GDPR 中规定的个人数据泄露通知义务。
2.1.6 描述给予处罚（包括行政罚款）的执行。

2.2 监管机构

考生能够...

2.2.1 说明监管机构的一般职责。
2.2.2 说明监管机构在个人数据泄露方面的角色和职责。
2.2.3 说明监管机构对实施 GDPR 的作用。

2.3 个人数据传输到第三国

考生能够...

2.3.1 描述应用于欧洲经济区境内数据传输的法规。
2.3.2 描述应用于欧洲经济区境外数据传输的法规。
2.3.3 描述应用于欧洲经济区和美国间的数据传输的法规。

2.4 企业约束性规则（BCR）与合同中的数据保护
考生能够...
2.4.1 说明企业约束性规则（BCR）的概念。
2.4.2 描述如何在控制者和处理者之间的合同中规定数据保护。
2.4.3 描述这类书面合同的条款。

3 数据保护实践

3.1 基于设计的和默认的数据保护
考生能够...
3.1.1 描述基于设计的和默认的数据保护的好处。
3.1.2 描述基于设计的数据保护的七大原则。

3.2 数据保护影响评估（DPIA）
考生能够...
3.2.1 列出数据保护影响评估的内容及实施时机。
3.2.2 列出 DPIA 的八大目标。
3.2.3 列出 DPIA 报告的主题。

3.3 使用中的个人数据
考生能够...
3.3.1 说明数据生命周期管理（DLM）的目的。
3.3.2 解释说明数据留存和数据最小化。
3.3.3 说明何为 cookie 及其用途。
3.3.4 描述反对个人数据用于直接营销目的的处理，包括剖析的权利。

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
adequate	充分的
appropriate technical and organizational measures	适当的技术和组织措施
authenticity	真实性
availability	可用性
awareness	意识
benchmark	基准
binding corporate rules (BCR)	企业约束性规则（BCR）
certification / certification bodies	认证 / 认证机构
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 / consistency mechanism	一致性 / 一致性机制
constitution	章程
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 concerning health	健康相关数据
data lifecycle management (DLM)	数据生命周期管理（DLM）
data privacy breach response plan	数据隐私泄露应对计划
Data Privacy Framework	数据隐私框架[2]
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 / 基于设计的隐私
data protection impact assessment (DPIA)	数据保护影响评估（DPIA）
data protection officer (DPO) • designation • position • tasks	数据保护官（DPO） • 任命 • 职位 • 任务
data subject	数据主体
data transfer	数据传输

[2] 2023 年 7 月欧盟通过了 欧盟-美国数据隐私框架充分性决定

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
derogation	豁免
documentation obligation	文档化义务
enforcement • administrative fines • administrative penalties • criminal penalties • dissuasive penalties • effective penalties • proportionate penalties	执行 • 行政罚款 • 行政处罚 • 刑事处罚 • 劝诫性处罚 • 有效性处罚 • 相称性处罚
enterprise	企业
EU types of legal act • decision • directive • opinion • recommendation • regulation	欧盟法规类型 • 决定 • 指令 • 意见 • 推荐 • 规定
European Data Protection Board • chair • confidentiality • independence • procedure • reports • secretariat • tasks	欧洲数据保护委员会 • 主席 • 保密 • 独立 • 程序 • 报告 • 秘书处 • 任务
European Data Protection Supervisor (EDPS)	欧洲数据保护主管（EDPS）
European Economic Area (EEA)	欧洲经济区域（EEA）
European Union legal acts on data protection	欧盟关于数据保护的法案
exchange of information	信息交换
exemption	豁免
filing system	归档系统
General Data Protection Regulation (GDPR)	《通用数据保护条例》（GDPR）
governing body	治理机构
group of undertakings	企业集团
information society service	信息社会服务
international organization	国际组织
joint controllers	联合控制者
judicial remedy	司法救济
lawfulness of processing	处理合法性
legal basis	法律依据
legitimate basis (GDPR recital 40)	合法基础（GDPR 序文 40）
legitimate ground (GDPR Article 17(1c), Article 18(1d), Article 21(1))	合法依据（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
notification obligation	通知义务
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	有关刑事定罪和罪行的个人数据
principles relation to processing of personal data (GDPR, Article 5) • accountability • accuracy • confidentiality • data minimization • fairness • integrity • lawfulness • purpose limitation • storage limitation • transparency	有关处理个人数据的原则（GDPR 第 5 条） • 可问责 • 准确性 • 保密 • 数据最小化 • 公正 • 完整性 • 合法性 • 目的限制 • 存储限制 • 透明度
prior consultation	事前协商
privacy	隐私
privacy analysis	隐私分析
privacy officer / chief privacy officer	隐私官 / 首席隐私官
processing (of personal data)	（个人数据）处理
processing situations • 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	处理场景： • 教会和宗教协会和数据保护规则 • 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 • 身份识别号码 • 保密义务 • 官方文件的公共查阅
processing which does not require identification	不涉及身份的处理
processor	处理者
profiling	剖析
proportionality, the principle of	相称性原则
pseudonymization	假名化
recipient	接收者
relevant and reasoned objection	相关和合理的反对
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 • restrictions • 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 • 多方式 • 通知义务 • 修正和删除 • 处理限制 • 限制 • 获偿权 • 反对权 • 透明度
rules of procedure	程序规则
security breach	安全漏洞
security incident	安全事件
security of personal data	个人数据安全
security of processing	处理安全性
sensitive data	敏感数据
service provider	服务提供商
seven principles for privacy by design	基于设计的隐私的七项原则
special categories of personal data • 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	个人数据的特殊类别 • 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	涉及的监管机构
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 • adequacy decision • appropriate safeguards • binding corporate rules • derogations • disclosures • international protection of personal data	向第三国和国际组织传输个人数据 • 充份性决定 • 适当的保障措施 • 约束性企业规则 • 减损 • 披露 • 个人数据的国际保护
vulnerability	脆弱性

