

市场监管行业标准编制说明

(参考格式)

1、基本信息				
1.1 标准名称	中文	市场监管行业数据隐私计算总体要求		
	英文	General requirements for privacy computing of market supervision industry data		
1.2 与国际标准和国外先进标准一致性程度情况	<input type="checkbox"/> 等同采用 <input type="checkbox"/> 修改采用 <input type="checkbox"/> 非等效采用 <input checked="" type="checkbox"/> 未采用	标准编号		
		英文名称		
		中文名称		
1.3 任务来源	批准立项的文件名称和文件号	市场监管总局关于下达2023年度市场监管行业标准制订计划项目的通知(国市监办发〔2024〕17号)	计划编号	2023MR0010
1.4 制(修)订	<input checked="" type="checkbox"/> 制定 <input type="checkbox"/> 修订(被修订标准名称及编号:)			
1.5 起止时间	2024年2月---2026年2月			
1.6 标准起草单位	中国科学院信息工程研究所、中国网络安全审查认证和市场监管大数据中心、河北省市场监督管理局、南阳市市场监督管理局、江西省市场监督管理局、江西省质量和标准化研究院、厦门市市场监督管理局、西安电子科技大学、中央网信办数据与技术保障中心、国家市场监督管理总局竞争政策与评估中心、中国轻工业信息中心、航天信息股份有限公司、京东城市(北京)数字科技有限公司、北京市计算中心有限公司、中移(苏州)软件技术有限公司等			
1.7 起草团队				

1.8 标准体系表内编号	
1.9 调整情况	标准参编单位调整：增加了中国网络安全审查认证和市场监管大数据中心、中央网信办数据与技术保障中心、竞争政策与评估中心、中国轻工业信息中心
2、背景情况	
2.1 目的、意义 (工作开展背景及要求)	<p>《数据安全法》《个人信息保护法》颁布实施，数据安全和个人信息保护是国家互联网+、数字经济和数据共享等战略的安全保障。中央全面深化改革委员会审议通过了《关于构建数据基础制度更好发挥数据要素作用的意见》，提出加快建设数据基础制度，以促进数据高效流通使用、赋能实体经济。这将极大地加快数据要素的市场化流通，提升数字经济规模。但数据共享和安全需要协同发展，数字技术和国民经济、社会发展融合得越深，面临的数据安全和个人信息保护的挑战也就越大。在维护国家数据安全、个人信息保护和商业秘密的同时，打破数据孤岛、畅通经济大动脉，就必须将数据安全和隐私保护贯穿于数据开发和流通的全过程。</p> <p>市场监管行业涉及市场主体统一登记注册，负责和指导市场监管综合执法，负责反垄断统一执法、监督管理市场秩序、宏观质量管理、产品质量安全监督管理、特种设备安全监督管理、食品安全监督管理综合协调、食品安全监督管理、统一管理计量、统一管理标准化、统一管理检验检测等工作，上述业务工作开展过程中，涉及众多企业信息，而这些企业的业务和数据资产中往往包含了众多用户的各类隐私信息，一旦在采集、传输、存储、处理、使用、销毁等全生命周期的不同环节中失控，轻则危害用户隐私，重则影响企业发展，甚至威胁国家安全，因此亟待从市场监管角度予以规范约束。</p> <p>隐私计算涵盖了信息搜集者、发布者和使用者在信息产生、感知、发布、传播、存储、处理、使用、销毁等全生命周期过程的所有计算操作，并包含支持海量用户、高并发、高效能隐私保护的系统设计理论与架构。隐私计算可以全生命周期地有效保护个人信息，打破数据孤岛，支持多系统融合的数据利用，安全充分的释放数据价值。</p> <p>本项目拟以市场监管行业为应用背景，重点关注含有用户隐私信息的数据在产生、感知、发布、传播、存储、处理、使用、销毁等全生命周期管理与监管问题，结合所涉及到的个人信息保护和权益保障的技术需求，计划制定市场监管行业数据隐私计算总体要求，主要包括市场监管行业管理用户隐私信息时的总体要求、市场监管行业隐私计算的总体技术框架与监管框架、市场监管行业隐私信息处理系统架构、隐私信息分享与利用过程中的要求等内容，进而规范和指导市场监管行业对隐私信息的全生命周期保护和监管要求。</p>

