匿名化技术应用指南
编制说明

（征求意见稿）

2024年7月

一、标准“范围”的内容

本文件给出了互联网业务中个人信息匿名化处理技术的应用指南，包括匿名化处理的目标与原则、实施框架、需求分析、方案制定、技术处理、效果评价、合规审查、管理保障等。

本文件适用于指导互联网业务中的个人信息匿名化处理活动，也适用于对互联网业务中个人信息匿名化处理活动的监督、管理、评估。

二、工作简况，主要包括:任务来源、主要工作过程、各起草单位和起草人及其在起草标准过程中所承担的工作等情况、对标准草案进行会议讨论范围、征求意见的范围、审查的范围

本文件由深圳市腾讯计算机系统有限公司作为牵头单位起草，中国联合网络通信集团有限公司、天翼安全科技有限公司、宏盟媒体集团中国等参与编制。

本文件于2023年12月在中国互联网协会通过立项，主要工作过程如下：

(1) 立项后，牵头单位组织形成编制组，并编写标准草稿；

(2) 2024 年 4 月，形成标准草案初稿；

(3) 2024 年 5 月，组织召开标准研讨会，对标准草案进行讨论；

(4) 2024 年 6 月，编制组根据讨论意见，修改完善标准草稿，形成征求意见稿。

三、标准编制原则和确定标准主要内容(如技术指标、参数、公式、性能要求、试验方法、检验规则等)的依据(包括试验、统计数据)

本文件遵循规范性、先进性与可操作性相结合的原则。一是标准编制严格遵循GB/T1.1-2020《标准化工作导则 第1部分:标准的结构和编写》及相关法律法规的要求进行；二是标准充分吸纳行业实践，标准研制过程中持续关注行业动态，积极调研相关企业实践经验；三是在标准的研制过程中，充分考虑标准的实施难度，确保标准能够在各种场景下得到有效应用。

本文件参考《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》等法律，以及各部委的规章制度对各行业数据安全、个人信息保护的要求。《个人信息保护法》提出个人信息经匿名化处理后所得的信息不属于个人信息，匿名化是指个人信息经过处理无法识别特定自然人且不能复原的过程。《关于构建数据基础制度更好发挥数据要素作用的意见》（“数据二十条”）提出创新技术手段推动个人信息匿名化处理，保障使用个人信息数据时的信息安全和个人隐私，以及促进数据要素有序流通。本文件旨在明确互联网行业匿名化处理的目标与原则、管理措施、技术措施、操作流程、效果评价方法等，以促进达成行业共识，从而促进互联网行业的合规、健康、稳定发展。

四、主要试验(或验证)的分析、综述报告

互联网领域是数据收集、使用、加工、提供和委托处理密集的行业领域，在互联网广告、互联网医疗、互联网金融、互联网政务等场景中，都涉及到包括个人信息在内的海量数据的流转流通，这些应用模式面临一定的安全合规风险。而匿名化技术是互联网领域中重要的数据安全保障措施，已发展出许多成熟的技术解决方案。

在互联网业务中，参与机构多，生态链条长，很多机构无法直接获得个人同意或取得同意的成本巨大，这些数据处理行为在个人信息保护、商业秘密保护等方面，面临一定的安全风险。匿名化的合法路径将是互联网行业数据利用的重要主要方式。但是，目前互联网行业内，对匿名化、去标识化、假名化、数据脱敏等概念界定交叉、模糊，对于匿名化处理的合规要求、技术措施、管理措施、效果评价等方面的实践经验与理解差异较大，也缺少明确的数据匿名化实施定义与可行方案。

本标准旨在从数据提供方、数据接收方、监管方等匿名化各相关方的角度出发，在在编制过程中与各方进行了充分的沟通与调研，通过对各相关方的讨论，得到了具有可落地性的标准内容。

五、标准在起草过程中遇到的问题及解决办法；重大分歧意见的处理经过和依据；有无重要技术问题需要说明

在本文件的修订过程中，无重大分歧意见和技术问题。

六、与国外标准的关系：包括：采用国际标准和国外先进标准的程度，与国外标准主要技术内容的差异

在国际标准方面，ISO/IEC JTC1（国际标准化组织与国际电工委员会联合技术委员会）发布了三项与匿名化相关的国际标准。

《ISO/IEC 29100－2011 信息技术 安全技术 隐私框架》中规定了假名化和匿名化的术语和内涵。

《ISO/IEC 20889－2018 隐私增强的数据去标识化技术的术语与分类》中明确了重识别攻击的方法，去标识化技术的分类，以及隐私评估模型。

《ISO/IEC 27559－2022 隐私增强的数据去标识化框架》提供了一个框架，包括环境评估、数据评估、去标识化的管控措施等，用于识别和减轻重新识别风险以及与去识别数据生命周期相关的风险。

