ICS 35.240
CCS L 70

中华人民共和国国家标准化指导性技术文件

GB/Z 297—2026

人工智能　隐私计算通用框架

Artificial intelligence—General framework for privacy computing

2026-09-24 发布

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅴ
引言 …… Ⅵ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 4
5　概述 …… 5
5.1　隐私保护的目标 …… 5
5.2　隐私信息全生命周期过程的计算操作 …… 5
6　隐私计算框架 …… 7
6.1　隐私计算框架组件 …… 7
6.2　隐私计算系统的组件风险 …… 8
7　隐私信息抽取与度量 …… 8
7.1　概述 …… 8
7.2　隐私信息抽取 …… 8
7.3　隐私信息分类分级 …… 9
7.4　隐私度量 …… 9
8　隐私度量动态调整 …… 9
8.1　概述 …… 9
8.2　场景识别 …… 9
8.3　度量调整 …… 9
9　隐私延伸控制 …… 10
9.1　概述 …… 10
9.2　延伸控制策略生成 …… 10
9.3　控制策略可控传递 …… 10
9.4　控制策略迭代调整 …… 11
9.5　策略执行可信验证 …… 11
10　隐私按需保护 …… 11
10.1　概述 …… 11
10.2　按需脱敏 …… 11
10.3　按需删除 …… 12
11　脱敏算法能力评估和保护效果评估 …… 13
11.1　概述 …… 13

11.2 脱敏算法能力评估 …… 13
11.3 保护效果评估 …… 15
12 存证与取证 …… 16
12.1 概述 …… 16
12.2 存证收集 …… 17
12.3 存证存储 …… 17
12.4 证据生成 …… 17
附录 A（资料性） 出行服务应用场景示例 …… 18
A.1 概述 …… 18
A.2 出行服务中的隐私信息处理 …… 18
附录 B（资料性） 信用计算应用场景示例 …… 20
B.1 概述 …… 20
B.2 隐私信息所有者或隐私信息提供者的计算操作 …… 20
B.3 隐私信息接收者或隐私信息使用者的计算操作 …… 21
附录 C（资料性） 隐私计算特性与隐私信息描述示例 …… 22
C.1 隐私计算特性 …… 22
C.2 隐私信息六元组 …… 22
C.3 隐私信息描述六元组生成过程 …… 23
C.4 文本类隐私信息描述生成示例 …… 23
C.5 图片类隐私信息描述生成示例 …… 25
附录 D（资料性） 迭代延伸控制示例 …… 28
D.1 概述 …… 28
D.2 隐私信息全生命周期中的迭代延伸控制 …… 29
D.3 脱敏延伸控制 …… 29
D.4 删除延伸控制 …… 31
附录 E（资料性） 按需脱敏过程示例 …… 33
E.1 概述 …… 33
E.2 按需脱敏操作过程示例 …… 33
E.3 出行服务系统 …… 34
E.4 不同系统数据流转 …… 35
附录 F（资料性） 脱敏算法分类示例 …… 37
F.1 概述 …… 37
F.2 基于差分隐私技术的脱敏算法 …… 37
F.3 基于泛化技术的脱敏算法 …… 40
F.4 基于匿名技术的脱敏算法 …… 42
F.5 基于置换的脱敏算法 …… 44
F.6 脱敏算法选择操作示例 …… 46

附录 G（资料性） 脱敏效果评估示例 …… 48
G.1 概述 …… 48
G.2 单次脱敏效果评估 …… 48
G.3 基于数据挖掘的脱敏效果评估 …… 49
G.4 脱敏系统效果评估 …… 50
附录 H（资料性） 脱敏算法能力评估示例 …… 52
H.1 概述 …… 52
H.2 脱敏算法评估维度权重确定 …… 52
H.3 敏感信息属性确定 …… 53
H.4 评估指标选定 …… 54
H.5 可逆性评估 …… 54
H.6 信息偏差性评估 …… 54
H.7 信息损失性评估 …… 55
H.8 复杂性评估 …… 55
H.9 评估报告生成 …… 55
参考文献 …… 56

