隐私计算 总体框架

编 制 说 明

标准起草工作组

2024年8月

1. **目的意义**

随着大数据、人工智能技术的发展，数据成为生产要素，数据流通利用成为促进数字经济发展的迫切需求。党和国家通过出台《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》等文件，引领促进数据要素的泛在流通。数据要素流通已上升为国家重大发展战略。

与此同时，个人隐私保护与数据流通之间的矛盾愈发凸显。泛在互联的数据共享加大了隐私信息在不同信息系统中有意或无意留存的可能性，个人信息保护面临的问题与日俱增。世界各主要国家和经济体高度重视公民的个人信息权益保障问题。例如：欧盟颁布了《通用数据保护条例》（GDPR），美国颁布了《加州隐私权法案》，我国先后颁布《数据安全法》，《个人信息保护法》等。

隐私计算技术旨在为流通共享的数据提供全生命周期供保护，成为数据共享和流通中至关重要的一环。隐私计算的目标在于构建一个覆盖隐私信息全生命周期的隐私保护体系，确保隐私信息在不同系统下不同处理环节均能得到有效保护，支撑隐私信息的泛在受控共享和流通利用。因此，隐私计算发挥着至关重要的作用：

（1）促进数据要素流通。在确保数据安全和个人隐私的前提下，隐私计算总体框架可以保证隐私信息出域的全生命周期保护，增强公众对数据使用的信任感，推动基于数据的服务业态创新，强化数据作为关键生产要素的作用，为数字经济的健康持续发展奠定坚实的基础。

（2）助企业降本增效。通过制定并实施隐私计算总体框架标准，指导企业在数据保护与处理上实现成本节约与效率提升。标准化的隐私计算框架为企业提供统一的技术框架和操作指南，减少了企业采用不正确的技术方案造成的巨大额外开支，增强企业的市场竞争力，使企业在保障数据安全的同时，能更高效地进行数据分析与应用，实现业务增长。

1. **任务来源**

尽管国内外在隐私保护计算技术方面积累了一定的经验，但其通常聚焦于相对孤立的应用场景和技术点，解决特定应用场景中存在的具体问题，缺乏能够将隐私信息与保护需求一体化的描述方法及计算模型，并缺乏能实现跨系统隐私信息交换、多业务需求隐私信息共享、动态去隐私化等复杂应用场景下的按需隐私保护计算架构，无法满足复杂信息系统的隐私保护需求，导致电子商务、导航、物流、社交、数据流通利用等典型应用场景下的隐私保护问题尚未得到根本性解决。因此，隐私计算总体框架需要达到以下目的：

（1）全生命周期保护。确保隐私信息在收集、存储、使用、交换、删除、脱敏、存证与取证等全生命周期各个环节得到充分的保护

（2）一致性保护。隐私信息在多个信息系统保存时，存在短板效应和一损俱损的风险，需要实现跨系统隐私信息流转的一致性保护。

（3）支持多次传播的延伸控制。通过延伸控制机制解决多次传播场景下的受控利用。

（4）支持按需脱敏。数据流通利用时对同一隐私信息在同一应用场景的不同阶段、或者同一隐私信息在不同应用场景下实现脱敏粒度差异的按需脱敏，解决隐私信息利用与隐私保护的平衡问题。

（5）提供基于脱敏效果评估反馈的脱敏自适应改进机制。隐私脱敏和隐私挖掘博弈相长，信息系统通过脱敏效果评估可以动态调整脱敏算法及其参数选择，在满足隐私信息利用的前提供下提高隐私保护强度，减少因隐私信息脱敏控制策略长期不变而导致隐私泄露。

综上所述，隐私计算的研究动机在于构建一个覆盖隐私信息全生命周期的隐私保护体系，提出隐私计算总体框架，实现对隐私信息以及隐私信息处理者保护能力的量化，并构建基于反馈的隐私保护策略调整机制，确保隐私信息在不同系统下不同处理环节均能得到有效保护，支撑隐私信息的泛在受控共享和流通利用。

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5月25日，召开立项评审会，邀请专家对草案给出建议。

4）2023年6月11日至2023年8月15日，期间进行了多次标准工作组内部讨论，并根据专家提出的建议进行修改，形成第二版草案。

5）2023年8月20日，邀请专家对第二版草案给出建议。

6）2023年8月25日至2023年9月28日，期间进行了多次标准工作组内部讨论，并根据专家提出的建议针对草案部分内容进行了细节的修改与调整，形成第三版草案。

7）2023年10月14日，邀请专家对第三版草案给出建议。

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**

本标准包含隐私计算框架、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、存证与取证等内容。详情如下：

1、隐私计算框架：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、存证与取证等功能组件。

2、隐私信息抽取与度量：通过对采集或接收的信息进行隐私信息分量识别和抽取，然后对隐私信息分量进行分类和度量。

3、隐私度量动态调整：在隐私信息抽取与度量的基础上，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。

4、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、删除等进行操作约束。

5、隐私按需保护：用于隐私信息处理者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。

6、保护效果评估：是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。

7、存证与取证：主要是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。

本标准适用于数据泛在流通与共享过程中隐私信息全生命周期保护、跨平台/跨系统/跨域流通利用的隐私延伸控制、隐私按需保护、保护效果评估等，适用于互联网、通信等领域的企业为主体的个人信息处理者、个人信息保护产品提供商、产品评测机构、个人信息保护合规审计评估机构、认证监管机构等，为隐私信息保护、隐私计算服务安全评估提供参考。

本标准牵头单位为中国科学院信息工程研究所，参加单位包括中国科学院信息工程研究所、中国电信股份有限公司、中国网络安全审查认证和市场监管大数据中心、四川昊华锐恒科技有限公司、成都西电网络安全研究院、国网上海研究院、北京市计算中心有限公司、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 25069-2022 信息安全技术 术语

GB/T 31500-2015 信息安全技术 存储介质数据恢复服务要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

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》

《中华人民共和国个人信息保护法》

目前尚未有类似的隐私计算总体框架的国家标准，本标准术语定义与内容和现有国家标准不存在冲突。