<p>2.2 与国内外相关标准、文献的关系</p>	<p>隐私计算是我国学者 2015 年在国际上首先提出的，经过几年的研究已基本完善。当前国家已将数据作为一种新的生产要素，通过数据要素市场加速数据流通、释放数据价值、促进数字经济发展的需求非常迫切，隐私计算是解决数据流通中个人信息保护的关键理论基础。</p> <p>为了促进隐私计算的技术推广应用，推动《数据安全法》《个人信息保护法》的落地实施，发挥隐私计算对个人信息保护的作用，亟需制定隐私计算的标准体系，以规范和引领正确使用隐私计算技术，避免将部分学者提出的同态加密、安全多方计算等技术纳入隐私计算范畴，误导隐私计算产业技术应用。此外，本标准还将支撑第三方评测机构和企业的自监管和网信主管部门的监管。</p> <p>国际标准制定方面，ISO/IEC 27701 是国际标准化组织发布的隐私信息管理体系标准，全称《安全技术—扩展 ISO/IEC 27001 和 ISO/IEC 27002 的隐私信息管理—要求与指南》，该标准提供了一个通用的隐私信息管理框架，包括组织机构应遵循的隐私原则和要求，以及实施和评估隐私控制的指南，适用于所有类型和规模的组织，包括公共和私营公司、政府机构和非盈利组织。然而，该标准缺少对个人信息保护各环节具体实现方面的技术要求，尚未形成体系化标准。此外，国内外研究者目前正在联合探讨在 IEEE 推动隐私计算标准的制定立项工作。</p> <p>国内标准制定方面，中国通信标准化协会组织制定 CCSA TC601《隐私计算多方安全计算产品性能要求和测试方法》、《隐私计算 联邦学习产品性能要求和测试方法》，这些标准虽然冠以隐私计算的名称，但实际内容都是同态加密、安全多方计算、联邦学习等密码学、人工智能等方面的内容，并不是真正的隐私计算，难以解决泛在环境下传播的个人信息全生命周期保护问题；在个人信息安全规范方面，我国已立项制定的 GB/T 37964-2019《个人信息去标识化指南》、GB/T 35273-2020《个人信息安全规范》、GB/T 39335-2020《个人信息安全影响评估指南》、JR/T 0171-2020《个人金融信息保护技术规范》等国家标准和行业标准只是聚焦个人信息保护的部分热点，尚未形成体系化标准。</p>
<p>3、编制过程</p>	

<p>3.1 分工情况</p>	<ol style="list-style-type: none"> 1. 中国科学院信息工程研究所 牵头单位，负责全面统筹标准编写工作，制定整体规划和时间表。组织召开各阶段的工作会议，协调各方进度。负责标准中核心框架和关键原则的确定。 2. 中国网络安全审查认证和市场监管大数据中心 业务指导单位，对标准中涉及的各类市场监管信息进行识别、分类，确定数据使用原则。 3. 河北省市场监督管理局 标准的实施单位，对标准的可实施性进行把控。 4. 河南省南阳市市场监管综合行政执法支队 标准的实施单位，对标准的可实施性进行把控。 5. 江西省市场监督管理局 标准的实施单位，对标准的可实施性进行把控。 6. 江西省质量和标准化研究院 标准化领域专业单位，专注于标准化领域内容的编写和完善。确保该领域条款的准确性和专业性。 7. 厦门市市场监督管理局 标准的实施单位，对标准的可实施性进行把控。 8. 中国轻工业信息中心 轻工行业应用单位，组织轻工企业进行标准应用。 9. 西安电子科技大学 重要技术提供单位，参与标准内容的起草和修改。 10. 中央网信办数据与技术保障中心 作为个人信息安全合规审计主管部门，负责对标准的个人信息合规审计提供需求支撑。 11. 竞争政策与评估中心 重要技术提供单位，参与标准内容的起草和修改。 12. 航天信息股份有限公司 重要技术提供单位，参与标准内容的起草和修改。 13. 京东城市（北京）数字科技有限公司 重要技术提供单位，参与标准内容的起草和修改。 14. 北京市计算中心有限公司 重要技术提供单位，参与标准内容的起草和修改。 15. 中移（苏州）软件技术有限公司 重要技术提供单位，参与标准内容的起草和修改。
-----------------	--

