隐私计算 脱敏算法能力评估技术要求

编 制 说 明

标准起草工作组

2024年8月

1. **目的意义**

数据作为“信息时代的石油”，已成为国家基础性战略资源，在推动经济高质量发展的同时，也带来了数据泄露等安全问题。隐私计算的算法能力评估缺乏统一的标准和方法，增加了数据安全的风险，对国家信息安全构成了威胁。

2020年由国家发改委发布的《关于加快构建全国一体化大数据中心协同创新体系的指导意见》中指出要开展通信网络安全防护工作，同步规划、同步建设和同步运行网络安全设施，提升应对高级威胁攻击能力。加快研究完善海量数据汇聚融合的风险识别与防护技术、数据脱敏技术、数据安全合规性评估认证、数据加密保护机制及相关技术监测手段等。2022年工信部发布的《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》提出要积极发展检测、评估、认证服务。建立数据安全检测评估体系，加强与网络安全等级保护评测等相关体系衔接。鼓励检测、评估、认证机构跨行业跨领域发展，推动跨行业标准互通和结果互认。推动检测、评估等服务与数据安全相关标准体系的动态衔接。

因此，开展脱敏算法能力评估是确保数据安全检测评估的一项重要工作，通过脱敏算法能力评估将有助于全面了解和掌握脱敏算法的脱敏能力和存在的问题，进而有针对性的补齐短板，推动隐私计算与数据安全能力建设协同发展。尤其在我国提高数据安全管理和个人信息保护水平的过程中， 这项工作是非常重要和必不可少的。其中，脱敏算法能力评估技术要求的关键作用在于：

1、社会各方都亟需可以统一评估脱敏算法能力的技术要求，以实现规范脱敏算法在数据处理中的应用流程和操作规范。

2、社会各方通过对脱敏算法能力的评估，可以有效降低敏感数据泄露和滥用的风险，保障个人隐私和敏感信息的安全。

3、社会各方通过对脱敏算法能力的评估，有助于提高数据安全信任，促进数据共享和合作，推动数据的开放和创新应用。

4、脱敏算法评估技术要求的制定有助于提升国家信息安全防护能力，防范数据泄露和滥用对国家安全的威胁。

5、各国缺乏一套统一的规范化的脱敏算法能力评估标准，用以促进国际间数据安全技术的交流与合作。

1. **任务来源**

在国际上，一些国际标准组织和技术机构已经制定和发布了脱敏算法能力评估的相关标准和指南。例如，ISO/IEC 27002《信息安全、网络安全和隐私保护—信息安全管理》和ISO/IEC 29101《信息技术—安全技术—隐私架构框架》等标准，提供了信息安全管理与隐私架构框架的要求和指南，其中包括了隐私计算和脱敏技术的相关内容。GDPR（《通用数据保护条例》）规定了个人数据的处理方式，包括了对个人隐私信息进行脱敏的要求和脱敏算法能力评估的相关内容。

在国内，一些行业组织和标准化机构也开始关注脱敏效果评估的标准制定和实践。例如，国家市场监督管理总局与国家标准化管理委员会发布的《信息安全技术 个人信息安全规范》标准，规定了个人隐私信息处理活动的原则和安全要求，其中包括了脱敏算法能力的相关内容。此外，标准制定机构和一些行业组织(如金融行业、医疗保健行业等)也开展了脱敏算法能力评估相关的指南和标准的实践研究工作， 完善脱敏算法能力评估的方法和技术。

并且，进行脱敏算法能力评估能够明确脱敏算法的算法类别、优势以及不足，有助于进一步采取有针对性的改进措施，持续改进和提高脱敏算法的能力和水平，匹配脱敏算法的应用场景。脱敏算法能力评估需保障不同的单位和团体所采用的脱敏算法具有合规性和一致性，谨防跨系统中的隐私泄露问题，预防全社会各系统隐私保护的短板效应。