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. L. Besemer
Privacy and Data Protection based on the GDPR Van Haren Publishing, 2020
ISBN: 978 94 018 0676 3 (paperback)
ISBN: 978 94 018 0677 0 (e-book)
ISBN: 978 94 018 0678 7 (ePub)

可选教材

B. European Commission
General Data Protection Regulation (GDPR) Regulation (EU) 2016/679) Regulation of the European Parliament and the Council of the European Union. Brussels, 6 April 2016，获取方式：http://eur-lex.europa.eu（pdf）或 https://gdpr-info.eu/（网页）

C. A. Cavoukian
Privacy by Design – The 7 Foundational Principles
Information & Privacy Commissioner, Ontario, Canada
https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

D. A. Calder
EU GDPR, A pocket guide
IT Governance Publishing
ISBN 978-1-84928-855-2（纸质版）
ISBN 978-1-84928-857-6（电子版）

备注

可选教材仅作为参考和深度学习使用。

因为考试文献教材提供了 GDPR 的足够知识，因此 GDPR 原文（来源 B）并非主要考试文献教材。考生应熟谙其他考试文献教材中对 GDPR 的引述。

教材考点分布矩阵

考试要求	考试明细	文献参阅	GDPR 参阅	ISO/IEC 27701 参阅
1. 隐私和数据保护基础和法规				
	1.1 定义	A，第 1 章	序文 1，2， 第 96-99 条	*无引述*
	1.2 个人数据	A，第 1 章， 第 2 章， 第 3 章， 第 4 章， 第 5 章	第 4.1(a)条， 第 9.1 条， 第 17 条， 第 4.10 条	第 7.2.2 款， 第 7.3.6 款
	1.3 合法依据与目的限制	A，第 3 章， 第 4 章	第 6.1 条， 第 24 条	第 7.2.2 款
	1.4 合法处理个人数据的进一步要求	A，第 3 章	第 25 条， 第 27-32 条，第 5 条	第 5.2.1 款. *标准通篇引用了第 5 条*
	1.5 数据主体权利	A，第 5 章	第 15 条， 第 16 条， 第 17 条， 第 18 条， 第 20 条， 第 21 条， 第 22 条	第 7.2.2 款， 第 7.3.2 款， 第 7.3.6 款， 第 7.3.9 款， 第 7.3.10 款， 第 7.5.1 款
	1.6 数据泄露和相关程序	A，第 11 章	第 4(12)条， 第 33 条， 第 34 条	第 6.13.1.5 款
2. 组织数据保护				
	2.1 数据保护对组织的重要性	A，第 2 章， 第 4 章， 第 10 章， 第 11 章， 第 12 章	第 7 条， 第 8 条， 第 13 条， 第 25(1)条， 第 30 条， 第 83 条	第 6.11.2.1 款， 第 6.11.2.5 款， 第 7.2.3 款， 第 7.2.4 款， 第 7.2.5 款， 第 7.2.8 款， 第 7.3.2 款， 第 7.3.6 款， 第 7.3.10 款， 第 7.5 款， 第 8.2.6 款， 第 8.5.2 款， 第 8.5.3 款
	2.2 监管机构	A，第 12 章	第 33 条， 第 34 条， 第 36 条	第 5.2.2 款， 第 6.13.1.1 款， 第 6.13.1.5 款， 第 7.2.5 款
	2.3 个人数据传输到第三国	A，第 8 章 第 9 章	第 29 条， 第 30 条， 第 45 条	第 7.2.8 款， 第 7.5 款， 第 8.2.2 款， 第 8.2.6 款

	2.4 企业约束性规则（BCR）与合同中的数据保护	A，第 2 章，第 9 章	第 24 条，第 28 条，第 47 条	第 5.2.1 款，第 6.12.1.2 款，第 7.2.6 款，第 7.2.8 款，第 7.5.1 款，第 8.5 款
3. 数据保护实践				
	3.1 与信息安全相关的，基于设计的和默认的数据保护	A，第 2 章	第 25 条	第 B.8.4 节，第 6.11.2.1 款，第 6.11.2.5 款，第 7.4.2 款
	3.2 数据保护影响评估（DPIA）	A，第 10 章	第 35 条	第 5.2.2 款，第 7.2.5 款，第 8.2.1 款
	3.3 使用中的个人数据	A，第 3 章，第 5 章，第 6 章，第 7 章	*无引述*	第 B.8.2.3 节

联系 EXIN

www.exinchina.cn

info.china@exin.com

WeChat ID: EXINCH