ICS 35.020
CCS L 70

MR

中华人民共和国市场监管行业标准

MR/T XXXXX—XXXX

数据脱敏控制技术要求

Technical Requirements for Data Desensitization Control

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局　　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》给出的规则起草。

请注意本文件的其他内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件由提出并归口。

本文件起草单位：

本文件主要起草人：

数据脱敏控制技术要求

1 范围

本文件描述了大数据泛在流通与共享下，隐私信息全生命周期脱敏控制技术要求，涵盖脱敏控制策略生成、控制策略可控传递、控制策略迭代调整、策略执行可信验证等内容，规范了脱敏控制合规性验证、脱敏控制监管接口的技术要求等。

本文件适用于规范市场监管领域各类组织的隐私信息脱敏处理活动，也适用于市场监管领域主管部门、第三方评估机构等组织对隐私信息脱敏处理活动进行监督、管理和评估。

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 45963.1-2025 数字政府架构框架 第1部分:参考模型

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 37988-2019 信息安全技术 数据安全能力成熟度模型

3 术语和定义

下列术语和定义适用于本文件。

3.1

市场监管数据 market regulation data

为对市场活动主体及其行为进行限制、约束等，市场监管主体在直接干预活动过程中形成的数据。

[来源：GB/T 45963.1—2025, A.3.5 b)]

3.2

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，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]

3.3

隐私信息 private information

能通过信息系统进行处理的敏感个人信息，是个人信息记录中的标识符、准标识符和敏感属性的集合。

注：隐私信息包括个人生物特征信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14岁以下（含）儿童的个人信息等。

3.4

隐私信息所有者 private information owner

隐私信息所标识或者关联的自然人、组织、设备或程序等实体。

3.5

隐私信息处理者 private information processor

对隐私信息进行收集、存储、使用、加工、传输、提供、公开、删除、脱敏、存证与取证等操作的实体。

3.6

隐私信息提供者 private information provider

向其他自然人、组织、设备或程序提供隐私信息的实体。

3.7

隐私信息接收者 private information recipient

接收其他自然人、组织、设备或程序提供的隐私信息的实体。

3.8

个人信息流转 transfer and sharing of personal information

个人信息在不同隐私信息处理者之间共享传播的过程。

3.9

原始信息 raw information

当前主体采集或者接收到的信息，其包含敏感个人信息，需要进行脱敏处理，且可以通过携带脱敏控制策略来实现个人信息的流转脱敏控制。

3.10

信息模态 information mode

个人信息载体数据的具体表示形式，比如数字、文本、图像、视频、语音等。

3.11

数据脱敏 data desensitization

通过一系列数据处理方法对原始信息进行处理以减少或消除敏感个人信息的一种数据保护方法。

[来源：GB/T37988-2019,3.12,有修改]

3.12

脱敏算法 desensitization algorithm

通过对隐私信息的技术处理,使其在不借助额外信息的情况下,无法识别或者关联隐私信息所有者。

注：脱敏算法包括k-匿名、差分隐私等算法。

[来源：GB/T 35273—2020,3.15]

3.13

脱敏算法集合 desensitization algorithm set

一组用于处理不同类型或者数据结构的敏感数据的技术和方法，目的是减少或消除数据中的敏感信息，以降低用户隐私泄露的风险。脱敏算法集合包括脱敏算法类别、脱敏算法、脱敏算法参数集合。

3.14

脱敏控制 desensitization control

个人信息流转过程中，针对信息在不同隐私信息处理者之间流转的各环节（例如：收集、公开、提供、传输等过程），结合不同信息实体，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。

3.15

脱敏意图 desensitization intention

反映了隐私信息所有者在分享个人信息时对信息的预期保护力度,其内容涉及信息采集、信息获取、信息处理、保护内容、使用权限、脱敏测评等信息传播全生命周期中的多个方面。

3.16

脱敏要求 desensitization requirements

待脱敏的隐私信息的脱敏等级、脱敏时机、脱敏算法及其参数选择等约束信息。

3.17

脱敏效果期望 expectation on desensitization performance

隐私信息执行脱敏操作之后所达到的预期效果。

3.18

脱敏控制策略 desensitization control policy

个人信息流转过程中脱敏要求、脱敏约束等脱敏控制相关要素的载体，多数嵌入信息中伴随信息一起传播。信息分享传播过程中，脱敏控制策略约束隐私信息处理者进行按需脱敏控制操作，是完成按需脱敏的主要依据。

注：脱敏控制策略主要包括隐私信息标识、脱敏算法选择、脱敏约束、脱敏效果评估结果等内容。

3.19

按需脱敏 on-demand desensitization

隐私信息处理者按照隐私信息的延伸控制要求进行脱敏的过程。

3.20

流转脱敏 desensitization within information transfer

个人信息流转过程中，一系列隐私信息处理者对隐私信息依次进行按需脱敏的过程。

3.21

首次脱敏 initial desensitization

在流转脱敏过程中，首个隐私信息处理者对个人信息进行隐私脱敏的过程。

3.22

迭代脱敏 iterative desensitization

在流转脱敏过程中,首次脱敏之后,后续隐私信息处理者对接收到的个人信息进行隐私脱敏的过程。

3.23

本地收敛脱敏 local objective-oriented desensitization

在流转脱敏过程中，隐私信息处理者在其管理域内，依照脱敏控制策略的约束，重复地进行脱敏算法选择、脱敏操作以及脱敏效果评测等步骤，直至满足脱敏效果期望的过程。

4 缩略语

下列缩略语适用于本文件。

UDP：用户数据报协议(User Datagram Protocol)

XML：可扩展标记语言(eXtensible Markup Language)

TCP：传输控制协议(Transmission Control Protocol)

API：应用程序接口(Application Programming Interface)

JSON：JS键值对数据(JavaScript Object Notation)

REST：表述性状态转移(Representational State Transfer)

