ICS 35.240
CCS L 67

团　　体　　标　　准

T/ISC 00XX—XXXX

匿名化技术应用指南

Application guidelines of anonymization technology in Internet advertising

（征求意见稿）

2024-7-2

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

中国互联网协会　　发布

目　　次

前　言

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。

本文件由中国互联网协会提出并归口。

本文件起草单位：。

本文件主要起草人：。

引　言

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。

在法律、法规、政策层面，《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、个人信息保护提出明确要求。《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。

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，因此有必要制定本团体标准，在互联网行业明确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，达成行业共识，从而促进互联网行业的合规、健康、稳定发展。

匿名化技术应用指南

1 范围

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。

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—2022 信息安全技术 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 37964—2019 信息安全技术 个人信息去标识化指南

GB/T 42460—2023 信息安全技术 个人信息去标识化效果评估指南

T/TAF 137—2022 基于差分隐私的用户个人信息保护技术要求

ISO/IEC 20889:2018 隐私增强的数据去标识化术语与技术分类

3 术语和定义

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与已识别或者可识别的自然人有关的各种信息。

[来源：GB/T 42460-2023，3.1]

注：不包括匿名化处理后的信息。

3.2

匿名化 anonymization

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。

注1：个人信息经匿名化处理后所得的信息不属于个人信息。

注2：匿名化是去标识化的极端情况，即在特定条件下特定主体有动机攻击重标识风险低于阈值。

3.3

去标识化 de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。

[来源：GB/T 35273-2020，3.15]

3.4

标识符 identifier

微数据中的一个或多个属性，可以实现对个人信息主体的唯一识别。

[来源：GB/T 37964—2019，3.6]

注：标识符分为直接标识符和准标识符。

3.5

直接标识符 direct identifier

微数据中的属性，在特定环境下可以单独识别个人信息主体。

[来源：GB/T 37964—2019，定义3.7]

3.6

准标识符 quasi-identifier

微数据中的属性，结合其它属性可唯一识别个人信息主体。

[来源：GB/T 37964—2019，定义3.8]

3.7

重标识 re-identification

把去标识化的数据集重新关联到原始个人信息主体或一组个人信息主体的过程。

[来源：GB/T 37964—2019，定义3.9]

4 缩略语

下列缩略语适用于本文件。

SQL：结构化查询语言(Structured Query Language)

URL：统一资源定位符 (Universal Resource Locator)

5 匿名化技术应用的目标与原则

5.1 匿名化技术应用的目标

匿名化处理的目的是在满足合规和安全风险可控的情况下，对数据资源进行合法有效利用，促进释放数据使用价值。

数据提供者开展匿名化处理活动宜符合以下的目标要求：

a) 安全合规目标

1) 依据相关法律法规规定，明确在未取得用户同意或其他法律依据情况下，如需继续开展个人信息处理活动，需要事先对个人信息进行匿名化处理；

2) 匿名化处理的数据及使用，限定在法律规定或个人告知同意的必要事项或目的所限定的范围内；

3) 对拟开展匿名化的主体、行为、对象及对应的同意授权及应用场景等条件，进行充分的风险评定与匿名化处理的必要性论证，满足合规性要求；
4) 符合《个人信息保护法》《数据安全法》《网络安全法》《民法典》等法律法规规定的合规性要求，即经过加工无法识别特定个人且不能复原。

b) 技术保障目标
1) 实施的匿名化处理技术能避免重识别的风险，且能控制重关联行为，所必需的辅助信息需要单独进行维护和管理；
2) 鼓励创新技术手段，通过匿名化处理技术保障促进数据安全和个人信息保护。

c) 数据使用目标
1) 匿名化处理并非追求完美、绝对的匿名化状态，现有的各项匿名化技术都无法彻底消除处理后的信息所残留的再识别风险。如果匿名化处理在满足合规合法的前提下，数据使用方或者可能获取匿名化信息的其他数据处理者无法访问或不掌握允许匿名化后的数据重新识别到数据主体的额外信息，或不具备合法重新识别数据主体的手段，或重新识别数据主体需要不合理的时间、努力或资源，则不视为是可复原的；
2) 所选取的匿名化技术，以及匿名化处理的程度，需要能满足业务合法、可控的数据应用需求，促进数据要素的安全合规流通。