3.2 起草阶段	<p>2024.02, 成立标准起草组</p> <p>2024.02-2024.03, 组织进行技术调研和资料收集</p> <p>2024.03, 于中国科学院信息工程研究所召开草稿研讨会, 对标准起草框架、内容进行研讨, 并形成初稿</p> <p>2024.04-2024.06, 继续完善草案</p> <p>2024.07, 于中国科学院信息工程研究所召开针对草案的专家评审会, 并根据专家意见进行修改, 并形成征求意见稿</p>
3.3 征求意见阶段	<p>2024.11, 拟定于 2024.11 开始面向社会征求意见</p>
3.4 标准审查阶段	<p>2025.01-2025.02, 拟定于 2025.01 开展标准审查</p>
<p>4、主要技术内容的确定</p>	

本标准规定了市场监管数据中隐私信息全生命周期过程的计算操作、隐私计算框架、隐私信息抽取与度量、隐私度量动态调整、隐私延伸控制、隐私按需保护、保护效果评估、存证与取证等框架核心组件的功能。主要包括：

1、术语和定义

本章节给出了“隐私信息”等术语的定义。

2、概述

本章节描述了数据隐私保护的目标、隐私信息全生命周期过程的计算操作，给出了隐私计算总体框架和参与者。

3、隐私计算框架

本章节概述了隐私计算框架的组成，包括：隐私信息抽取与度量、隐私度量动态调整、隐私延伸控制、隐私按需保护、保护效果评估、存证与取证等。

4、隐私信息抽取与度量

本章节对市场监管行业数据中的隐私信息抽取域度量提出了要求，包括隐私信息抽取、隐私信息分类、隐私信息度量三个方面进行了要求。

5、隐私度量动态调整

本章节针对识别隐私信息所属的应用场景，并针对性地动态调整隐私信息分量的敏感度或保护程度并提出了要求，包括场景识别、度量调整。

6、隐私延伸控制

本章节提出隐私延伸控制对数据泛在流通与共享过程中脱敏、存储、使用、交换、发布、删除等提出操作约束要求，包括：延伸控制策略生成、控制策略可控传递、控制策略迭代调整、策略执行可信验证。

7、隐私按需保护

本章节提出根据隐私信息所有者或隐私信息提供者的脱敏要求、隐私信息模态以及隐私信息接收者的隐私保护能力等因素，对隐私信息分量进行场景自适应的脱敏和删除操作要求，包括脱敏算法能力评估、按需脱敏、按需删除。

8、保护效果评估

本章节提出对从脱敏后的隐私信息中恢复损失信息的难度，或者恢复已删除隐私信息的可能性进行评价的要求，包括单次脱敏效果评估、基于数据挖掘的脱敏效果评估、脱敏系统效果评估、删除效果评估。

9、存证与取证

本章节对隐私计算其他功能组件的运行、隐私信息的处理等情况进行可信记录，以便于开展内部监测、或者按照法律法规接受外部监管者的合规审查、侵权行为追踪溯源的服务请求提供必要的证据和技术接口，包括存证收集、存证存储、证据生成。

5、验证情况（适用时填写）

5.1 验证单位情况	验证单位	验证人员	验证时间
			年 月 日

			年 月 日
			年 月 日
			年 月 日
5.2 验证过程			
5.3 验证数据分析			
5.4 验证评价			
5.5 其他应说明的情况			
6、附加说明（可选）			
6.1 宣贯标准的建议			
6.2 修订和废除现行有关标准的建议			

6.3 作为强制性标准或推荐性标准的建议					
6.4 其他需要说明的情况					
6.5 参考文献					
联系人	张玲翠	联系电话	18500152861	电子邮箱	zhanglingcui@iie.ac.cn
<p>注：1.本格式的通用部分为第 1 章、第 2 章、第 4 章和第 6 章。 2.第 5 章和第 6 章为可选项，其余为必填项。</p> <p style="text-align: right;">编写日期： 年 月 日</p>					