5 概述

5.1 脱敏控制的目的

脱敏控制的目的是：首次脱敏时，通过脱敏控制反映隐私信息所有者的脱敏意图；后续脱敏时，通过脱敏控制反映隐私信息所有者以及前序隐私信息提供者的脱敏意图，以在市场监管过程中，避免因数据流通与共享导致的隐私泄露，保障敏感个人信息和商业秘密的安全性和合规性。含有脱敏控制的市场监管数据流转过程如图1所示。首次分享者采集采集市场监管相关的个人或企业信息后，执行首次脱敏操作，即按照隐私信息所有者设定的脱敏意图，进行本地收敛脱敏，直至达到预期脱敏效果。首次分享者在共享信息时，更新脱敏控制策略并随信息共享给迭代脱敏者。迭代脱敏者接收信息之后，执行迭代脱敏，即结合具体应用场景，选定合适脱敏算法集合，进行本地收敛脱敏，直至达到预期脱敏效果。

流转脱敏过程中，脱敏控制流程需要存证，以支持脱敏控制违规事件的检测与问题溯源。

5.2 脱敏控制的基本原则

5.2.1 有效性

有效性要求脱敏控制的过程是健壮的，即脱敏控制系统应具备在安全威胁之下，依然可以确保各隐私信息处理者按照脱敏意图进行脱敏操作。

5.2.2 准确性

准确性要求各隐私信息处理者能够综合考虑原始信息、应用场景、隐私信息接收者防护能力等多种因素，选择合适的脱敏算法集合，对隐私信息中不同信息模态的数据进行精准脱敏，确保数据在脱敏后的实用性和安全性。

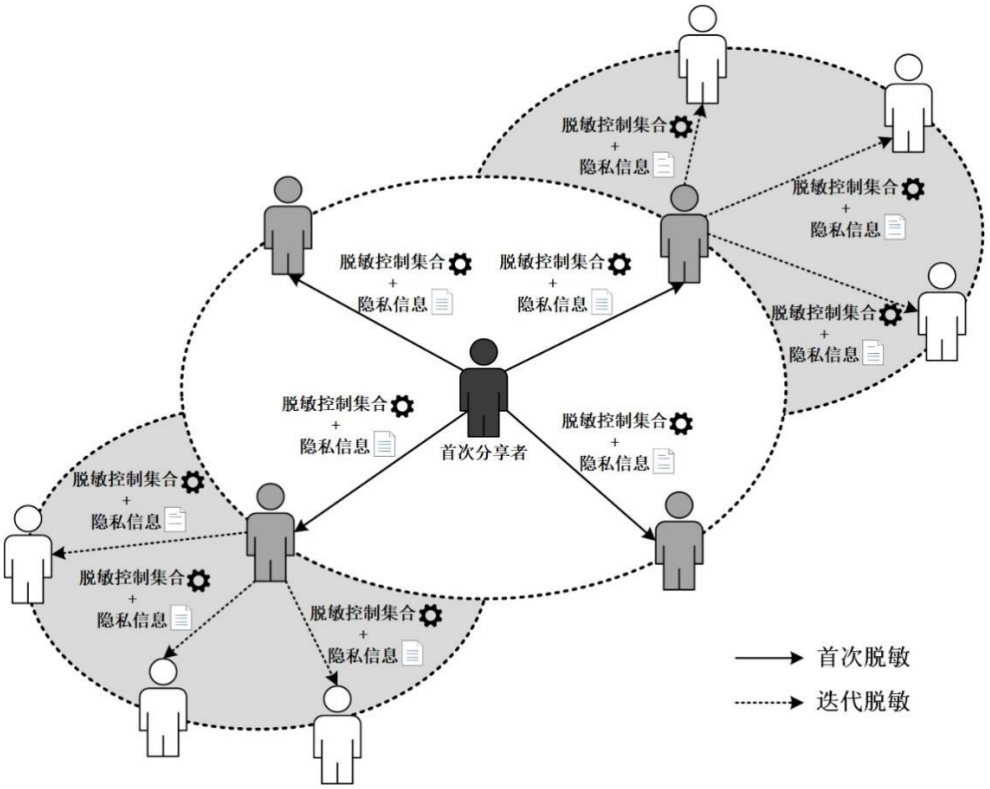

图1　脱敏控制约束下的数据流通与共享过程

5.2.3　一致性

一致性要求对相同的隐私信息，不同算法的隐私保护效果都使隐私信息分量的敏感度趋近于零，即不同算法在不同系统中隐私保护的趋势保持一致。

5.2.4　迭代性

迭代性要求在数据流通与共享过程中，不同隐私信息处理者按照脱敏控制的约束，对接收到的数据进行场景自适应的按需脱敏。

5.2.5　可审计性

可审计性要求在脱敏控制系统在各个阶段加入安全审计机制，严格、详细记录脱敏过程中的相关信息，形成完整数据存证记录，以便后续问题排查与数据追踪分析。

5.3　脱敏控制的流程

5.3.1　脱敏控制流程概述

如图2所示，脱敏控制框架关注数据跨域流通与共享场景下，相关隐私信息处理者对接收到的原始信息展开脱敏操作的管理和控制工作，包括脱敏控制策略生成、脱敏算法选择与执行、控制策略可控传递、控制策略迭代调整、策略执行可信验证、脱敏控制存证等步骤。

版式文档流通与共享场景下的脱敏控制流程示例参见附录A。

5.3.2　脱敏控制策略生成

脱敏控制策略生成是指，在数据流通与共享过程中，通过系统化、标准化的方法，结合隐私信息所有者或前序隐私信息提供者的脱敏意图、当前隐私信息处理者的脱敏意图及设备环境等条件，动态地针对特定隐私信息，生成脱敏控制策略的过程。脱敏控制策略旨在确保市场监管数据在跨组织、跨系统或跨应用流通与共享时，相关隐私信息处理者的脱敏处理环节能得到恰当且有效的控制，最大程度保护个人隐私权益和商业机密，确保数据在监管过程中的合规性与安全性。

