ICS 33.030
CCS M21

团　　体　　标　　准

T/CAAAD 004-2022　　T/CCSA 424-2022

互联网广告 匿名化实施指南

Digital advertising-Implementation guide of anonymization

2023 - 01 - 03 发布　　2023 - 01 - 06 实施

中国广告协会　中国通信标准化协会　　发 布

版权声明

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。

本文件为互联网广告数据安全与个人信息保护系列标准之一，该系列标准的名称和结构预计如下：

——《互联网广告 数据应用和安全技术要求》；

——《互联网广告 个人信息告知同意指南》；

——《互联网广告 匿名化实施指南》；

——《互联网广告 群体标识技术要求》；

——《互联网广告 数据分类分级指南》；

——《互联网广告 数据流通平台技术架构》；

——《互联网广告 隐私计算平台技术要求》。

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。

本文件由中国广告协会和中国通信标准化协会共同提出，并分别归口。

本文件起草单位：中国信息通信研究院、上海数据交易所有限公司、中国广告协会、蚂蚁科技集团股份有限公司、公安部第三研究所、上海世代企业发展促进中心、利欧集团数字科技有限公司、郑州信大捷安信息技术股份有限公司、北京快手科技有限公司、北京京东世纪贸易有限公司、秒针信息技术有限公司、北京师范大学、华控清交信息技术（北京）有限公司、北京瑞莱智慧科技有限公司、上海柠盟数据技术有限公司、阳狮广告有限公司。

本文件主要起草人：杨正军、杨阳、申翔宇、崔妍、樊振华、白晓媛、胡永涛、邱俊琼、高富平、周崧陞、姚轶珺、刘献伦，刘为华、落红卫、王昕、刘晓燕、张泽华、李然、刘骁、刘沛、吴沈括、张浩明、范杰、郭颖、瞿喆、陈维娜、陈俊丞、杨燕。

引 言

互联网广告业务是数据使用、加工、提供和委托处理密集的行业领域。在广告投放、程序化交易、广告归因等场景，均涉及到个人信息相关的数据在不同机构间的提供、加工、传输、使用等处理行为，由于互联网广告业务的多机构参与的生态长链的特性，很多机构数据处理无法直接获得个人同意，这些数据处理行为在个人信息保护、商业秘密保护、国家安全等方面，面临安全风险。

匿名化是互联网广告领域实现数据安全利用的重要路径。在互联网广告数据处理活动中，数据是动态变化的，包括控制主体的变化、数据形态的变化、数据内容的变化等。要使动态下的数据匿名化能够有效进行和能被证明，有必要在互联网广告行业明确匿名化定义，形成行业共识，并提出实现路径。在合法、合规的前提条件下，制定能平衡安全合规和市场需求的标准，充分发挥互联网技术的优势，增强数字行业的竞争力，发挥数据要素的商业价值。

为适应信息通信业发展对标准文件的需求，由中国通信标准化协会和中国广告协会共同组织制定该团体标准，推荐有关方面采用。有关对本文件的建议和意见，向中国通信标准化协会和中国广告协会反映。

互联网广告 匿名化实施指南

1 范围

本文件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。

本文件适用于各类互联网广告业务，包括广告投放、程序化交易、广告监测等应用场景下的数据匿名化处理活动。其他领域的相关活动也可参照进行。

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 35273 信息安全技术 个人信息安全规范

GB/T 37964 信息安全技术 个人信息去标识化指南

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，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：个人信息经匿名化处理后所得的信息不属于个人信息。

3.3

去标识化 de-identification

个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

3.4

数据标记 data token

数据上承载的信息主体标识(符)经适当的去标识化处理后的结果。

注：数据标记在数据匿名化处理过程中具有替代标识(符)的主键索引与归因作用。

3.5

广告主 advertiser

为推销商品或者服务，自行或者委托他人设计、制作、发布互联网广告的自然人、法人或者其他组织。

3.6

互联网广告经营者 operator

接受委托提供互联网广告设计、制作、代理服务的自然人、法人或者其他组织。

3.7

互联网广告发布者 publisher

利用互联网媒介为广告主或者广告主委托的广告经营者发布广告的自然人、法人或者其他组织。

3.8

媒体 media

发布、展示广告的载体。

3.9

受众 audience

广告主投放广告触达并产生影响的人口群体。

4 缩略语

下列缩略语适用于本文件。

ADX	广告交易市场	Advertising Exchange
DMP	数据管理平台	Data Management Platform
DSP	需求方平台	Demand Side Platform
IDFA	广告标识符	Identifier For Advertising
IMEI	国际移动设备识别码	International Mobile Equipment Identity
RTB	实时竞价	Real Time Bidding
SSP	供应方平台	Supply Side Platform

5 匿名化概述

5.1 参考架构

互联网广告匿名化实施架构如图1所示，以机构的数据处理行为为对象，通过“技术保障、评估规制、过程控制”的互信制衡机制，构建安全可信环境，开展匿名化处理，实现数据合规利用。

第一，建立业务匿名化开展所需的合规评估见证规则与方法，使整个数据利用过程的各机构的各种处理行为能够受约束；

第二，在开展数据利用前，通过适当的、高级别的数据去标识化、密态化等技术处理，使得在没有其他独立管理的额外信息的辅助下，数据对其他各方为“无法识别特定自然人且不能复原”，并形成有效证据；

第三，在数据利用过程中，通过行业共识的过程控制体系，通过限定和控制各行为环节的数据内容、处理形式和约束条件，形成受控环境和安全边界，使得数据在各个处理行为环节中保持匿名化状态，更能通过对关联的控制而约束数据的合规使用，并有效留存相应符合匿名化要求的合规性证据；

