隐私计算 脱敏控制技术要求

编 制 说 明

标准起草工作组

2024年8月

1. **目的意义**

2022年，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》，提出加速建设数据基础制度，以促进数据要素的高效合规流通使用，在保护公民个人信息权益的前提下，挖掘数据价值，赋能实体经济。

然而，随着互联网和数字技术的普及，大量个人信息被收集和处理，这些信息收集和使用，虽然极大促进了技术的进步，但也导致了个人隐私泄露和滥用。未经授权的数据访问、数据泄露事件和对个人信息的商业化使用已引发了全球性的关注和担忧。在数字经济时代，数据共享和数据安全需要协同发展，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。

脱敏控制是指个人信息流转过程中，针对信息在不同个人信息控制者之间流转的各环节（例如：采集、分享、交换等过程），结合不同信息主体，不同处理阶段的差异化脱敏要求，对隐私信息进行合理控制和迭代脱敏操作的技术。为了促进数据共享和数据安全需要协同发展，开展脱敏控制相关的标注制定，对于确保数据的合规跨域流通至关重要。通过制定脱敏控制相关标准，将有助于全面梳理信息跨域流通共享过程中存在的问题，进而针对个人信息控制者提出技术要求，推动数据要素流通机制与个人信息权益保障技术体系的协同发展。尤其在我国全面加速建设数据基础制度过程中，这项工作是非常重要和必不可少的。其中，脱敏控制技术要求的关键作用在于：

1、业界亟需面向数据要素流通场景下的脱敏控制技术框架，以便支撑隐私保护合规产品的开发。

2、业界缺乏对脱敏控制技术的全面了解，导致数据要素流通过程中，因为短板效应引发的隐私泄露问题。

3、脱敏控制技术要求的制定，有助于提升个人信息权益保障能力，防范数据泄露和滥用对个人合法权益的侵犯。

4、主管监管部门在了解数据要素流通场景下脱敏操作方面的抓手不够成熟，无法支撑相关决策的制定。

5、世界范围内缺乏一套统一的规范化的脱敏控制流程，以促进国际间数据安全技术的交流与合作。

1. **任务来源**

在当前我国个人信息权益保障技术体系建设过程中，虽然存在一些与脱敏相关的标准，但这些标准的关注点各异。例如：单一数据域内的脱敏流程规范化问题、脱敏算法能力评估问题、脱敏算法脱敏效果评估问题以及行业性的脱敏流程规范化等。既有标准在一定程度上促进了脱敏技术标准化与规范化，但无法有效针对数据要素跨域流通场景下的个人信息保护问题。

在当前全球化和数字化的经济环境中，数据的跨域流通成为了推动商业和技术创新的关键动力。对于个人信息控制者而言，充分利用各型业务流程中采集的个人数据，已经成为提升服务效率、优化资源配置、增强客户满意度的重要手段。然而，这一过程中对用户数据的收集、处理和分析必须建立在严格遵守法律法规、保护信息安全和数据安全的基础之上。

目前，国内外尚未制定出数据跨域流通场景下个人信息控制者应遵循的脱敏控制技术标准。这一空缺不仅限制了各行业数据利用和服务创新方面的潜力，也增加了各行业在处理跨域数据时面临的合规风险。因此，作为隐私计算技术体系的重要组成部分，制定一套脱敏控制技术标准，特别是从数据要素跨域流通的角度出发，对于个人控制者合规地收集、使用和保护用户数据，促进数据安全和个人信息保护，具有重要意义。

1. **编制过程**

1）2023年3月2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3月29日，提交项目立项申请书。

3）2023年4月3日至2023年5月20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5月25日，召开立项评审会，邀请专家对草案给出建议。

5）2023年7月10日至2023年12月10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12月16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**

本标准描述了个人信息流转传播下，隐私信息全生命周期脱敏控制技术要求，规范了脱敏控制合规性验证、违反脱敏控制违规事件处置与通报、脱敏控制监管接口的技术要求等。详情如下：

1、脱敏控制概述：描述了脱敏控制的目的，应遵循的基本原则以及脱敏控制的流程，主要包括：脱敏意图理解、脱敏控制集合生成、脱敏算法选择、脱敏算法执行以及脱敏控制存证。

2、脱敏控制通用技术要求：针对脱敏控制流程的各个阶段，提出针对性的技术要求。主要包括：脱敏意图理解技术要求、脱敏控制集合生成的技术要求、脱敏算法选择技术要求以及脱敏控制存证技术要求。

3、脱敏控制的合规性验证技术要求：用以验证个人信息控制者对接收到的信息进行脱敏操作过程中，是否按照预定约束进行了脱敏控制集合生成、脱敏操作以及存证。

4、脱敏控制监管接口技术要求：为了便于对个人信息控制者的脱敏控制过程进行合规监管，个人信息控制者应提供面向主管监管机构的存证接口、通报与处置接口，以便后者对个人信息控制者的操作进行监管、违规通报以及处置。

本标准适用于规范各类组织在个人信息流转下的个人信息脱敏处理活动，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进行监督、管理、评估提供参考。

本标准牵头单位为中国科学院信息工程研究所，参加单位包括西安电子科技大学、中国网络安全审查认证和市场监管大数据中心、电子科技大学、国网智能电网研究院有限公司、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、普华永道商务咨询(上海)有限公司、北京市计算中心有限公司、中移(杭州)信息技术有限公司等。

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 22239-2019 信息安全技术 信息系统安全等级保护基本要求

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

《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》

目前尚未有类似的脱敏控制相关的国家标准，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。