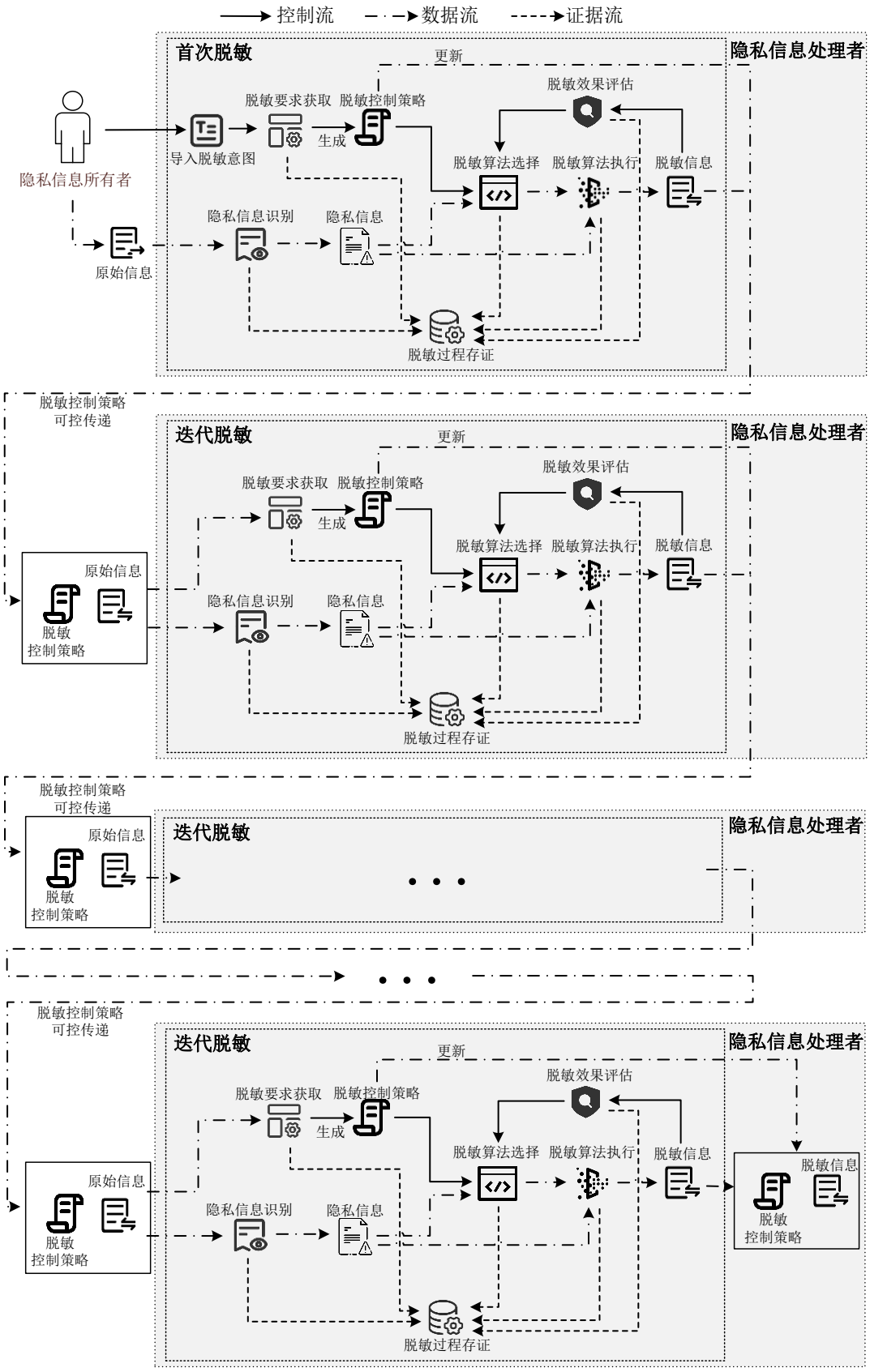

图2　隐私信息处理者的脱敏控制流程

5.3.3 脱敏算法选择执行

脱敏算法选择执行是指，根据获取的脱敏控制策略，结合原始信息中的隐私信息、信息模态、应用场景等因素，筛选确定合适的脱敏算法集合，并据此对原始市场监管数据中的敏感信息进行按需脱敏。脱敏算法执行完毕后，对脱敏数据进行脱敏效果评估，判断是否满足脱敏要求。若保护效果评估未达到预期脱敏效果，则对脱敏算法集合中的脱敏算法及其参数进行更新调整。隐私信息处理者可根据脱敏效果评估结果，执行多次脱敏，直至达到预期效果。按需脱敏具体流程参见附录B。

5.3.4 控制策略可控传递

控制策略可控传递是指，在市场监管数据流通与共享过程中，脱敏控制策略能跟随共享的监管数据在不同隐私信息处理者之间安全、可靠且有序的传输。控制策略可控传递过程需要确保脱敏控制策略在传递过程中不被未经授权的篡改或泄露，保障其完整性和安全性，同时确保策略能够准确无误地到达指定的市场监管数据接收者，确保数据在跨组织、跨系统的市场监管过程中遵循统一的隐私保护要求与合规性标准。

5.3.5 控制策略迭代调整

控制策略迭代调整是指，脱敏控制策略在市场监管数据的不同处理者之间流转时，能够根据应用场景、监管需求等因素的变化，进行正确的更新调整，支撑按需脱敏。该过程主要关注于脱敏控制策略在不同市场监管数据处理者之间的传递过程中，根据实际应用场景的变化、脱敏效果的评估结果以及各个数据处理者的脱敏意图，对脱敏控制策略的内容进行适时、合理的调整。