5.2 匿名化技术应用的原则

数据提供者开展匿名化处理活动，宜遵循如下的原则：

a) 主体权益保护：匿名化过程需要满足国家对数据安全和个人信息保护等的相关要求， 保障个人信息主体享有的法定权利，不应与个人信息主体的基本权利和自由相冲突；
b) 发挥数据价值：匿名化处理在满足合规合法的前提下， 能够满足业务的合法、可控的数据应用需求，发挥数据价值；
c) 过程有序可控：匿名化的实施过程需要维护有限可控的数据利用环境秩序，并使得效果可评估、 证据可保存；
d) 可控可计量：匿名化的处理过程需要能通过技术方法实现对数据的使用控制，匿名化的效果需要能通过技术手段实现量化评估。

6 匿名化技术应用的实施框架

匿名化处理的实施框架，如图1所示。

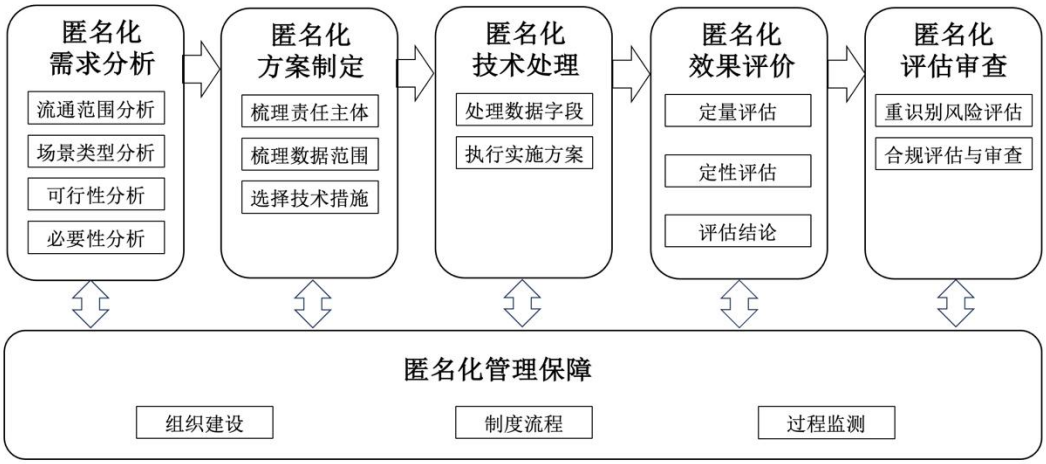

图1 匿名化技术应用的实施框架

其中，匿名化处理的实施框架主要包括匿名化需求分析、匿名化方案制定、匿名化技术处理、匿名化效果评价、匿名化评估审查等步骤。

匿名化需求分析主要包括流通范围分析、场景类型分析、可行性分析、必要性分析等步骤。

匿名化方案制定主要包括厘清责任主体、梳理数据范围、选择技术措施等步骤。

匿名化技术处理主要包括处理数据字段、执行实施方案等步骤。

匿名化效果评价主要包括K匿名效果评估模型、差分隐私评估模型、线性敏感度评估模型等方式。

匿名化评估审查主要包括重识别风险评估、合规评估与审查等。

在匿名化处理过程中，需对整个过程进行保障，包括组织建设保障、制度流程保障和过程监测保障等。

7 匿名化需求分析

7.1 流通范围分析

在数据流通场景中，数据的流通范围主要包括：

a) 组织内部的流通，比如公司内跨主体的数据流通；

b) 组织外部两方流通，比如公司与某合作方之间的数据流通；

c) 组织外部多方流通，比如公司与上游合作伙伴、下游合作伙伴三方的数据流通；

d) 对外公开，比如公司对外公开披露匿名化处理后的数据。

对于不同的数据流通范围，匿名化处理的要求和效果评价方法会有所不同。具体可参见第10章“匿名化处理效果的评估”的要求。

7.2 场景类型分析

在数据流通场景中，宜根据不同的场景类型，选用不同的匿名化处理技术。涉及到匿名化处理的场景类型主要包括：

a) 统计分析：数据处理者进行数据的挖掘分析时，将个人信息进行匿名化处理后再进行数据分析使用；
b) 开发测试：为了验证业务应用功能或业务算法模型，在系统测试、联调时，将个人信息匿名化处理后再进行开发测试使用；
c) 现网应用：在实时的现网应用场景中，可通过细粒度的访问控制，实现不同用户对同一个人信息访问时进行匿名化处理，实现脱敏展示；