第四，在数据利用后，保存并维护各种存证备案的内容，以备需要时可以有相应的材料及依据予以合规性证明。

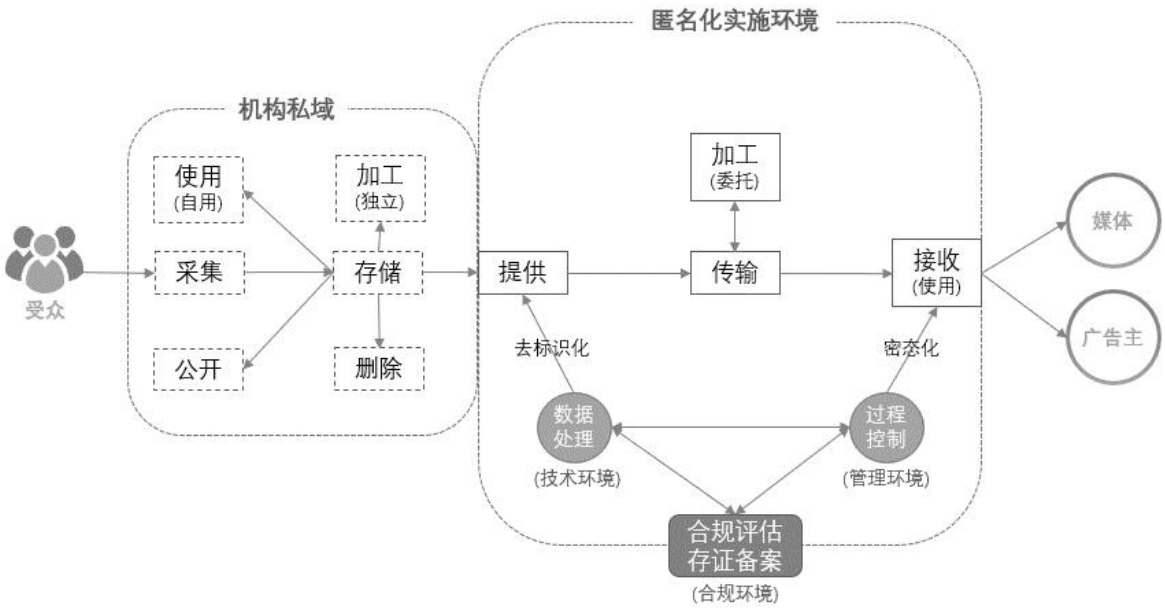

图 1　互联网广告数据处理行为与匿名化实施架构示意

5.2　适用主体

匿名化处理适用的主体包括广告主、广告经营者（如 DSP、SSP、广告代理等）、广告发布者（如媒体）、及其他服务提供者（如 DMP，广告监测公司等）四类角色。相关主体应根据自身角色定位、处理行为、处理数据内容，判定是否进行匿名化处理。互联网广告场景、行为与主体关系图如图 2 所示。

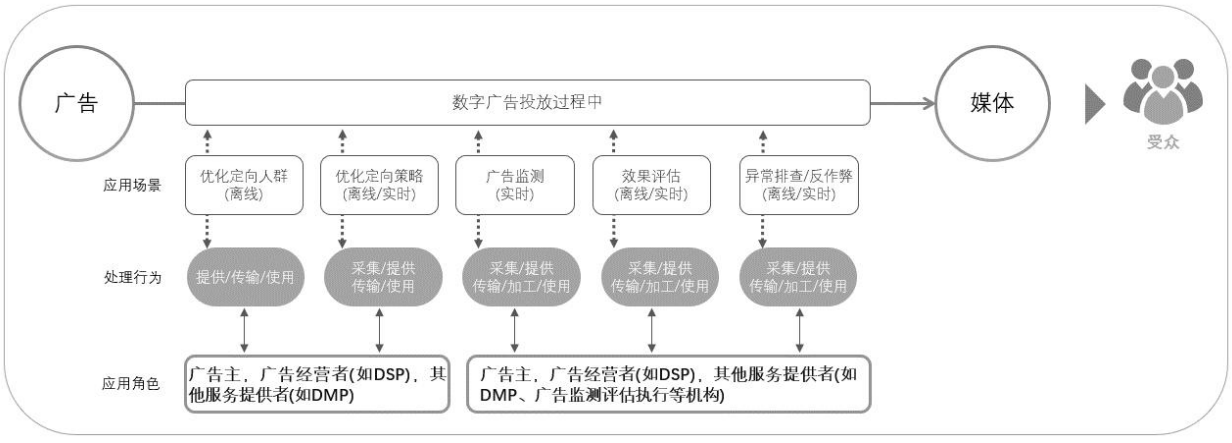

图 2　互联网广告场景、行为与主体关系图

5.3　适用行为

匿名化处理适用的行为主要包括“提供、加工(联合)、传输、使用(他用)”等多主体域间的数据处理行为，不包括“采集、存储、删除、公开、加工(独立)、使用(自用)”等单主体域内的数据处理行为。

5.4　适用对象

匿名化处理的适用对象主要为互联网广告业务中所必需的、包含个人信息或可能导致形成个人信息的数据，一般由标识+标签组成，常见组成与分类见附录 A。

5.5 适用场景

互联网广告包括广告投放、程序化交易、广告监测、映射、人群包、留资、归因等业务场景， 根据业务场景中广告数据的不同处理行为能够获取信息主体同意的难易程度、及主体与对象间的行为关系，针对各处理行为有序开展匿名化处理，具体参考附录 B。

6 匿名化目标与原则

6.1 匿名化目标

6.1.1 构建可信环境

构建安全可信的匿名化处理环境，使得行为的三要素“主体、行为、对象”为可管控、可取证、可审计。

6.1.2 开展合规评估

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，形成合规性结论。

6.1.3 基础技术保障

实施环境的匿名化处理技术应能避免重识别的风险，且能控制重关联行为，所必需的辅助信息应单独维护和管理，以形成独立的控制和证明。

6.1.4 使用范围限制

匿名化处理的数据及使用，限定在法律规定或个人同意的必要事项或目的所限定范围内。

6.2 匿名化原则

6.2.1 主体权益保护

匿名化过程应满足国家对数据安全和个人信息保护等的相关要求，保障信息主体享有的法定权利，不应与信息主体的基本权利和自由相冲突。

6.2.2 平衡产业发展

匿名化处理在满足合规合法的前提下，应能够满足互联网广告业务的合法、可控的数据应用需求。

6.2.3 机构互信制衡

各方形成共识，共同组成“技术保障、评估规制、过程控制”三者相互信任制衡的服务与控制体系，开展匿名化处理与数据应用相关活动。

6.2.4 过程有序可控

匿名化的实施过程应能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。

7 匿名化过程

7.1 概述

匿名化处理过程，包括环境维护、确定目标、技术处理、效果评估和行为控制等步骤，并对上述各步骤的实施过程和效果进行有效的管理和监测。匿名化处理过程如图3所示；匿名化处理过程的案例见附录C。

图 3　匿名化处理过程

7.2　环境维护

7.2.1　总体要求

匿名化处理的环境包括技术环境、合规环境和管理环境，形成“技术安全、评估规制、过程控制”相互信任制衡体系，具备控制与服务能力，使得参与各机构的匿名化处理行为安全、合规和有序。