5.3.6 策略执行可信验证

策略执行可信验证是指，市场监管数据提供者验证脱敏控制策略在传递至数据接收者后，能够被完整正确地执行。这一过程通过一系列验证措施，保障市场监管数据处理者能够确信数据接收者已严格遵循既定的控制策略要求，从而维护数据流通与共享过程中的隐私保护的完备性和合规性，确保市场监管数据在跨组织、跨系统的流转过程中符合监管要求，避免数据滥用或隐私泄露。

5.3.7 脱敏控制过程存证

脱敏控制过程存证是指，对市场监管数据脱敏控制流程各环节的执行过程、操作记录、生成结果等信息进行日志存证，为后续市场监管数据的完备删除和主被动监管等隐私信息全生命周期、全流程的保护提供良好的存证基础。脱敏过程存证包括脱敏控制执行过程存证和脱敏控制策略传递存证。

6 脱敏控制通用技术要求

6.1 脱敏控制策略生成

脱敏控制策略生成使用自然语言处理、形式化分析等技术，按照前序市场监管数据提供者和当前隐私信息处理者的脱敏意图，产生计算机程序可处理的脱敏控制策略。此过程宜遵守以下要求：

a) 针对市场监管数据被首次流转的应用场景，支持数据所有者导入脱敏意图；
b) 针对市场监管数据非首次流转的应用场景，支持通过前序的市场监管数据所有者、数据信息提供者或数据处理者的脱敏控制策略，获得脱敏意图；
c) 数据所有者向数据处理者提供脱敏意图的时机，包括但不限于：数据收集之前获取、数据收集之后获取、数据流通与共享之前获取等方式；
d) 根据脱敏意图，生成脱敏要求，其内容应包括但不限于：脱敏意图标识、获取与调整脱敏意图方式、脱敏意图来源、脱敏级别等；
e) 通过自然语言处理等技术，对获取的脱敏意图进行解析，并结合市场监管数据模态、数据接收者的隐私保护能力、应用场景等因素，生成脱敏控制策略；
f) 脱敏控制策略的内容包括但不限于：原始市场监管数据中待脱敏的敏感信息、脱敏算法集合及其参数、获取原始信息的过程中的相关信息，以及原始信息在传输到当前主体之前经过的脱敏流程和相关信息；

g） 采用数字签名技术对脱敏控制策略进行签名，确保其内容的真实性和不可篡改性。签名过程应使用安全可靠的密钥管理机制，保障签名的有效性；
h） 脱敏控制策略采用底层系统无关的标准化描述，支持脱敏控制策略的跨系统传递。

6.2 控制策略可控传递

控制策略可控传递采用密码学技术保障脱敏控制策略在市场监管数据提供者和数据接收者之间传递过程中的完整性、机密性、不可剥离性、不可抵赖性和保护一致性。此过程宜遵守以下要求：

a） 完整性，利用消息验证码等技术，保证脱敏控制策略在传递过程中不可被非授权方式更改或破坏；
b） 机密性，可采用密码技术对脱敏控制策略进行加密保护，保证脱敏控制策略不可被未授权的第三方解析，避免脱敏控制策略被非法获取而导致的隐私泄露；
c） 不可剥离性，采用可信执行环境、密码学等技术将脱敏控制策略嵌入被交换的市场监管数据中，并保证脱敏控制策略和隐私信息的关联关系不能被破坏；
d） 不可抵赖性，采用数字签名技术对市场监管数据的脱敏控制策略进行处理，确保控制策略来源的真实性，避免数据处理者否认其前序市场监管数据提供者所生成的脱敏控制策略；
e） 保护一致性，市场监管数据跨系统交换或采用数据使用安全技术进行联合利用时，需对数据提供者和接收者的脱敏算法保护能力和脱敏效果进行关联的保护量化映射，量化映射关系存于脱敏控制策略中。

6.3 控制策略迭代调整

为了支持脱敏控制策略在市场监管数据提供者和数据接收者之间流转时的动态更新，控制策略迭代动态调整宜遵守以下要求：

a） 从接收到的市场监管数据中，解析并获取前序数据处理者嵌入的脱敏控制策略；
b） 当前市场监管数据接收者根据脱敏控制策略中的脱敏强度等元素，确定脱敏算法集合及其参数，并更新脱敏控制策略；
c） 当前市场监管数据接收者将数据脱敏后的脱敏效果评估结果，记录于脱敏控制策略中；
d） 根据后续市场监管数据接收者的隐私保护能力、应用场景、数据模态等信息，调整脱敏要求和脱敏效果期望，并更新脱敏控制策略；
e） 更新后的脱敏控制策略，连同当前基于脱敏控制策略处理过的脱敏信息，安全传递给后续市场监管数据接收者；
f） 支持在脱敏控制策略中嵌入部分或全部前序数据处理者信息，需至少包含前一级数据处理者的信息；
g） 若脱敏效果评估结论未达到预期脱敏效果阈值，则需调整脱敏算法集合及其参数，并更新脱敏控制策略；
h） 可采用可信环境等技术措施，保证脱敏控制策略更新调整过程的安全性与可信性。

6.4 策略执行可信验证

为验证脱敏控制策略是否被市场监管数据接收者完整、正确地执行，策略执行可信验证应遵守以下要求：

a） 支持当前市场监管数据处理者验证数据传播链上任一后续数据接收者和数据处理者是否按预期执行了脱敏控制策略；
b） 市场监管数据接收者对脱敏数据的脱敏效果评估结果，可采用可信日志存证、密码学等技术进行处理，支持验证数据接收者是否按预期完整、正确地执行了脱敏控制策略；
c） 可将脱敏控制策略的生成、解析及执行功能部署在可信执行环境中，支持脱敏控制策略执行的可信验证。