d) 系统运维：运维人员在运维的工作中，直接连接生产数据库进行查询时，需要对查询的个人信息进行匿名化处理。

7.3 必要性分析

分析匿名化处理的必要性时，宜考虑如下方面：
a) 法律法规要求。业务侧宜结合国家、地区或行业的相关政策、法律、法规等规定，判断待收集、存储、使用、加工或向第三方提供的数据是否涉及匿名化的相关要求。
b) 监管设定要求。业务侧宜结合本行业、领域内相关监管部门要求，判断待收集、存储、使用、加工或向第三方提供的数据是否涉及匿名化的特别监管要求。
c) 履行约定承诺需要。业务侧宜结合自身是否与数据来源主体或者其他利益相关方存在数据匿名化处理的相关约定、声明或承诺，判断待收集、存储、使用、加工或向第三方提供的数据是否涉及匿名化的履约需求。
d) 业务经营策略需要。业务侧宜结合业务运行拓展过程中需要进行必要的数据统计分析、科学研究、训练测试等，综合考量数据特性和敏感程度，判断数据内外部应用时是否需要进行匿名化处理。

7.4 可行性分析

匿名化处理的具体实施可能会受限于数据类型、业务场景、技术成熟度、操作成本等因素，进行可行性分析宜考虑以下内容：
a) 待处理的数据受特殊监管要求，不宜进行匿名化处理；
b) 待处理的数据属于非结构化数据或动态更新变化的数据，匿名化处理难度较大、成本较高，且风险不可控；
c) 匿名化处理运行过程中，可能会对相关信息系统造成不合理负荷，或者产生难以接受的数据存储及计算成本；
d) 数据经过匿名化处理，在现有技术能力下，可能依旧无法满足标识符无法识别且不能复原的合规要求；
e) 数据经过匿名化处理，在具体业务场景下，可能严重丧失数据的可用性，无法满足预设的业务用途要求。

业务侧经可行性分析后，认定匿名化处理方案难以实现的，可以考虑在受控环境下进行相对匿名化处理，或者寻求其他替代的可行合规方案。

可行性分析的示例，参见附录A。

8 匿名化方案制定

8.1 厘清责任主体

匿名化处理实施工作的相关责任主体宜包括：

a) 执行方：匿名化处理的发起者和策划者，通常是数据的控制者或管理者，负责确定匿名化的目标、范围和策略，并执行和实施匿名化处理过程，对匿名化处理的行为和结果负责。执行方通常是数据流通中的数据提供方；
b) 使用方：实际使用匿名化数据的主体。使用方需要遵守相关承诺或协议，按照约定的用途和范围使用数据，并承担相应的责任，确保在使用数据的过程中不侵犯数据主体的隐私权益，并遵守相关的法律法规和行业规范；使用方通常是数据接收方；
c) 监督方：负责对匿名化处理过程进行监督和评估，确保数据处理过程合规、安全风险可控。可以对实施方的操作进行抽查或审计，对匿名化后的数据进行验证和测试，以确保数据的匿名性和可用性达到预期目标。监督方通常是组织的法务合规部门。