7.2.2　技术环境

开展匿名化处理的存储计算与网络资源等基础技术设施，应满足以下条件：

——安全，基础设施的安全能力符合国家行业主管部门的要求；

——受控，对数据处理和输入/输出具有管控机制，且可被证明；

——可信，数据处理和输入/输出的过程和结果可被测评和审计；

——可证，数据处理过程按照 7.4 技术处理要求进行，且可被证明。

7.2.3　合规环境

根据广告业务场景，梳理业务流程、业务对象、合作条款、数据合约，收集评估基础材料，参考附录D，提炼和分类业务的影响因子，依据法律条款推论各种影响因子间的互斥/相容性关系，建立影响因子间关系的合规(逻辑)规则库，封装形成评估方法工具，构成合规环境并定期维护更新，具体包括：

——影响因子：包括主体资质、授权(同意)依据、数据分类分级、数据预处理方式、处理行为约束等；

——规则量化：依据法律条款推论各种影响因子间的互斥/相容性关系，建立影响因子间关系的合规(逻辑)规则库；

——工具封装：合规评估工作应利用封装化的方法工具进行，以保障证据的有效性。方法工具应及时修正，以及时响应法律法规的进展和有权机构的监管要求；

——记录存档：技术测评结论、合规评估报告，评估见证书或法律意见书、过程监管记录等应妥善保存，其中实施机构(组织)间的数据处理行为相关的，宜在公信机构存证备案，以适时出证。

7.2.4　管理环境

管理环境由实施机构自行组建或联合公信机构、技术测评机构和合规评估机构等共同组建，应能响应合规评估的结论，参与管理各机构的行为过程，管理环境应满足以下要求：

——应具备分域管理功能，使参与数据匿名化处理的各方可自控分域数据，各方对自控域内的数据和加工行为负责；

——应能维护数据对提供方外的任意方匿名，支持数据匿名化加工，管理数据的传输方式，限制数据的使用方式；

——应能响应机构间的约定和先行评估的结论，控制标记下的数据关联，开启或禁止数据匿名化处理的过程；预备实时熔断能力，及时响应和制止风险事件；

——应能形成可审计的数据匿名化处理过程监管记录，并可进一步支持更高层级的监管。

7.3 确定目标

7.3.1 确定实施主体

匿名化发起的实施机构应核查相关的数据交换、利用或服务协议，确定需要开展匿名化处理的机构。

7.3.2 选择实施数据

确定需开展匿名化的数据，确定数据的主体标识与项值内容，具体包括：

——了解数据是否属于组织列入的重要数据或敏感信息范畴，数据应用时是否存在匿名化的要求；

——了解数据来源相关信息系统的业务特性，了解这些数据采集时是否做过匿名化的相关承诺；

——了解业务内容和业务流程，了解数据是否涉及重关联行为的控制要求；

——依据法律法规及本文件，判断待处理数据是否存在匿名化需求。

7.3.3 限定处理行为

实施机构应根据 5.5 适用场景的划分，确定自身业务的匿名化适用性，并根据自身角色，参照 5.3 适用行为的分类，限定拟开展匿名化的数据处理行为，并准备对应措施以开展行为控制。

7.4 技术处理

7.4.1 总体要求

遵循GB/T 37964-2019，选择适当的数据预处理技术方法，开展数据预备处理。

7.4.2 预备数据的格式与内容

预备处理后的数据，应符合以下格式与内容规格，使其在匿名化处理环境中对原始处理方外的其他方匿名，并进行相应的分类，使其能被有序控制关联及限制后续使用。预备处理形成的数据的最小元数据定义、描述及约束条件如下：

——标识(符)，指数据中信息主体的唯一性识别编码。须对原始标识(符)进行去标识化处理，转换为无识别性的“标记”，并以“标记”为索引进行数据匿名化实施；

——数据项，指数据不同维度的定义（如数据库的各种字段定义）。原始标识(符)不得成为数据项进入实施；除非评估认定具备个人同意或其他合法性基础，数据项不得含有敏感个人信息的内容（敏感个人信息判定参见 GB/T 35273—2020 附录 B）；

——数据值，指对数据项的赋值，包括字符型、数字型、日期型、日期时间型、布尔型、二进制等类型。原始标识(符)不得成为数据值的部分或全部内容；除非具备个人同意或其他合法性基础，数据值宜符合 K 匿名要求。

7.4.3 数据标识(符) 技术处理

针对互联网广告行业的常用标识(符)的处理技术，应遵循GB/T 37964-2019，并满足以下条件。

——标记匿名：

- 标识经处理后成为标记，标记不可逆，且标记生成所必要的额外信息或密钥被独立维护与管理，处理过程中使用的相关密码算法和技术应符合国家主管部门以及相关国家标准/行业标准的要求；
- 标记能够抗密码分析，在匿名化处理环境内，除生成标记的实施主体之外，其它任何机构主体无法识别和复原识别至特定信息主体。

——标记隔离：

- 标记在实施主体私域内具有唯一性；
- 在各个实施主体的同一信息主体的“标记”各不相同。

——关联控制：

- 可通过密码算法等相应技术，控制各方标记间的关联；并依据合规评估结论，将数据关联到已识别的信息主体标识(符)，且只对评估合格范围内的信息主体进行；
- 标记间关联的控制密钥由独立管理机构(部门)负责分配和实施管理，该管理机构(部门)应具备充足的安全保障能力，并保证其过程规范性和技术通用性。

——有据可查：

- 标记生成、受控关联的过程有据可查，以便于溯源；
- 标记生成和受控关联的过程能记录涉及的实施主体、数据标记、时间戳等信息，并可靠保存，以便于在风险事件发生后进行追查和补救。