6.5 脱敏控制过程存证

脱敏控制过程存证使用审计日志、数字签名等技术，确保市场监管数据在脱敏处理过程中可追溯、可验证。此过程宜遵守以下要求：

a) 在脱敏算法选择时，可对考虑的因素，例如：应用场景、信息模态、后序隐私信息处理者防护能力等，进行存证，并对选定的脱敏算法集合进行存证；
b) 对更新后的脱敏算法控制集合进行存证；
c) 在进行脱敏操作时，可就脱敏操作的执行时间、执行者、所采用的脱敏算法集合及相关参数等信息进行存证；
d) 在接收原始市场监管数据时，对接收到的原始信息中的脱敏控制策略信息进行存证；
e) 在将脱敏控制策略传递给后续市场监管数据控制者时，对脱敏控制策略内容及相关信息进行存证；
f) 对接收的脱敏控制策略来源进行可信认证；
g) 在正确接收脱敏控制策略后，给予确认消息，并对确认信息进行存证。

7 脱敏控制合规性验证的技术要求

7.1 脱敏控制策略生成合规性验证

脱敏控制策略生成合规性验证，宜遵守以下要求：
a) 支持对获取的脱敏意图和生成的脱敏要求进行匹配性验证，以确保市场监管数据的脱敏意图理解过程的合规性；
b) 采用形式化分析技术，对脱敏控制策略进行验证，确保策略完全符合市场监管数据的脱敏要求，且策略内部各项内容之间不存在逻辑冲突或执行障碍。

7.2 控制策略可控传递合规性验证

控制策略可控传递合规性验证，宜遵守以下要求：
a) 市场监管数据处理者在将脱敏控制策略传递给后序数据处理者时，应对脱敏控制策略内容进行存证；
b) 市场监管数据处理者在将脱敏控制策略传递给后序数据接收者时，应对数据接收者的身份进行验证。

7.3 控制策略迭代调整合规性验证

控制策略迭代调整合规性验证，宜遵守以下要求：
a) 支持对市场监管数据的脱敏意图和对应的脱敏控制策略进行匹配性验证；
b) 支持获取原始市场监管数据中含有的脱敏控制策略，以及脱敏操作过程实际采用的脱敏控制策略，并对比两者的一致性。

7.4 策略执行可信验证合规性验证

策略执行可信验证合规性验证，宜遵守以下要求：
a) 对生成的日志等记录进行审查，确保市场监管数据脱敏控制策略执行可信验证的完备性，并能追溯到具体的数据处理者；
b) 所有验证过程及结果按照要求格式进行保存和归档，以便后续审计和责任追溯。

7.5 脱敏控制过程存证合规性验证

脱敏控制存证合规性验证，宜遵守以下要求：
a) 按照章节 6.5 的技术要求，对市场监管数据脱敏控制全程进行存证；
b) 提供存证合规验证接口，对存证过程的合规性进行验证。

8 脱敏控制监管接口的技术要求

8.1 存证接口的技术要求

8.1.1 自存证接口技术要求

市场监管数据的脱敏控制自存证接口，支持将脱敏控制过程产生的日志信息，写入本地存储系统。在设计和实现上，对自存证接口的要求如下：

a) 上报处理数据请求的接口平台支持跨平台使用，支持 Windows、Linux 等常用操作系统；
b) 上报处理数据请求的传输方式应支持标准的传输协议，包括不限于 REST API、消息系统、TCP/UDP 等标准协议；
c) 上报处理数据请求的内容应采用结构化或半结构化格式，包括不限于 JSON、XML 等格式；
d) 上报存证信息的内容应附有自身的签名，以确定存证信息来源；
e) 上报处理数据请求的内容应至少包括存证摘要、信息模态、目的、处理时间、处理方式、处理结果、操作人员/组织等相关操作日志。

8.1.2 监管机构存证接口

市场监管数据的脱敏控制自存证系统向监管机构上报必要存证信息,以便在出现脱敏控制违规事件时进行取证与溯源分析。在设计和实现上，对监管机构存证接口要求如下：

a) 向所属监管机构上报存证信息，应遵循最少必要原则，即在本地存储全部存证信息，向所属监管机构上报取证、溯源所需的最少必要信息；
b) 向所属监管机构上报存证信息之前,应就上报内容、采用协议等信息，进行确认；
c) 市场监管数据处理者与所属监管机构之间的存证信息传输应使用具备低开销、防篡改、抗抵赖的安全通信协议，确保证据信息的完整性、真实性和可靠性；
d) 监管机构对隐私信息处理者采用事中检查机制，确保数据处理行为合法合规。

8.2 通报与处置接口的技术要求

当市场监管数据流转脱敏过程中出现违反脱敏控制的事件时，在设计和实现上，对通报与处置接口的要求如下：

a) 在发生脱敏控制违规事件后，应根据事件的影响程度，及时向应用关联的单位、机构、主管部门或国家相关部门报送事件信息。报送的事件信息包括但不限于：发现事件的人员、时间、地点，涉及的隐私信息，发生事件的系统名称，对其他互联系统的影响等；
b) 发生违规事件的单位应提供相关接口，配合国家主管部门完成事件调查和溯源；
c) 具体通报详细要求参见团体标准《侵权事件通报与协查技术要求》（T/CSAC XXXX-YYYY）。

8.2.1 脱敏控制违规事件通报接口

出现脱敏控制违规事件后，在遵守《侵权事件通报与协查技术要求》（T/CSAC XXXX-YYYY）的基础上，对涉事市场监管数据处理者的要求如下：

a) 涉事隐私信息处理者，应对违反脱敏控制事件的影响程度展开评估，及时向应用关联的单位、机构、国家主管部门通报违规事件信息；
b) 通报事件信息包括但不限于：发现事件的人员、时间、地点，涉及的隐私信息，脱敏意图，违规类型等；
c) 涉事隐私信息处理者,应提供相关取证接口，配合国家主管部门或者其他相关部门完成事件调查；
d) 涉事隐私信息处理者提供的取证接口，应支持国家主管部门获取存证信息，开展违规事件调查和问题溯源。