8.2 梳理数据范围

匿名化处理中，梳理数据范围的步骤宜包括：

a) 圈定后续业务所需数据范围。基于业务场景确定不同数据字段的匿名化需求，明确支撑具体业务所需处理的大致数据类型和范围，分析数据的性质、内容、格式、关系和体量等基本情况；
b) 移出无需处理的非敏感数据。为减轻匿名化操作的存储和计算成本，提升数据处理的效率，可以将不影响匿名化结果无需匿名化处理的数据集，先行移出至备用数据库表；
c) 移入可能关联识别的数据记录。抽取其他数据集中可能与待处理数据具有关联识别可能，或者其他可能影响匿名化效果的数据记录，一并纳入匿名化处理范围。

8.3 选择技术措施

在业务场景中，匿名化技术的选择，宜从可用性、时效性、安全性、合规性等方面进行综合评估：

a) 可用性：包括数据的特征保留、数据的真实性、数据的有效性等；
b) 时效性：包括匿名化过程的自动化执行、时间占用情况、计算资源的占用情况、存储资源的占用情况、成本等；
c) 安全性：包括抗重识别风险、可靠性、可控性等；
d) 合规性：包括对于法律法规的依从性等。

匿名化处理技术措施的选择要素，可参见附录B。

9 匿名化技术处理

9.1 处理数据字段

需要处理的数据字段宜包括：

a) 直接标识符：在特定环境下，可以单独识别个人信息主体的属性；
b) 准标识符：结合其他属性，可以唯一识别个人信息主体的属性；
c) 敏感属性：不能识别个人信息主体，但是涉及敏感个人信息的属性；

d） 其他属性：敏感个人信息之外的属性信息。

直接标识符和准标识符的识别，可参见GB/T 42460-2023 中附录A、附录B和附录C。

9.2 执行实施方案

执行匿名化技术实施方案的步骤宜包括：

a） 针对不同的属性，指定不同的去标识化处理措施，比如统计技术、密码技术、抑制技术、假名化技术、泛化技术、随机化技术、数据合成技术等；具体的去标识化技术措施，参见 GB/T 37964—2019 附录 A；

b） 针对不同的匿名化处理措施，设定不同的算法参数，比如掩码的位数，掩码的字符等。

匿名化处理技术的适用场景，可参见附录 C。

10 匿名化效果评价

10.1 评价目标

对于匿名化技术应用，应以构建相对且可行的匿名化整体解决方案机制，以数据接收方在可控环境中管控重新识别的风险为主要目标。即以数据接收方无法识别特定自然人且不能复原，作为匿名化处理效果评价的判断依据。

10.2 评价方法概述

匿名化效果评价方法包括基于K匿名的效果评价方法、基于差分隐私的效果评价方法、基于线性敏感度模型的评价方法等。

本文件主要介绍基于K匿名的效果评价方法。

基于差分隐私的效果评价方法、基于线性敏感度模型的评价方法，可参见ISO/IEC 20889中第10章的内容。

10.3 基于 K 匿名的效果评价方法

10.3.1 概述

对于离线库表结构的数据集，宜使用K匿名进行匿名化效果评估。即经过匿名化处理后数据集中某条记录如存在K条重复记录，则说明该记录的匿名化处理程度达标。

K匿名是计算数据集重标识风险水平的一种简单方法。根本上说，它是指在一个数据集中可以分组在一起的最小数量的相同记录。在评估数据集的总体重标识风险时，通常采用最小的组来表示最坏的情况。K匿名值为1意味着该记录是唯一的。

K匿名值越高意味着重标识风险越低，相反，K匿名值越低意味着风险越高。通常而言，应该尽可能设置更高的k-匿名阈值，以最大限度地减少任何重标识风险。

度量方法：计算数据集中每个等价类的记录数，确保每个等价类至少包含K个记录。K值越大，隐私保护程度越高。基于K-匿名值进行定量评估时，建议结合场景系数和环境系数来进行评估。场景系数表示数据匿名化后使用场景的安全系数，如组织内部使用、向特定第三方提供、公开发布等；环境系数表示数据流通时，数据流通环境的技术保障能力和管理保障能力。