7.4.4　数据项/值匿名技术处理

为应对不同的应用场景、使用目的、个人同意等条件，应选择使用 GB/T 37964-2019 的数据处理技术，对拟实施的数据项及数据值（数据内容）进行技术处理。

以“K匿名模型”为例，数据项值的技术处理效果如下：

——时间相关数据项：最少应区分为实时、小时-天、周-月、年-无效四层；

——时间无关数据项：以处理后数据集的该数据项的相同赋值条数为计，最少应区分为<1000,1000-5000,>5000 三层。

7.5　效果评估

7.5.1　技术测评

实施机构自身或委托专业技术测评机构，参考国内相应的个人信息去标识化效果分级与评定标准对拟实施的数据技术处理的匿名化效果进行验证。

7.5.2　合规评估

采用自评估或委托评估等方式，以数据匿名化处理活动相关的实施主体、过程行为、实施数据等为评估对象，妥善利用合规环境，形成合规性评估报告和法律意见书。

7.6　行为控制

7.6.1　提供行为

基于合法控制的数据，有限输出经预备处理形成的、可匿名化处理的数据。其提供行为的要求为：

——源数据为合法取得、合法持有并实际控制，不应将不具备合法性基础的源数据直接提供；

——响应数据应用需求，对拟提供的数据进行符合 7.4 的技术处理；

——通过数据交换协议、合同等方式，约定数据接收方的责任和义务；

——准确记录和存储所提供数据的实施内容和情况，包括委托处理、共享使用、权益转让等的日期、规模、目的以及数据接收方的基本情况等。

7.6.2　传输行为

基于合法的数据应用，从提供方获取数据。其传输行为的要求为：

——接收方应具有相应的数据安全能力以保护信息主体权利，不得有法律法规所禁止的情形，如获取后非法出售、非法提供等；

——严格遵守与提供方约定的合同义务，对任何超越范围和违反合同约定的使用行为承担法律责任；

——如有数据再提供或转委托的需求，应在与提供方的合同中明确约定；转委托应对被委托进行数据计算的第三方的行为负责；

——应经由加密状态下的求交计算，筛选并仅传输有限交集的数据标记所对应的、与提供方的合同所约定的“属性、行为、关系”等数据内容，禁止主体标识(符)的传输；
——如需将接收数据内容关联至已识别的信息主体原始标识(符)，接收方须具有合法、明确、具体的个人信息处理目的，且已经具备后续相关行为的个体同意等合法性基础。

7.6.3 加工行为

接受提供方或接收方的委托，遵守先行评估结论和委托协议的约束，对依约获取的数据进行计算处理，形成满足不同目的的数据(集)或数据服务。其加工行为要求为：

——严格依据与委托方签署的委托协议而进行存储、加工(计算)、销毁等数据处理行为，对任何超越范围和违反协议的行为承担法律责任；
——具备安全适当的技术手段、组织措施，防范数据泄露；必要情况下，计算方还宜通过国内数据安全保护相关审核，以证明其具备防止数据泄露的能力；
——在委托方技术平台之外进行加工处理时，应受匿名化实施环境的约束，使用独立的数据标记且关联受控。

7.6.4 使用行为

数据使用环节，应区分数据利用模式对个人识别性的要求，基于评估见证结论，充分考虑对个体、群体的识别性影响，在保持传输到达或加工后的数据的匿名状态下，限定数据的有限使用。其使用行为要求为：

——鼓励“非识别”的使用：
- 数据应用指向群体或无需明确身份的个体，接收方无需取得同意，经评估后获取经 7.4 技术处理的数据，开展非识别下的数据应用，如归因、统计、监播等。

——控制“已识别”的使用：
- 数据应用指向个体，接收方的数据处理行为已取得个人信息主体的同意，将“个人同意范围内的数据项/值(标签)”关联至信息主体标识(符)，从而开展已识别下的数据应用相关业务，如定向投放；
- 已识别下的数据利用，不论是否经过数据加工行为，应严格评估接收方数据处理行为取得同意的方式和授权范围。

——禁止“可识别”的使用：
- 数据应用指向个体，使用前未获同意，遵循其他法律条款，从数据中重新识别个人后开展应用；
- 该模式原则上应排除在商业化的互联网广告利用外。

7.7 过程监管

7.7.1 过程记录

机构组织内的数据匿名化，应确保匿名化的每一步骤均约束在匿名化处理环境中实现了预定目标，并有效记录和保存。具体要求为：

——在匿名化的各个步骤中，需在确定目标步骤撰写匿名化工作方案，明确各步骤要完成的工作，并在确定目标、技术处理、效果评估阶段记录工作过程和结果，形成文档；
——组织管理层在匿名化处理的各个步骤完成时，对该阶段记录文档进行审查，检查输出文档是否齐全和内容完备，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；
——监控审查过程也应记录到文档中，记录内容至少包括监控审查对象、时间、过程、结果和措施等内容。

7.7.2　存证备案

机构组织间的数据匿名化，除7.7.1过程记录外，还应在公信机构，以数据交换/共享/流通/交易的合约为单位，有效备案并存证关键记录，以形成有效的匿名化证明，并支持审计与审查。具体包括：

——事前备案，将测评报告、评估报告、评估结论、与法律见证书进行备案；

——事中存证，匿名化处理执行过程关键记录进行存证，如关联控制记录；

——事后验证，匿名化处理后，支持审计机构对匿名化效果进行验证。

8　组织措施

8.1　组织管理

建立数据安全管理和评价考核制度，制定数据安全保护计划和风险评估机制，制定事件处置预案等安全制度，并组织开展教育培训等。

8.2　能力匹配

具备必要的业务资质与信息安全等级，具备与所面临的安全风险相匹配的安全能力，并采取合理管理措施和技术手段，保护个人信息的保密性、完整性、可用性。

8.3　数据治理

预先进行数据治理，履行数据安全保护义务，采取加密、脱敏、备份、访问控制、审计等技术或者其他必要措施，加强数据安全防护。

8.4　事件响应

发现滥用或泄漏等风险事件，立即通知事件相关方停止相关行为，采取或要求采取有效补救措施，控制或消除面临的安全风险；必要时解除业务关系，删除已传输接收的数据。

8.5　应用限制

区分数据应用对个人或群体的影响，限制数据应用方向与范围，开展数据合规管理与应用。

附 录　A
（资料性）
互联网广告数据组成与分类描述

以信息主体为观察对象，互联网广告匿名化实施的数据，由识别主体的“标识”，+ 描述主体属性/行为/关系的“标签”组成，互联网广告匿名化实施常见数据描述格式参见表 A.1。

表 A.1 互联网广告匿名化实施常见数据描述格式

分类			定义	举例	功能或作用
标识	标识数据	社会身份	直接关联个人的社会属性信息	姓名	1)区分社会个人（自然人）
					2)识别个人
		生物标识	借助技术手段可以核验个人身份的生物信息	人脸	1)区分生物个人
					2)验证身份
					3)医疗和健康研究
		数字标识	不直接与个人关联，但直接与某个人相联系的网络设备 ID	用户名等网络和设备 ID	1)区分网络用户
					2)链接现实主体与网络行为（记录）的纽带
					3)触达用户
标签	属性数据	自然属性	描述个人自然和社会属性	性别\出生\身高等	1)将人分类或分群
		社会属性		职称职位等	2)区分某人或识别个性特征
	行为数据		个人与时间和空间相关的行为或活动记录	个人行为、活动、社交等的记录	1)了解个人行为习惯，识别个性特征
					2)预测行动动向
	关系数据		个人与个人之间的关联性数据	如微信群	1）将人分类或分群 2）触达用户

