

# ISO27701隐私信息管理体系简介

产品名称	ISO27701隐私信息管理体系简介
公司名称	贯标集团
价格	.00/件
规格参数	
公司地址	南京市仙林大道10号三宝科技园1号楼B座6层
联系电话	4009992068 13382035157

## 产品详情

### ISO27701 隐私信息管理体系

“

ISO27701是对ISO27001信息安全管理和ISO27002安全控制的隐私扩展，全称《安全技术—扩展ISO27001和ISO27002的隐私信息管理—要求与指南》，是ISO标准委员会以ISO 27001为基准，以ISO27552为蓝本，建立发布的隐私信息管理体系标准，为保护个人隐私提供指导。

ISO27701标准的发布，填补了隐私信息管理体系的空白，将隐私保护的原则、理念和方法，融入到信息安全保护体系中，并且对PII控制者和PII处理者进行了较为详细且落地性强的规定，给企业在隐私保护和信息安全方面给出了指导建议。

“

### 认证价值

“

ISO27701是在隐私保护方面对ISO/IEC27001信息安全管理和ISO27002安全控制的进一步拓展，通过提供

隐私保护指引，明确角色和责任，对于降低企业隐私合规难度，便于企业提供合规证明，增强社会各方信任具有重要意义，具体收益如下：

满足合规要求：通过明确对PII处理者生命周期的隐私保护要求，可以明确隐私保护管理合规目标，减轻组织合规负担的同时降低组织合规风险

完善数据安全能力和风险管理：提高组织管理数据安全和隐私风险的能力，通过流程分析，在流程的输入、输出、控制各个环节中，识别、分析、验证隐私保护需求，减少甚至消除隐私泄露的风险

增强对个人信息管理的信任：业务伙伴通常会要求PII处理者提供相关证据，来证明其产品能符合适用的隐私管理体系要求。通过得到授权的第三方机构对PII处理者进行审计验证，可以极大地降低合规沟通成本，有助于向公众传达组织的可信度

“

## 应用背景

“

数据滥用、数据窃取、隐私泄露以及“大数据杀熟”等数据安全问题呈现爆发趋势。在此背景下，全球各个国家纷纷颁布相关法律法规，对数据安全和隐私保护相关问题进行严格的规范与引导。2018年欧盟GDPR《General Data Protection Regulation》生效，2021年，欧盟在GDPR中采信由监管机构认可或国家认可机构认可的第三方认证机构颁发的认证证书。2017年6月1日，《中华人民共和国网络安全法》（通常简称《网安法》）颁布实施，2021年11月1日，我国的《个人信息保护法》生效。为规范组织内部个人隐私信息安全管理，满足各国相关隐私保护法律法规的要求，ISO/IEC27701认证需求越来越明显。

“

## ISO27701认证对象

“

标准设计的目的在于借助更多的要求增强现有 ISMS，以建立、实施、维护和持续改进隐私信息管理体系 (PIMS)。标准概述了适用于个人身份信息 (PII) 控制者和 PII 处理者的框架，以有效管理隐私控制，降低个人隐私权面临的风险。它适用于所有类型和规模的组织，包括公共和私营公司、政府实体以及非盈利组织。

“

## ISO27701与ISO27001的关系

“

ISO / IEC 27701 是ISO / IEC

27001信息安全管理隐私扩展，是由其衍生的。由于许多组织已经建立了基于ISO/IEC 27001的信息安全管理体系(ISMS)，并以ISO/IEC 27002为指导，为保护隐私奠定了基础。

ISO/IEC 27701通过附加要求来增强现有的信息安全管理体系，以便建立、实施、维护和持续改进隐私信息管理系统(PIMS)。

“

## ISO27701认证的流程

“

在完成ISO27701体系商务合同和体系建立和试运行后，将邀请第三方认证机构进行现场审核，具体流程如下：

步骤1 – 根据组织的规模及业务类型提供定制化的建议，在您签署建议书后，审核即可开始。

步骤2 – 提供可选择的针对准备情况与薄弱环节的“预审”服务。

步骤3 – 正式审核。第一阶段——准备情况评估：对组织建立的文件化体系及其他重要体系进行评估，提出不符合项。办理ISO27701隐私信息管理体系认证流程

步骤4 – 第二阶段：包括与工作人员面谈、文件记录的检查以及对工作实践的现场考察，提出审核发现。审核合格后会签发证书。

步骤5 – 根据合同，每一年对体系和整改计划的实施进行监督审核。

步骤6 – 证书签发满3年期后，实施再认证审核。