通常而言，在外部数据共享场景中，应设置尽可能高的k-匿名值（例如：5或更大）；而内部共享和数据长期存储场景的k-匿名值可以更低（例如：3）。

10.3.2 计算方式

对于离线库表结构的数据集，建议基于K匿名进行效果评估。建议采用如下的计算方式来计算匿名化程度：

匿名化程度 = 数据集K匿名值最小值＊场景系数 ＊ 环境系数

要求：匿名化程度>=1，匿名化程度越高越好。

其中：

a) 数据集K匿名值最小值：表示数据集中，经过匿名化处理后，具备相同的准标识符字段组合的记录的条数的最小值；

b) 场景系数：表示数据集被使用的具体场景，如组织内部流通、组织外部流通、对外公开等；

c) 环境系数：表示数据流通时，数据流通环境的技术保障能力和管理保障能力。

基于K匿名的效果评价的示例，可参考附录D。

10.3.3 K 值计算

对于给定的离线库表结构的数据集，定量评估主要是对K匿名的最小K值的计算。计算方式如下：

a) 先识别出直接标识符和间接标识符；具体可参见参考GB/T 42460-2023附录A、附录B和附录C。由于评估方与匿名化处理方通常不同，因此需要重新识别；

b) 将数据集中的直接标识符假名化、加密或剔除；直接标识符假名化或加密之后，作为敏感属性来处理；

c) 针对匿名化处理后的间接标识符的组合，找出数据集中所有的等价类；即数据集中与某个数据项具备相同的间接标识符的数据项的集合；

d) 针对每个等价类，找出等价类大小，即K-匿名中的K值；

e) 找出数据集中的K值的最小值。

10.3.4 对场景系数的定量评估

定量评估还包括场景系数的设定。k-匿名值的场景系数需要根据不同的应用场景，进行设置。

通常而言，在外部数据共享场景中，应设置尽可能高的k-匿名值（例如：5或更大）；而内部共享和数据长期存储场景的k-匿名值可以更低（例如：3）。

建议的场景系数，如下表F.1所示：

表F.1 场景系数建议

场景	建议的场景系数
组织机构内部同一个主体下的数据流通	1/3
组织机构内部跨主体的数据流通	1/4
组织机构外部两方的数据流通	1/5
组织机构外部多方的数据流通	1/6

对外公开	1/20

注：在实际使用时，可根据具体的使用场景，适当调整。

10.3.5 对环境系数的定性评估

定性评估主要是对环境系统的评估。环境系数包括对技术保障能力和管理保障能力的综合评估。

a) 技术保障能力，具体包括：
   1) 安全和隐私控制能力。比如，是否采用权限管理、访问控制策略等；
   2) 数据流通技术保障能力。比如，是否采用安全隔离、数据沙箱、封闭域、专区、隐私计算等技术；
   3) 重识别攻击的动机和能力。比如，是否采用技术手段，抗重识别攻击等。
b) 管理保障能力：包括组织建设、制度流程、人员能力、协议合同约束、审计机制、事件与应急管理、风险控制能力等管理保障能力的综合评估。

对于环境保障能力，建议采用定性评估的方式。环境保障能力的中间值建议为1。当环境保障能力较低时，建议调高对于K-匿名值最小值的要求，以提升整体的匿名化程度。

10.3.6 形成评估结论

基于定性评估中的环境系数，和定量评估的K值和场景系数结果，使用10.3.2节中的计算方式，可以形成评估结论，评定给定的数据集是否满足匿名化条件。

对于匿名化程度评价的结果，可以有如下的运用方式：

a) 可以对整个数据集给出评价值，看是否满足预定的匿名化程度要求；
b) 针对数据流通场景，可以先设定出K匿名值，根据评价结果，剔除出低于预定K值的数据项；
c) 可以对低于预定K值的数据项继续作匿名化处理（如泛化、抑制等），直到数据集中的数据项全部满足匿名化程度要求。