附 录 B
（资料性）
互联网广告数据交换与利用场景

互联网广告包括广告投放、程序化交易、广告监测、映射、人群包、留资、归因等业务场景， 根据业务场景中的不同处理行为能够获取信息主体同意的难易程度、及主体与对象间的行为关系，针对各处理行为有序开展匿名化处理，具体参考表 B.1 互联网广告数据交换与利用常见场景简表。

表 B.1 互联网广告数据交换与利用常见场景简表

场景	行为	环节	交换数据内容	交换数据 ID 情况	交换方向/参与方	交换协议/技术
普通广告投放模式	曝光	①个人用户的客户端向媒体 web 服务器发出广告请求，	客户端信息	设备 ID user agent	C-S（客户端向媒体 web 服务器） S-S（媒体 web 服务器向自己或第三方的广告投放服务器）	嵌入的 js 代码或者 sdk
		②广告投放服务器根据预先设定的投放规则，判断向 web 服务器返回广告的投放信息，包含素材地址，链接地址等。	素材请求 监测代码	无	S-S（投放服务器向 cdn 以及背后的素材服务器、监测服务器发出（可能第一方，可能第三方））	HTTP
		③广告投放服务器反馈给 web 服务器素材地址和监测代码地址，并记录一次曝光。	素材请求 监测代码	无	S-S（广告投放服务器反馈给 web 服务器）	HTTP
		④web 服务器向客户端反馈请求。并记录一次 web 服务行为完成。	http 请求回馈信号	无	C-S（web 服务器向客户端）	HTTP
		⑤，客户端渲染素材，并执行监测代码，生成新的数据反馈给素材或监测服务器。	监测信息	设备 ID user agent	C-S（客户端向监测服务器或素材服务器）	HTTP

	点击	在广告曝光发生后，消费者个人在客户端触发点击行为，	客户端信息	设备 ID user agent	C-S（客户端向媒体的 web 服务器） S-S（web 服务器一路向广告投放服务器或者多个第三方监测服务器，最终到达广告主的落地页服务器）	HTTP 协议的 302 跳转
	点击后续	广告主落地页服务器收到点击转跳过来的客户端请求，执行 web 渲染，	客户端信息	设备 ID user agent	C-S（客户端向第三方监测服务器或者广告投放服务器的域）	嵌入的 js 代码或者 sdk
程序化竞价广告投放模式	映射	①个人用户的客户端向媒体 web 服务器发出广告请求，	客户端信息	设备 ID	C-S（客户端向媒体 web 服务器）	
		②媒体 web 服务器上的映射代码与 SSP 或 ADX 服务器交换映射 ID	客户端 ID 与映射 ID	设备 ID 映射 ID	S-S（媒体 web 服务器向 SSP 或 ADX 服务器）	如果是 PC 端 HTTP 协议的 302 跳转； 如果是移动端，采用 OAID 的 SDK 或者其他映射 ID 技术
		③SSP 或 ADX 服务器与 DMP 服务器请求获得指定 ID 对应的标签信息	映射 ID， 标签信息	映射 ID	S-S（SSP 或 ADX 服务器向 DMP 服务器双向）	
	竞价	④SSP 或 ADX 服务器向下游购买方 DSP 服务器发出询价广播	交易 ID， 映射 ID， 标签信息 交易用信息	映射 ID 交易 ID	S-S（SSP 或 ADX 服务器向 DSP 服务器）	
		⑤下游购买方 DSP 服务器与本方的 DMP 服	映射 ID， 标签信息	映射 ID	S-S（DSP 服务器向 DMP 服务器双向）	

		务器请求获得指定 ID 对应的标签信息（大部分为离线异步请求）				
		⑥买方 DSP 服务器向 ADX 服务器反馈出价请求和推送素材的 URL	交易 ID， 映射 ID， 交易用信息 素材信息	映射 ID 交易 ID	S-S（DSP 服务器向 ADX 服务器）	
		⑦ADX 服务器判断竞价，并反馈竞价结果给 DSP 服务器和 SSP 服务器（SSP 服务器可能会有第二次竞价过程并将结果反馈给 ADX 服务器）	交易 ID， 映射 ID， 交易用信息	映射 ID 交易 ID	S-S（ADX 服务器向 DSP 服务器和 SSP 服务器双向）	
	曝光	⑧胜出方 DSP 推送广告投放信息给 ADX 服务器或 SSP 服务器	交易 ID， 映射 ID， 素材信息 监测代码	映射 ID 交易 ID	S-S（DSP 服务器向 ADX 服务器或 SSP 服务器）	
		⑨ADX 服务器或 SSP 服务器反馈给 web 服务器素材地址和监测代码地址，并记录一次曝光	交易 ID， 映射 ID， 素材信息 监测代码	映射 ID 交易 ID	S-S（ADX 服务器向媒体 web 服务器）	
		⑩web 服务器向客户端反馈请求。并记录一次 web 服务行为完成	HTTP 请求回馈信号	无	C-S（web 服务器向客户端）	
		⑪客户端渲染素材，并执行监测代码，生成新的数据反馈给素材或监测服务器	监测信息	设备 ID	C-S（客户端向监测服务器或素材服务器）	
	点击	⑫在广告曝光发生后，消费者个人在客户端触	交易 ID， 映射 ID，	映射 ID 交易 ID	C-S（客户端向传递给媒体的 web 服务器）	HTTP 协议的 302 跳转