前　言

本文件为规范类指导性技术文件。

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本文件起草单位：中国科学院信息工程研究所、中国电子技术标准化研究院、西安电子科技大学、国家信息中心、中国移动通信集团有限公司、山东省计算中心(国家超级计算济南中心)、华中科技大学、上海交通大学、杭州安恒信息技术股份有限公司、杭州海康威视数字技术股份有限公司、北京百度网讯科技有限公司、阿里云计算有限公司、科大讯飞股份有限公司、浙江理工大学、中兴通讯股份有限公司、北京快手科技有限公司、OPPO广东移动通信有限公司、中国电力科学研究院有限公司、深信服科技股份有限公司、浪潮云信息技术股份公司、杭州萤石软件有限公司、工业和信息化部电子第五研究所、公安部第三研究所、中国科学院软件研究所、中信银行股份有限公司、北京数安行科技有限公司。

本文件主要起草人：李凤华、范科峰、李晖、张玲翠、牛犇、马骋昊、罗海宁、邱勤、叶珩、宋祁朋、吴晓明、何媛媛、邱卫东、苗春雨、林克章、王建奎、李世奇、张云畅、邹德清、赵兴文、沈剑、刘霈霖、落红卫、付艳艳、于鹏飞、叶润国、饶飞、郑鸿咚、魏光辉、刘继顺、唐鹏、李婷、徐思嘉、陈隆、何双羽、张雅楠、陈伟、刘玉红。

引　言

人工智能广泛应用加大了对多源数据动态使用的需求，同时也促进了数据流通与共享应用。支撑人工智能应用的数据包含了大量个人隐私信息，在模型训练和推理过程中依赖于多域数据共享，模型迭代训练还需要长期和不断拓展的数据更新供给，迫切需要隐私计算通用框架来保障隐私信息的全生命周期延伸控制和按需保护。

隐私计算通用框架标准旨在明确隐私保护的目标，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计算操作过程中得到体系化保护。明确隐私计算通用框架、组件风险，通过定义包含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参与者和基本功能，提供隐私计算服务的实现机制，解决跨生态圈跨平台隐私保护的一致性、隐私延伸控制策略的可信可控传递、隐私按需保护的可控性，以及根据隐私保护效果评估的结果自动反馈修正隐私延伸控制策略、修正脱敏算法及其参数选择、修正删除方法选择等问题，解决隐私计算兼容性差、生态隔离问题，降低跨平台迁移及互联互通障碍，促进跨生态圈数据泛在流通与共享过程中隐私信息全生命周期保护，帮助人工智能、互联网、通信等领域的企业有效地开发跨生态圈的隐私计算系统，提升企业个人信息保护合规水平，为完善我国人工智能应用的个人信息保护治理体系、维护个人在网络空间的合法权益提供标准化支撑。

人工智能　隐私计算通用框架

1　范围

本文件描述了隐私保护的目标、隐私信息全生命周期过程的计算操作，提出了隐私计算通用框架，给出了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、脱敏算法能力评估和保护效果评估、存证与取证等框架核心组件的功能。

本文件适用于人工智能、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。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069　信息安全技术　术语

GB/T 35273　信息安全技术　个人信息安全规范

3　术语和定义

GB/T 25069、GB/T 35273 界定的以及下列术语和定义适用于本文件。

3.1

个人信息　personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注：包含个人信息本身及其衍生信息，不包括匿名化处理后的信息。

［来源：GB/T 35273—2020，3.1，有修改］

3.2

标识符　identity

个人信息中的一个或多个属性，能实现对个人信息主体的唯一识别。

注：包括姓名、电话号码、身份证号码等信息。

［来源：GB/T 37964—2019，3.6，有修改］

3.3

准标识符　quasi-identifier

个人信息中的属性，结合其他属性能唯一识别个人信息主体。

注：常见的准标识符有：性别、出生日期或年龄、事件日期（例如入院、手术、出院、访问）、地点（例如邮政编码、建筑名称、地区）、族裔血统、出生国、语言、原住民身份、可见的少数民族地位、职业、婚姻状况、受教育水平、上学年限、犯罪历史、总收入和宗教信仰等。

［来源：GB/T 37964—2019，3.8，有修改］