11 匿名化评估审查

11.1 重识别风险评估

组织宜基于匿名化处理效果来识别重标识风险，并形成评估报告。其步骤宜包括：

a) 评估匿名化处理效果：在数据流通前，业务部门对匿名化处理的效果进行自评，判别重识别风险，并形成自评记录或报告，包括实施团队、过程行为、数据对象、数据结果等，评估过程和结果宜形成记录或报告；
b) 评估数据用途：业务部门管理层需要依据数据发布共享用途、重标识风险、数据有用性最低要求等因素，以及验证结果、匿名化各步骤实施过程中的监控审查纪律等因素，做出是否认可数据匿名化处理结果的决定；
c) 业务部门宜根据情况变化或定期进行重标识风险评估，并与预期可接受风险阈值进行比较，以保障个人信息安全性。情况发生变化是指重标识风险的相关要素发生变化，相关要素包括但不限于：数据使用者、目标信息系统、目标信息安全环境、新增数据处理行为、新增匿名化数据；

d) 通过匿名化实施评估后，如涉及后续传输、提供、存储、加工等行为，控制数据内容与匿名化实施评估保持一致。业务部门不得在通过评估后另行再增加关联其他标识符或者技术回滚等导致与评估情况不符的不合规行为，如出现该情况应重新评估。

11.2 合规评估与审查

组织宜依据法律法规、组织制度文件等相关依据，对数据处理活动开展合规评估和审查。

12 匿名化管理保障

12.1 组织建设

组织机构在匿名化处理的组织建设方面，宜遵守如下的实施指引：

a) 设立专门负责个人信息的团队或岗位；
b) 明确相关人员在匿名化处理流程中的职责和权力；
c) 定期对员工开展个人信息保护和匿名化处理相关的培训；
d) 提高员工对个人信息保护和匿名化处理的意识。

12.2 制度流程

组织机构在匿名化处理的制度流程方面，宜遵守如下的实施指引：

a) 建立匿名化处理过程中标识符识别和处理的规则库，供组织内部参考实施；
b) 建立匿名化处理过程中合规评估的流程与要点；
c) 建立匿名化处理效果评价的方法与流程；
d) 建立匿名化处理的控制体系，通过限定和控制数据使用中的数据内容、处理形式和约束条件，形成受控环境和安全边界，通过对关联的控制而约束数据的合规使用，并有效留存相应的合规性证据。

12.3 过程监测

组织机构在匿名化处理的过程记录方面，宜遵守如下的实施指引：

a) 对匿名化处理的步骤进行监测，并记录日志；
b) 日志内容包括时间、处理人、处理措施、处理结果等内容；
c) 在匿名化处理的步骤完成时，对相关记录进行不定期抽查，检查输出记录是否齐全和内容完备；
d) 及时发现已经出现或可能出现的错误或偏差，并采取适当控制措施，监督各步骤执行过程得到完整和有效地执行。

附 录 A
（资料性）
匿名化处理的可行性分析示例

以某业务为例，对于实现匿名化处理后，业务与技术上的主要难点与利弊分析，如表 A.1 所示。

表A.1 匿名化处理的可行性分析

序号	情形	分析
1	匿名化处理不利于以“非结构性方式”储存的数据。	文字、图片、音讯、视频等档案，必须依靠内部自定义“需要匿名化处理的个人信息范围” 才能达到匿名化处理。如：服务器日志（纯文字记录）、音频、视频、图片等。必须依靠自定义的数据范围才能进行特别处理，而针对非结构性数据 定义较全面的 “个人信息” 范围实属困难。就算勉强定义过后、在该类数据中勾出已定义数据也有一定成本、影响日常操作。
2	完全匿名化处理后、数据失去“关联值”的弊端。	把个人信息完全匿名化后，所有的数据表（包括不含个人信息的数据表）会变成数据孤岛，数据失去了用作统计分析的价值（无法导出汇总数据的工作），也使得整体业务宏观统计分析失去可信可靠的依据。
3	运行匿名化处理过程后、对系统性能做成的成本及负荷。	运行匿名化处理的过程后，会生成一份额外的匿名化处理后的数据表，在当前的存量数据基础上，执行匿名化处理过程，会额外带来 2-3 倍的数据存储及计算成本。
4	依据合规要求，需要确保“个人信息还原可能性”降至 0%的几率。	业务拥有庞大的中央数据库、非常复杂的数据命脉。数据储存形式、管理团队、数据流也各自不同。就算中央数据库、数据平台等提供的数据访问平台已确保国内员工不能访问平台中的海外用户个人信息，也难保个别员工 “绝对无法”从其他系统、平台中复原 透过前者所取得的数据。