		发点击行为	客户端信息		S-S（web 服务器向 DSP 服务器，ADX 服务器，SSP 服务器最终到达广告主的落地页服务器）	
		⑬DSP 服务器将点击信息传递至 DMP 服务器	交易 ID， 映射 ID， 客户端信息	映射 ID 交易 ID	S-S（DSP 服务器向 DMP 服务器）	
	点击后续	⑭广告主落地页服务器收到点击转跳过来的客户端请求，执行 web 渲染	客户端信息 (+refer)	设备 ID user agent	C-S（客户端向广告主落地页服务器双向）	
		⑮广告主落地页服务器将点击后续行为传递至 DMP 服务器	交易 ID， 映射 ID， 客户端信息 (+refer)	映射 ID 交易 ID 设备 ID user agent	S-S（广告主落地页服务器向 DMP 服务器）	
广告监测模式-客户端嵌入式	曝光监测	①个人用户的客户端向媒体 web 服务器发出广告请求的同时向嵌入的 js 监测代码或者 SDK 发出请求	客户端信息 广告投放信息	设备 ID user agent	C-S（客户端向 web 服务器）	
		②js 监测代码或者 SDK 记录一次曝光，并记录客户端信息	客户端信息 广告投放信息	设备 ID user agent	C-T-S（客户端向嵌入的第三方域的 js 代码或者 SDK 的后台服务器发送）	嵌入的 js 代码或者 sdk
	点击监测	①个人用户的客户端向在媒体 WEB 服务器上的点击地址执行点击请求（包含了串行的点击代码）	客户端信息 广告投放信息	设备 ID user agent	C-T-S（客户端向嵌入的第三方域的 js 代码或者 SDK 的后台服务器发送）	

		②点击代码可以多次通过 302 协议跳转传递至下一个监测服务器	客户端信息 广告投放信息	设备 ID user agent	S-S（第三方域 js 或者 SDK 后台服务器之间）	HTTP 协议 302 跳转
	点击后续监测	客户端通过广告点击代码的 302 协议跳转到广告主落地页服务器，同时请求了嵌入在落地页服务器上的 js 代码或 SDK	客户端信息 广告投放信息	设备 ID user agent	S-S（第三方域 js 或者 SDK 向落地页服务器 客户端向落地页服务器）	HTTP 协议 302 跳转
广告监测模式-服务器端接口	曝光监测	①个人用户的客户端向媒体 web 服务器发出广告请求，	客户端信息 广告投放信息	设备 ID user agent	C-S（客户端向媒体 web 服务器）	嵌入的 js 代码或者 sdk
		②web 服务器将请求计数和必要数据通过 API 接口传递给监测服务器（异步或同步）	客户端信息 广告投放信息	设备 ID user agent	S-S（媒体 web 服务器向第三方服务器）	API 接口
	点击监测	①个人用户的客户端点击了广告投放服务器反馈的广告	客户端信息 广告投放信息	设备 ID user agent	C-S（客户端向广告投放服务器）	嵌入的 js 代码或者 sdk
		②点击代码可以多次通过 302 协议跳转传递至下一个监测服务器	客户端信息 广告投放信息	设备 ID user agent	S-S（监测服务器之间）	HTTP 协议 302 跳转
	点击后续监测	①客户端通过广告点击代码的 302 协议跳转到广告主落地页服务器	客户端信息 广告投放信息	设备 ID user agent	C-S（客户端向落地页服务器） S-S（监测服务器向落地页服务器）	HTTP 协议 302 跳转
		②广告主落地页服务器通过 API 接口将请求计数和必要数据通过 API 接口传递给监测服	客户端信息 广告投放信息	设备 ID user agent	S-S（落地页服务器向监测服务器）	API 接口

		务器（异步或同步）				
映射嵌套代码	映射	①客户端在 A 域服务器（通常是 ADX 服务器）上发出访问请求	时间 客户端信息	cookieID user agent	C-S（客户端向 A 域服务器）	
		②A 域服务器向 B 域服务器传递客户端的请求，包括 A 域服务器在客户端的 cookieID	时间 客户端信息	cookieID user agent	S-S（A 域服务器向 B 域服务器）	cookie
		③如果 B 域服务器中没有映射过这个 cookieID，则 B 域服务器通过 A 域服务器向浏览器反馈一个<img src="[A 域名]/?B=[B ID]">	时间 客户端信息	cookieID user agent	S-S（B 域服务器向 A 域服务器）	cookie
		④客户端触发 A 域下 cookie mapping 服务器	时间 客户端信息	cookieID user agent	C-S（客户端向 A 域服务器）	
		⑤A 域的 cookie mapping 服务器查找 B 域设置的 cookie mapping URL，并进行 HTTP 协议的 302 跳转至 B 域服务器，重定向到 B 域服务器携带的 A 域 cookieID	时间 客户端信息	cookieID user agent	S-S（A 域服务器 B 域服务器）	HTTP 协议 302 跳转
		⑥B 域服务器向客户端发送透明图片 1*1 像素，并种植 B 域 cookieID 给客户端	时间 客户端信息	cookieID user agent	C-S（B 域服务器向客户端）	cookie

		⑦B 域服务器上保留 B 域 cookieID 与 A 域的映射关系	时间 客户端信息	cookieID user agent	无交换	
映射-SDK	映射过程	①客户端向 APP 服务器发出访问请求	时间，多种 ID	多种 ID	C-S（客户端向 APP 服务器）	
		②APP 通过 SDK 向操作系统获得客户端设备的映射匿名 ID	时间，多种 ID	多种 ID	S-S（APP 服务器向 SDK 发行方服务器）	各种 ID 映射技术
		③APP 将映射的匿名 ID 发送至外部的数据处理者	时间，多种 ID	多种 ID	S-S（APP 服务器向数据处理者服务器）	各种 ID 映射技术
		④外部数据处理者如果没有这个匿名 ID 信息，则通过 SDK 向操作系统的查询服务器查询映射匿名 ID 的映射关系，并建立与自己域下的 ID 映射关系	时间，多种 ID	多种 ID	S-S（数据处理者服务器向 SDK 发行方服务器）	各种 ID 映射技术
		⑤外部数据处理者新的匿名 ID 映射关系表	时间，多种 ID	多种 ID	无交换	
人群包	制作标签	①DMP 服务器与数据源服务器之间映射（执行映射-嵌套代码或者映射-SDK 流程）	时间，多种 ID, 客户端信息	多种 ID	S-S（DMP 服务器向数据源服务器）	各种 ID 映射技术
		②DMP 服务器制作生成标签与映射 ID 的关系	时间，多种 ID, 客户端信息 标签信息	多种 ID	无交换	标签算法
	传递标签	③DMP 服务器与需求方服务器（可能是	时间，多种 ID,	多种 ID	S-S（DMP 向需求方服务器）	各种 ID 映射技术