这些国际标准，可以作为本团标的参考和借鉴，以及内容输入。

七、修订标准时，说明与标准前一版本的重大技术变化，并列出所涉及的新、旧版本的有关章条(可引用标准前言的内容)；废止/代替现行有关标准的建议

本文件为制定标准，非修订标准。

八、说明标准与其他标准或文件的关系(可引用标准前言的内容)，特

别是与有关的现行法律、法规和强制性国家标准的关系

1、法律法规方面：

（1）《网络安全法》

第四十二条规定，网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

解读：匿名化数据（“经过处理无法识别特定个人且不能复原”）的收集， 无需征求被收集者同意。

（2）《个人信息保护法》

第七十三条明确了匿名化的定义，是指个人信息经过处理无法识别特定自然人且不能复原的过程。

第四条，明确了个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

（3）《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》（数据二十条）：

第六条中提到，通过创新技术手段，推动个人信息匿名化处理，保障使用个人信息数据时的信息安全和个人隐私。

国内外对匿名化方面都有一些研究，技术稳定，可以作为本团标的输入。

2、标准方面：

（1）国家标准方面

在国家标准方面，全国信息安全标准化技术委员会制定和发布了匿名化相关的国家标准。

GB/T 35273-2020《信息安全技术 个人信息安全规范》中明确，在超出个人信息存储期限、个人信息控制者停止运营其产品或服务、个人信息主体注销账户等场景中，个人信息控制者可以对所持有的个人信息进行删除或匿名化处理。

GB/T 37964-2019 《信息安全技术个人信息去标识化指南》主要描述了个人信息去标识化的目标和原则，提出了去标识化过程和管理措施。

GB/T 42460-2023 《信息安全技术 个人信息去标识化效果评估指南》主要提供了个人信息去标识化效果分级与评估的指南。

目前，全国信息安全标准化技术委员会正在制定《数据安全技术 匿名化处理指南》的国家标准，已立项，标准正在研制中。

（2）行业标准方面

在行业标准方面，中国通信标准化协会正在匿名化相关的行业标准，主要包括：

《个人信息去标识化处理技术使用指南》用于在数据发布、数据共享过程中，网络运营者根据发布订阅用户双方需求，选取合适的个人信息去标识化技术方法提供指南。

《数据流通 匿名化处理技术要求》旨在研究可用于实现匿名化处理的技术手段，根据处理的模式、阶段、效果等方面，系统梳理并形成匿名化处理技术体系框架；以及研究各类匿名化处理技术的基本功能要求，基于各类技术的特性，针对体系框架中的各类技术给出实现匿名化目标所需要达到的通用、必要的功能要求。

《数据流通 匿名化处理效果评价方法》旨在研究匿名化效果评价方法的整体框架，结合国内外匿名化的相关法律法规、标准规范情况，梳理评价方法的主要流程以及各阶段评价范围，形成一套通用框架。以及研究重点评价指标，一方面确定选取的评价指标以及指标计算方式，另一方面依据行业实践及相关规范，设置满足匿名化要求的指标范围，可根据场景按照等级划分。

（三）团体标准方面

在团体标准方面，中国广告协会与中国通信标准化协会联合发布了 T/CAAAD 004-2022 《互联网广告 数据匿名化实施指南》的团体标准，主要规定了互联网广告匿名化的概述、目标和原则，提出了匿名化过程和组织措施，并给出了技术指引建议。

当前，在互联网行业这个特定领域内，还缺乏个人信息匿名化技术应用指南的行业标准，来指导匿名化处理技术在互联网业务中的应用。

3、产业方面：

目前，各大互联网公司、安全公司、通信企业、科研院所等在匿名化方面，已经有丰富的实践经验，可以作为本标准内容的输入。

九、标准作为强制性标准或推荐性标准的建议

建议本文件作为推荐性团体标准。

十、贯彻国家标准的要求和措施建议(包括组织措施、技术措施、过渡办法等内容)；标准发布后，对国内外业界可能产生的影响

建议本文件作为推荐性团体标准发布实施，指导互联网业务中的个人信息匿名化处理活动，也适用于对互联网业务中个人信息匿名化处理活动的监督、管理、评估，以引导企业向着更加规范、健康的方向发展。

十一、标准是否涉及知识产权的情况说明；如标准中含有自主知识产权，说明产品研发程度、产业化基础及进程

本文件未涉及。

十二、其他应予说明的事项

本文件未涉及。