基于以上难点与利弊分析，不论在可行性、难易度、移除风险的可能性、利弊权衡方面，勉强追求匿名化数据处理是不合理的。

因此，在匿名化处理方式比较难实现的情况下，业务可考虑以假名化处理方式处理，减低数据敏感度，同时减低当中涉及的风险。

附 录 B
（资料性）
匿名化处理技术措施的选择要素

在业务场景中，匿名化技术的选择，宜从可用性、时效性、安全性、合规性等方面进行综合评估。

B.1 可用性

可用性的评估，主要包括如下几个方面：

a) 特征保留：匿名化后的数据尽可能地体现和保持原始数据的原有特征，且尽可能多的保留原始数据中的有意义的信息，以减小对使用该数据的系统的影响；
b) 真实性：匿名化后的数据，与原始数据的符合度；
c) 有效性：保证数据的开发、测试、使用等过程中不会受到匿名化的影响。

示例：

a) 可用性相对较高的技术包括：同态秘密共享、确定性加密、保序加密、同态加密等。
b) 可用性相对较低的技术包括：数据聚合、抑制技术、统计技术、随机技术、泛化技术、数据截断等。

B.2 时效性

时效性主要包括如下几个方面：

a) 自动化执行：保证匿名化的过程可通过程序自动化实现，可重复执行；
b) 时间占用：匿名化处理过程所占用的时间；
c) 计算资源的占用：匿名化处理过程所占用的计算资源；
d) 存储资源的占用：匿名化处理过程所占用的存储资源；
e) 成本：匿名化处理过程所需要的成本。

示例：

计算性能相对较低的技术包括：同态加密、同态秘密共享等。

B.3 安全性

安全性主要包括如下几个方面：

a) 数据使用环境：数据使用环境为公开环境、受控环境等；
b) 抗重识别风险：保障匿名化后的数据重识别的风险在可接受的范围内；
c) 可靠：保障匿名化算法不被同质属性、概率、知识推断等手段攻击，确保匿名化技术安全可靠；
d) 可控：匿名化的数据仍需采取合适的方式控制知悉范围，通过恰当的安全管理手段，防止数据外泄。避免因扩散范围过广导致的多源串联交叉比对分析导致风险增加。

示例：

相对而言，抗重识别的技术包括：数据聚合、同态加密、同态密码共享等。

易受重识别攻击的技术包括：确定性加密、保序加密、抑制技术等。

假名化技术容易受到对假名分配表的攻击。

采用了隐私计算环境、可信执行环境、数据沙箱、封闭域等受控的数据流通环境时，安全性相对较高。

B.4 合规性

合规性主要体现在对《个人信息保护法》等法律法规的依从性等方面。

附 录 C
（资料性）
匿名化处理技术的适用场景

C.1 数据统计分析场景

C.1.1 场景描述

数据统计分析场景指数据分析工程师进行数据挖掘分析时，将敏感数据脱敏后再进行数据分析使用。将数据导出到数据文件或者大数据平台，来进行分析。

C.1.2 场景特点

在数据分析场景下，需要重视数据之间的关联性、分析结果，脱敏后的数据应保留原有的数据关系与格式，确保数据脱敏后不会影响分析结果。

C.1.3 技术方案

宜采用泛化、均化等技术。

C.2 系统开发测试场景

C.2.1 场景描述

数据从生产环境导出到测试环境时，一般是为了验证业务应用功能或业务算法模型。是指系统测试、联调时，将敏感数据脱敏后再进行开发测试使用。

C.2.2 场景特点

为了防止敏感数据泄漏，在满足测试环境业务验证的前提下，只提供保持最小化数据特性的匿名化数据。在开发测试场景下，需要重视数据的可用性，因此匿名化处理可以采用相同含义的数据替换原有的敏感数据。