		ADX、DSP、SSP 或者广告主端服务器）之间映射（执行映射-嵌套代码或者映射-SDK 流程）	客户端信息			
		④DMP 服务器将映射 ID 与标签传递给需求方服务器	时间，多种 ID，客户端信息，标签信息	多种 ID	S-S（DMP 向需求方服务器）	
人群包-RTA 接口		①ADX 或者 SSP 向买方发出 ID（目前只有大型广告主）	时间，多种 ID，客户端信息，标签信息	多种 ID	S-S（ADX 服务器或 SSP 服务器向 DSP 服务器）	API 接口
		②执行程序化竞价广告模式映射过程	时间，多种 ID，客户端信息，标签信息	多种 ID	同程序化竞价映射过程	各种 ID 映射技术
		③广告主判断 ID 是需要的，通知 DSP 服务器执行购买程序，如果不是需要的则通知 DSP 放弃竞价	时间，多种 ID，标签信息	多种 ID	S-S（广告主向 DSP 服务器）	
		④执行程序化广告竞价④-⑮				
留资		①客户端通过广告或者搜索或者直接访问到达留资页面	时间，多种 ID，客户端信	多种 ID	S-S（原访问 web 服务器向落地页服务器）	

			息， 广告投放信息			
		②个人在留资页面填写要求的信息	时间，多种 ID， 客户端信息	多种 ID	无交换	
		③写入数据库（媒体、广告主或者广告主委托的第三方）	时间，多种 ID， 客户端信息， 个人留资数据	多种 ID	C-S（客户端向某一方服务器） S-S（三方服务器之间）	

[a] C-S 行为场景：
即第一方客户端(含 PC 与手机终端的各种系统软件与应用软件)，向第一方服务端提交数据的行为过程。
该过程适用采用信息主体同意下的数据利用机制，数据许可未转移，非必要进行匿名化处理。

[b] C-T-S 行为场景：
即第一方客户端采集的数据提交给第三方插件(JS/SDK 等)，再由插件提交数据给第三方服务端的行为过程。
该过程中，数据许可在信息主体可知的前端发生转移，该第三方理应已获信息主体同意。如同意存在缺陷，该过程宜进行匿名化处理。

[c] S-S 行为场景：
即服务端与服务端进行数据交换的行为过程。
该过程中，数据许可在信息主体不可知的后端发生转移，除非第一方的提供行为已获得信息主体的单独同意，或具备其他合法性依据，该过程应进行匿名化处理。

附 录　C
（资料性）
匿名化过程举例

C.1　总体说明

某广告主委托某 DSP 在多个媒体平台进行广告投放并邀请用户试用的某次广告活动，以投放后的数据交换过程的匿名化实施为例，总体过程如表 C.1 匿名化过程概述部分的图 3 所示。

C.2　环境维护

假设该 DSP 已按本文件建设并具备了相应的技术、合规和管理环境，并已有机构或部门能够按图 C.1 匿名化实施建议流程，开展和维护三类环境。

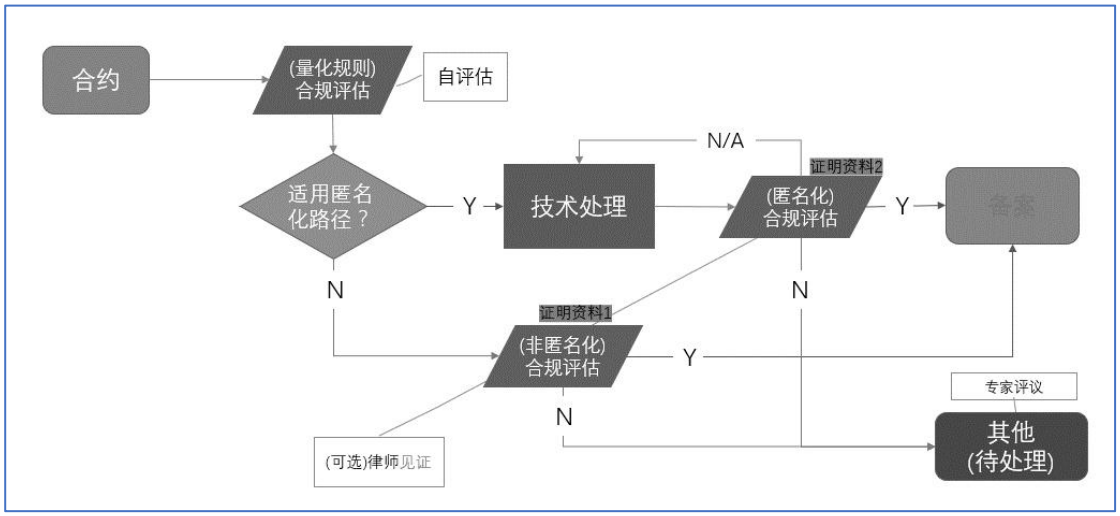

图 C.1 匿名化实施建议流程

C.3　目标确定

如图 C.2 所示，案例 DSP 的该场景的数据交换与利用过程包括：

——DSP 投放后收集受众浏览点击等行为记录，DSP 分析形成优化标签，用于广告主自有 APP 的定向再营销；
——投放中形成的用户留资信息，DSP 收集后转发给广告主，由广告主开展后续试用。