8.2.2 脱敏控制违规事件处置接口

针对脱敏控制违规事件的处置，在遵守《侵权事件通报与协查技术要求》（T/CSAC XXXX-YYYY）的基础上，对涉事隐私信息处理者的要求如下：

a) 脱敏控制违规事件导致隐私信息所有者个人信息权益受到侵害时，应依照相关法律规定及时告知隐私信息所有者；
b) 脱敏控制违规事件发生后，应提供相关接口，允许隐私信息处理者删除相关隐私信息；
c) 脱敏控制违规事件发生后，涉事隐私信息处理者，应按照脱敏控制策略，重新进行本地收敛脱敏。

附 录 A
（资料性）
脱敏控制示例

A.1 概述

本附录以版式文档为例，展示脱敏控制流程，重点介绍脱敏控制策略生成、脱敏算法选择执行等环节，供脱敏控制系统设计者参考。

本示例中，某隐私信息提供者拥有一份版式文档，其中包含不同信息模态的隐私信息。由于不同应用场景下的各种业务需求，该版式文档在不同的隐私信息处理者之间流转共享。在版式文档流转共享过程中，各隐私信息处理者采用脱敏控制流程保护版式文档中的隐私信息。

本示例可以形式化描述为如下：含有隐私信息的版式文档 X，隐私信息提供者 S，脱敏控制策略 P，其中，$X=\{X_1,X_2,\dots,X_k,\dots,X_n\}$ 由n个隐私信息分量组成，每个隐私信息分量 X_k 的组成内容是 $X_k=\langle c,A,\Gamma,\Omega,\Psi,P\rangle$,其中，$c$ 是隐私信息分量的内容，A 是隐私属性向量（量化隐私信息分量及分量组合的保护程度），Γ 是广义定位信息集合，Ω 是审计控制信息集合（流转过程中的主客体信息和被执行的操作记录），Ψ 是脱敏控制操作集合（信息分量及其组合可被执行的操作），P 是脱敏控制策略。在信息分享过程中，S_{i-1} 将信息分享给 S_i，S_i 再分享给 S_{i+1}，信息要根据三者的传递关系和隐私信息接收者的不同，逐渐减少信息所含内容。

A.2 面向版式文档的跨域脱敏控制示例

面向隐私版式文档的脱敏控制的过程如下：

a) 脱敏控制策略生成，该过程包括脱敏意图理解和脱敏控制策略生成，具体过程如下：
   1) 脱敏意图理解：隐私信息处理者执行首次脱敏时，根据提供的脱敏意图生成机器可识别、可执行的脱敏要求；执行迭代脱敏时，根据前序隐私信息处理者的脱敏控制策略解析生成相应脱敏要求；
   2) 脱敏控制策略生成：为了满足脱敏要求，对分享的版式文档生成脱敏控制策略 P，划分需脱敏的内容。在迭代脱敏过程中，隐私信息处理者提取已有脱敏控制策略，并结合当前隐私信息提供者的属性和隐私信息接收者的隐私保护能力，生成新的脱敏控制策略。针对信息分量X_k，根据已有脱敏控制策略$X_k.P_{exist}$，结合当前分享者S_i的属性和接收者S_{i+1}的隐私保护能力，迭代生成隐私信息分量X_k的第 j 条脱敏控制策略 $X_k.P_j$、调整后的脱敏控制策略$X_k.P_j$ 以及控制集合调整动作 t；

b) 脱敏算法选择执行，该过程包括敏感数据识别、脱敏算法选择、脱敏算法识别、脱敏效果评估，具体过程如下：
   1) 敏感数据识别：使用关键词匹配、支持向量机、自然语言处理等信息识别算法和人工方式，根据数据特征和使用环境，标识版式文档中的敏感数据，包括其位置和格式。对数据进行分类分级，明确隐私数据的类别和敏感级别；
   2) 脱敏算法选择：根据脱敏控制策略、隐私信息分量类别及敏感级别，确定脱敏效果期望。遍历已有脱敏算法集合 Ψ 及其参数，评估各算法的脱敏效果。根据期望和评估结果，通过映射表或机器学习，选择候选脱敏算法，构建与脱敏控制策略对应的脱敏算法集合；
   3) 脱敏算法执行：基于脱敏控制策略 $X.P$，对版式文档 X 中的每个隐私信息分量X_k，在不同信息模态下执行脱敏算法。针对不同的信息模态（如图像、文字等），根据保护策略实施差异化脱敏；
   4) 脱敏效果评估：脱敏操作完成后，进行脱敏效果评估以确保文档保持可用性且不含到达脱敏效果期望阈值。利用深度学习模型检测可能的隐私泄露，使用数据质量评估工具确保数据可用性和一致性，同时实时评估隐私信息接收者的防护能力，以确保个人数据得到有效保护；

c) 控制策略可控传递，该过程包括控制策略可控传输的保密性实现、真实性实现、安全性实现，具体过程如下：
   1) 保密性：使用加密技术确保控制策略在传输过程中的保密性，实施基于角色的访问控制，仅授权的隐私信息接收者能解密和访问策略；