C.2.3 技术方案

宜主要采用替换、变形、扰乱、泛化、均化、时间随机、数值随机等技术。

C.3 系统日常使用场景

C.3.1 场景描述

系统的日常使用场景主要包括：

a）数据从生产环境导出到租户环境：一般是用于统计分析和数据挖掘；

b）用户访问生产环境中的数据：为实现敏感数据保护，可通过细粒度的访问控制，实现不同用户对同一敏感数据访问时进行不同的展示，对低权限用户进行匿名化展示；

c）运维人员访问生产环境中的数据：运维人员访问生产环境中的数据是为了验证平台或业务的正常运行，不需要获取真实的敏感数据。为防止敏感数据泄漏，只需提供为运维人员匿名化处理后的数据。

C.3.2 场景特点

系统的日常使用场景的特点主要包括：

a） 对于用户访问生产环境中的数据的场景，业务系统访问时效性要求较高；

b） 对于数据从生产环境导出到租户环境，匿名化操作发生在数据批量迁移时，时效性要求低；

c） 运维人员访问生产环境中的数据的场景，访问业务系统时效性要求较高。

C.3.3 技术方案

对于数据访问的场景，宜采用不可逆脱敏算法对数据进行匿名化展示，防止运维人员接触敏感信息。

附 录 D
（资料性）
基于 K 匿名的匿名化效果评价的示例

D.1 数据集

参考GB/T 42460—2023《信息安全技术 个人信息去标识化效果评估指南》中附录D.2中的数据集。

某组织内部共享的一批用户的广告投放记录数据集，已经对姓名、年龄等属性进行去标识化处理，如下表F.2所示。

表D.1 某组织内部的去标识化数据集

姓名	年龄	业务编码
男	35 ~ 40	700225
女	35 ~ 40	355421
男	51 ~ 55	355611
男	35 ~ 40	455641
女	45 ~ 50	355421
男	41 ~ 45	255456
男	51 ~ 55	355421
男	35 ~ 40	756987
女	35 ~ 40	700227
男	51 ~ 55	379044
女	35 ~ 40	455641
男	41 ~ 45	355459
女	45 ~ 50	700225
男	41 ~ 45	487792
女	45 ~ 50	437562
男	51 ~ 55	736920

D.2 计算 K 匿名值

针对上述的数据集，计算等价类的大小，即K值。如表D.2所示：

表D.3 数据集中的等价类大小

等价类	准标识符		等价类大小（K值）
	性别	年龄	
1	男	35 ~ 40	3
2	男	41 ~ 45	3
3	男	51 ~ 55	4
4	女	35 ~ 40	3
5	女	45 ~ 50	3

可见，在上表中，该数据集的K匿名最小值为3。

D.3 场景系数评估

由于该数据共享的场景是该组织在其组织内部的数据共享，其场景系数为1/3。

D.4 环境系数评估

经评估，该组织内部的技术保障能力和管理保障能力较高，其环境系数为1。

D.5 评估结果

基于10.3节的评价方法，匿名化程度 = 3 * 1/3 * 1 = 1，满足匿名化要求。

参 考 文 献

[1] 《中华人民共和国网络安全法》 2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通过

[2] 《电信和互联网个人信息主体个人信息保护规定》 2013 年 7 月 16 日中华人民共和国工业和信息化部令第 24 号公布，自 2013 年 9 月 1 日起施行

[3] GB/T 35273—2020 《信息安全技术 个人信息安全规范》

[4] 中国信息通信研究院产业与规划研究所、北京国际大数据交易所 数据清洗、去标识化、匿名化业务规程（试行）

[5] T/CAAAD 004—2022 T/CCSA 424—2022 互联网广告 数据匿名化实施指南