目前，国内外还未对脱敏算法能力评估进行标准化，社会各方在对脱敏算法能力评估的实践中积累了丰富的经验，但存在维度考虑不足，体系化程度不足等问题，亟需制定相关标准，用以体系化、全面化地对实践进行指导，完善脱敏算法能力评估技术要求。制定脱敏算法能力评估技术要求标准将有助于解决这一难题，推动数据安全和隐私保护的发展、实现评估的系统化和全面性；同时，标准也有助于进行脱敏算法能力评估的实践，从而进一步维护数据安全，促进数据共享与应用。

1. **编制过程**

1) 2023年4月5日，规范研制正式启动会。标准牵头单位对前期的研究工作进行了汇报。确定了标准的研究思路和分工。

2) 2023年4月15日，提交项目立项申请书。

3) 2023年4月16日至2022年6月24日，期间进行了多次标准工作组内部讨论，并针对标准大体框架与内容方向进行了修改与调整，形成第一版标准草案。

4) 2023年7月1日，召开立项评审会，邀请专家对草案给出建议。

5) 2023年7月4日至2022年11月4日，期间进行了多次标准工作组内部讨论，针对标准内容进行了细节的修改与调整。

6) 2023年11月6日，形成第二版标准草案，并召集了标准草案的内部闭门研讨会。

7) 2024年1月30日，继续完善标准草稿，形成第三版。

8）2024年6月28日，召开专家评审会，邀请专家对修改后的版本进行评审。

9）2024年8月，形成征求意见稿。

1. **主要内容技术指标确立**

本标准规范了脱敏算法能力评估技术要求的概述、脱敏算法能力评估通用技术要求及脱敏算法能力评估的报告要求。详情如下：

1、概述：脱敏算法能力评估技术要求的概括性描述，其中包括目的、算法评估的基本原则和用途三个方面。

2、脱敏算法能力评估通用技术要求：用以评估脱敏算法能力的通用技术要求，包括脱敏算法分类、脱敏算法能力评估指标体系、脱敏算法可逆性评估、脱敏算法信息偏差性评估、脱敏算法信息损失性评估、脱敏算法复杂性评估六个部分。

3、脱敏算法能力评估的报告要求：用以规范生成的脱敏算法能力评估报告，帮助主管监管部门、第三方评估机构灯组织对隐私信息脱敏处理活动进行监督、管理和评估，包括形成评估报告的目的、评估报告的组成内容、评估项目概述组成内容、评估指标、单项评估结果分析、整体评估组成内容及等级评估结论组成内容七个部分。

本文件适用于规范各类组织的隐私信息脱敏处理活动，也可为主管监管部门、第三方评估机构等组织对隐私信息脱敏处理活动进行监督、管理和评估提供参考。

本标准牵头单位为西安电子科技大学，参与单位包括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、北京理工大学、四川昊华锐恒科技有限公司、成都西电网络安全研究院、长春吉大正元信息技术股份有限公司、国网上海研究院、普华永道商务咨询(上海)有限公司等。

1. **与相关法律法规和国家标准的关系**

本标准的总体结构和编写方法按照GB/T 1.1-2020《标准化工作导则 第一部分：标准化文件的结构和起草规则》的规定执行。本标准参考的相关法律、法规和标准文件如下：

GB/T 35273—2020《信息安全技术 个人信息安全规范》

GB/T 25069-2022《信息安全技术 术语》

GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》

GB/T 37964-2019《信息安全技术 个人信息去标识化指南》

《中华人民共和国网络安全法》

《中华人民共和国数据安全法》

《中华人民共和国个人信息保护法》

《关键信息基础设施安全保护条例》

《网络安全审查办法》

《网络数据安全管理条例（征求意见稿）》

目前尚未有类似的脱敏算法能力评估技术要求的国家标准，本标准内容与现有国家标准不存在冲突，相关术语定义与其他网络安全国家标准保持一致。