2) 真实性：利用数字签名确认策略的真实性，详细记录传输过程以保证可验证性和追溯性；
3) 安全性：采用可信执行环境技术保障处理过程的安全性；

d) 控制策略迭代调整，该过程包括脱敏控制策略解析、更新、防篡改，具体过程如下：
1) 脱敏控制策略解析：利用自然语言处理技术解析前序隐私信息处理者嵌入的脱敏控制策略，生成操作性强的脱敏控制策略；
2) 脱敏控制策略更新：通过规则引擎，根据隐私信息接收者的隐私保护能力、应用场景和数据模态等动态更新脱敏控制策略；
3) 脱敏控制策略防篡改：利用数字签名技术对更新后的脱敏控制策略进行签名，以确保策略的真实性和防篡改性；

e) 策略执行可信验证，该过程包括策略执行远程验证、审计日志记录、传播链验证，具体过程如下：
1) 远程验证：使用远程验证技术，确保隐私信息接收者能验证后序隐私信息处理者是否按预期执行了脱敏控制策略；
2) 审计日志记录：通过安全审计日志系统记录和分析隐私信息处理过程中的所有操作，保证脱敏控制策略执行的可验证性和可追溯性；

f) 脱敏过程存证，该过程包括脱敏过程日志存证、存证记录防篡改，具体过程如下：
1) 脱敏过程日志存证：记录数据脱敏的各个阶段活动，包括数据采集、脱敏方法、执行时间、执行者身份等信息；
2) 存证记录防篡改：采用数字签名技术确保存证记录的完整性和真实性。

附 录 B
（资料性）
按需脱敏过程示例

B.1 概述

在网约车出行服务系统中，会涉及大量的用户隐私信息，例如：位置数据、行程详情、银行账号和个人习惯等。出行服务系统在日常运营中，会针对上述敏感个人信息进行采集、脱敏、计算、共享和删除等各种操作，若处理不当，可能会导致严重的隐私泄露。在脱敏控制的协同下，按需脱敏可针对业务系统不同阶段的隐私信息跨域流转提供按需隐私保护能力，支撑在不泄露用户具体数据的前提下，实现数据的有效利用。

本附录以出行服务系统的数据流转为例，介绍了按需脱敏在不同数据流转场景的示例及使用方法，供设计开发脱敏控制以及按需脱敏功能时参考。

B.2 按需脱敏操作过程示例

当出行服务结束后，出行服务过程中收集的隐私信息被上传至后台信息服务系统。此阶段后数据流转过程如图B.1所示。出行服务系统在符合个人信息保护要求的条件下，结合具体的业务内容，可以在本系统内合规地脱敏、存储、使用和删除收集的个人信息，也可以在同机构跨系统、跨机构跨系统等场景下进行隐私信息流转。

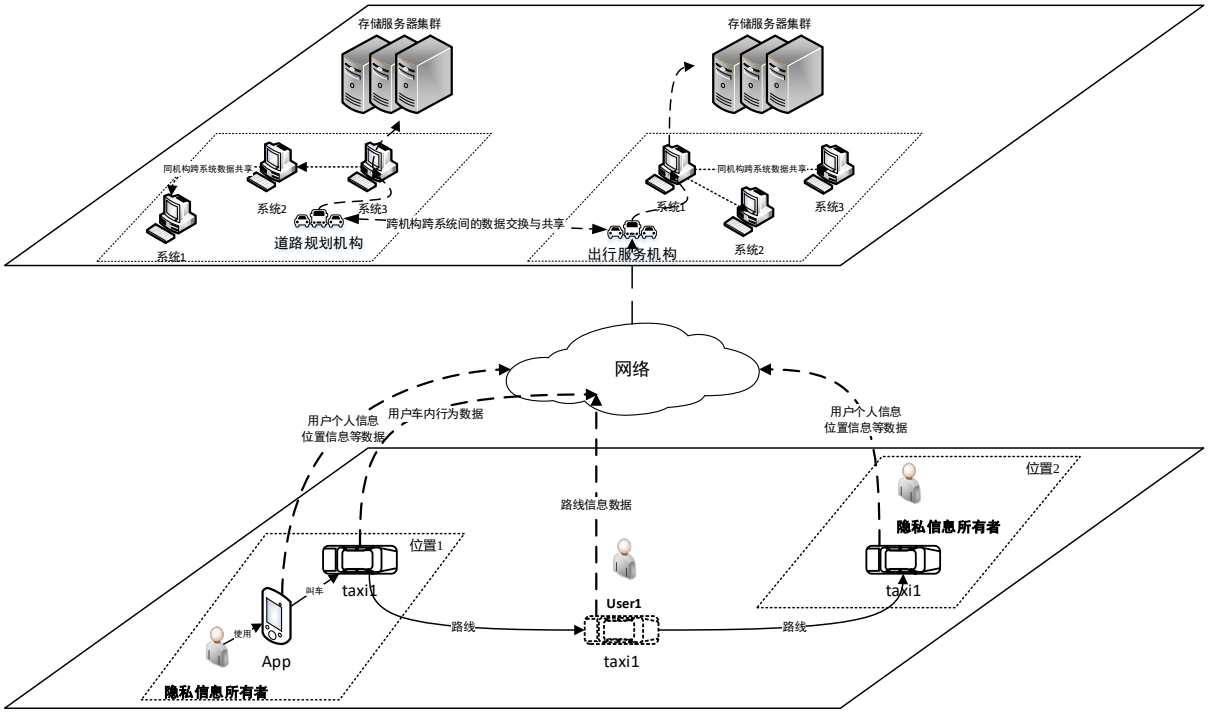

图 B.1 出行服务数据流转示意图

B.3 出行服务系统

B.3.1 导航过程中

在导航过程中出行服务数据可以不脱敏，原始出行数据示见表B.1。

表 B.1 原始出行数据示例（用于导航，本示例系 AI 生成）

手机号码	姓名	订单号	银行卡号	支付账号	当前地址	目的地址
28187829965	张三	396537022565915380530859437422 9	955880233087 0599	28187829965	广西壮族自治区玉林市北流市塘岸收费站入口(北海方向)	广西壮族自治区玉林市北流市城西一路 16 号朝阳旅社(城西一路)
25708026968	李四	390086189924410740605595764682 4	955880226161 5799	25708026968	四川省攀枝花市东区新源路 110 攀枝花市公安局	四川省攀枝花市东区新宏路与机场路交叉口西南 150 米学府广场
25938458003	王五	257316701149557223481131466286 1	955880226161 5799	25938458003	重庆市城口县复兴街道太和社区银子岩隧道龙城宏翰复兴派出所(城口县复兴街道社区卫生服务中心西北)	重庆市城口县城口县朱家沟
28281903000	赵六	233175952402818818344786041098 0	622200226161 5798	28281903000	广西壮族自治区崇左市天等县 506 县道南 150 米社区医院	广西壮族自治区崇左市天等县天宝路西 100 米

B.3.2 导航结束后

在导航结束后，根据隐私信息所有者设定的脱敏要求，出行服务提供商，即隐私信息处理者，针对不同模态信息采用适合的脱敏算法集合处理。例如：为了保护用户隐私，通过匿名化处理方法对移动电话号码、支付信息等隐私信息进行保护，达到对可标识到具体个人的信息匿名化处理。在位置信息等发送到服务器前，本地设备可通过实施差分隐私技术添加随机噪声。例如，对于出发地、目的地等位置数据可以添加一定范围内的随机偏移。出行服务后的数据脱敏示例见表B.2。

表 B.2 出行服务后的数据脱敏示例（用于路线规划算法优化，本示例系 AI 生成）

手机号码	姓名	订单号	银行卡号	支付账号	当前地址	目的地址
281****9965	张**	3965370225*********08594374229	95588*****870599	281****9965	广西壮族自治区玉林市北流市塘岸收费站入口(北海方向)	广西壮族自治区玉林市北流市城西一路 16 号朝阳旅社(城西一路)
257****6968	李**	3900861899*********55957646824	95588*****615799	257****6968	四川省攀枝花市东区新源路 110 攀枝花市公安局	四川省攀枝花市东区新宏路与机场路交叉口西南 150 米学府广场
259****8003	王**	2573167011*	95588*****	259****8003	重庆市城口县复兴街	重庆市城口县城口县朱家

		*********11314662861	615799		道太和社区银子岩隧道龙城宏翰复兴派出所(城口县复兴街道社区卫生服务中心西北)	沟
282****3000	赵**	2331759524*********47860410980	62220*****615798	282****3000	广西壮族自治区崇左市天等县506县道南150米社区医院	广西壮族自治区崇左市天等县天宝路西100米

B.4 不同系统数据流转

B.4.1 同机构

出行服务系统在完成导航服务后，所收集的个人信息需要按照脱敏控制的要求进行处理，脱敏后的隐私信息可用于本机构出行服务外其他业务功能，例如：纠正出行服务的路线、精确线路的导航、分析实时的道路状况等功能。不应用于与业务不相关的功能，例如：分析用户的家庭住址、单位地址、消费水平和个人偏好等。因此，当需要在出行服务商内部其他系统使用用户数据时，应对上述用户隐私信息，感知隐私分量，结合信息模态等信息，对其采用合适的脱敏算法进行处理。同机构不同系统数据流转的数据脱敏示例见表B.3。

表B.3 出行服务后同机构不同系统数据流转下的按需脱敏结果（用于机构内区域车辆调度支持，本示例系AI生成）

手机号码	姓名	订单号	银行卡号	支付账号	当前地址	目的地址
281	张**	396	955	281	广西壮族自治区玉林市北流市塘岸收费站	广西壮族自治区玉林市北流市城西一路
257	李**	390	955	257	四川省攀枝花市东区新源路	四川省攀枝花市东区新宏路与机场路交叉口
259	王**	257	955	259	重庆市城口县复兴街道太和社区	重庆市城口县城口县朱家沟
282	赵**	233	622	282	广西壮族自治区崇左市天等县506县道	广西壮族自治区崇左市天等县天宝路

B.4.2 不同机构

在出行服务系统向不同机构的其他系统进行数据流转的场景中，出行服务机构需要综合考虑使用场景、隐私信息接收者的隐私保护能力等因素，生成脱敏控制策略，并将其嵌入待流转数据中，以约束接收隐私信息的隐私信息接收者和隐私信息处理者的脱敏操作。接收隐私信息的隐私信息处理者需要按照脱敏控制要求对流转的隐私信息执行脱敏操作，并进行脱敏效果评估，直至完成脱敏控制策略中脱敏效果期望的要求。不同机构不同系统数据流转的数据脱敏示例见表B.4。

表 B.4 出行服务系统向不同机构系统进行数据流转场景的按需脱敏结果示例（用于旅游机构统计，本示例系 AI 生成）

手机号码	姓名	订单号	银行卡号	支付账号	当前地址	目的地址
281****9965	***	000000000000000000000000000000000	00000000000000000	00000000000	广西壮族自治区	广西壮族自治区
257****6968	***	000000000000000000000000000000000	00000000000000000	00000000000	四川省	四川省
259****8003	***	000000000000000000000000000000000	00000000000000000	00000000000	重庆市	重庆市
282****3000	***	000000000000000000000000000000000	00000000000000000	00000000000	广西壮族自治区	广西壮族自治区

参 考 文 献

[1] GB/T 25069-2022 信息安全技术 术语

[2] GB/T 35273-2020 信息安全技术 个人信息安全规范

[3] GB/T 31500-2015 信息安全技术 存储介质数据恢复服务要求

[4] 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）

[5] 中华人民共和国数据安全法（2021 年 6 月 10 日第十三届全国人民代表大会常务委员会第二十九次会议通过）

[6] 中华人民共和国个人信息保护法（2021 年 8 月 20 日第十三届全国人民代表大会常务委员会第三十次会议通过）

[7] 关键信息基础设施安全保护条例（2021 年 4 月 27 日国务院第 133 次常务会议通过）

[8] 网络安全审查办法（2021 年 11 月 16 日国家互联网信息办公室 2021 年第 20 次室务会议审议通过）