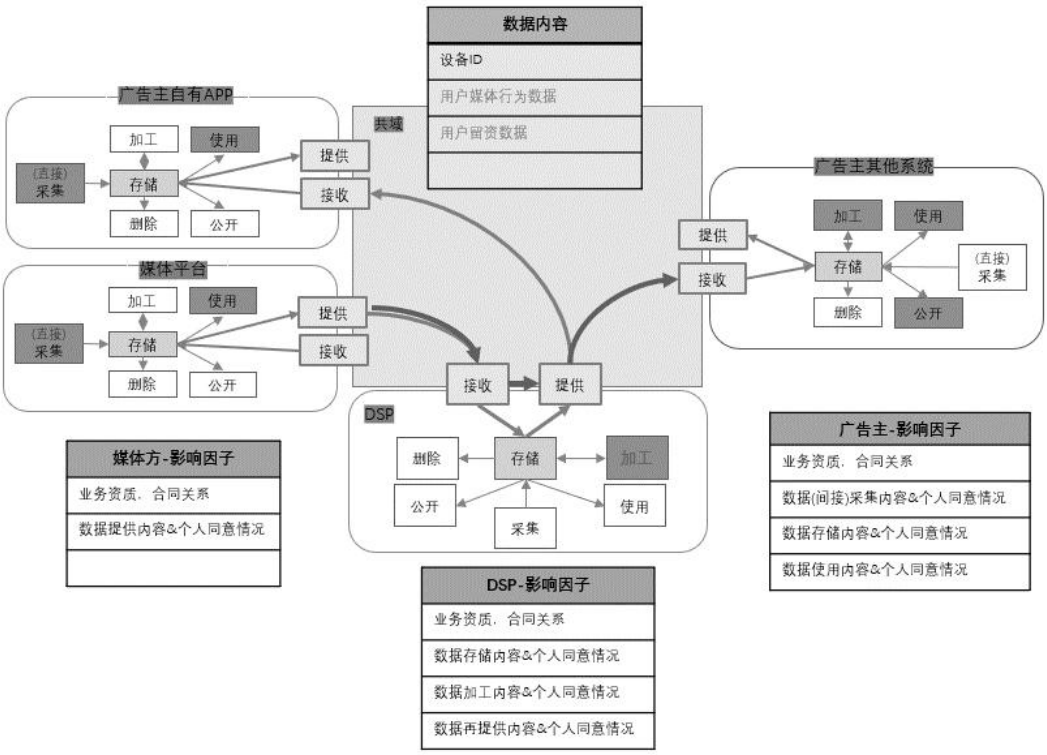

图 C.2 本案例的主体行为约束与数据交换利用过程示意

其中，与匿名化相关的关键目标包括：

——合约：DSP 与媒体的协议(或 DSP 代持广告主帐号)，DSP 与广告主的协议；

——主体：广告主、DSP、媒体平台、(暂不考虑监播活动)；

——数据：用户浏览点击记录(以某种设备号广告标识符为主键)、留资信息(以手机号为主键)；

——行为 1(对访问记录)：媒体-提供；DSP-接收/存储/加工/提供；广告主-接收/存储/使用；

——行为 2(对留资信息)：媒体-提供；DSP-接收/提供；广告主-接收/存储/使用；

——影响因子：见图 C.2 单列表部分。

针对案例中的 DSP，其匿名化实施的目标确定的过程为：

——核查合约服务涉及数据是否包含个人信息或可能导致形成个人信息，核查标准：

- 是否以个人为对象、关于个人、与个人有关；
- 是否存在各方均使用的唯一性标识符。

——核查是否具有(或需要)入域(服务器)的存储/加工/使用/提供等数据处理行为：

- 如果没有或不需，无需匿名化实施；但需注意避免(接收与提供)操作终端的存储行为，建议技术核查并清除；
- 如果具有或需要，从“主体-行为-数据”三方面，核查相对应的用户同意范围与内容情况，如有不符，则需匿名化实施，并妥善选择匿名化实施点与实施方式。

本案例中，行为记录部分，该 DSP 角色需要入域处理数据但缺失个人的同意，应匿名化。留资信息部分，DSP 仅为转发，无入域的数据处理行为，无需匿名化。

C.4 技术处理

针对需匿名化处理和无需匿名化处理的情形，其技术处理分别如下：

——针对需匿名化处理的用户浏览点击记录：

- 用适当的去标识化技术处理主键字段；
- 泛化用户浏览点击记录表中的时间字段；
- 泛化其他字段（本案例未进行处理）。

——针对无需匿名化处理的留资信息：

- 其他安全技术防范操作终端的信息泄漏和转发过程的免存储；
- 无需进行数据各种字段的去标识化和泛化操作。

——依据匿名化实施后的数据的利用是否需识别个体，选择对应的匿名化实施节点：

- 无需识别个体，私域执行，在接收至存储的节点进行技术处理。
- 需要识别个体；共域执行(第三方额外信息介入)，在接收前的节点进行技术处理，相关技术处理过程应经技术测评。

C.5 效果评估

自身或委托第三方开展合作评估及存证备案，具体包括：

- 技术测评，匿名化实施数据为对象，匿名效果的技术测评；
- 合规评估：合规评估报告及相关的见证书或法律意见书。

C.6 行为控制

针对案例中的 DSP，其数据交换过程中，主要涉及的 4 种行为及对应的行为控制要求如下：

——传输行为，即接收媒体的受众浏览与留资信息：

- 应控制数据内容与合约保持一致；
- 接收过程保持数据的匿名化，基于现实条件，DSP 匿名技术处理在接口阶段进行，以保证本方接收入库存储的匿名状态。

——提供行为，相关数据交付至广告主和广告主 app：

- 应控制数据内容与合约保持一致；
- 提供过程保持本方数据的匿名化；
- 应依据合规评估报告中对数据使用行为的分类，控制共域匿名化的关联(归因)过程：对于团标的已识别情况，评估证明广告主已有清晰同意，开放关联能力，广告主可后续定向投放；团标的可识别情况，本案例不涉及； 团标的非识别情况，无同意或依据，关闭关联能力，广告主仅可利用匿名数据开展统计分析。

——存储行为，存储接收的受众浏览信息，支持后续加工特定数据标签：

- 应控制数据内容与合约保持一致；
- 存储过程保持数据的匿名化。

——加工行为，基于接收的受众浏览信息加工特定数据标签：

- 应控制数据内容与合约保持一致；
- 加工过程保持数据的匿名化。

C.7 过程监管

整个实施过程，案例中的DSP存档、并向中立监管组织备案的材料包括：

——匿名化技术证明，由技术提供方出具；

——合规评估报告，由合规评估方出具；

——律师法律意见，由法律机构出具；

——密态关联记录，由技术提供方出具。

附 录 D
（资料性）
评估基础材料与量化方法建议

根据广告业务场景，梳理业务流程、业务对象、合作条款、数据合约，收集评估基础材料，包括且不限于表 D.1 评估基础材料信息所列，提炼和分类业务的影响因子，依据法律条款推论各种影响因子间的互斥/相容性关系，建立影响因子间关系的合规(逻辑)规则库，封装形成评估方法工具，构成合规环境并定期维护更新。

表 D.1 评估基础材料信息表

资质和证书		说明
营业证照	营业执照	扫描件
	牌照/特许经营许可证扫描件	例如；行业相关的专业牌照，例如金融类、支付类、教育类等
	ICP 增值经营许可证	扫描件
	其他证照	扫描件
数据保护证明	主体内设数据保护相关组织架构图	机构文件
	信息系统安全等级保护备案证明	扫描件
	信息安全管理体系认证证书	扫描件
	保障个人信息安全和个人信息主体合法权益的措施说明	方案说明
	数据相关的投诉和维权渠道、安全事件通知机制和应急处置机制等	方案说明
实施角色说明	提供方原生数据采集方式说明	盖章加注日期扫描件
	提供方与接收方隐私条款文件	盖章加注日期扫描件
	提供方与接收方用户协议模板文件	盖章加注日期扫描件
实施过程说明	数据传输加密技术说明文件	方案说明
	数据碰撞方式技术说明文件	方案说明
	数据交集识别检查说明文件	例如：可信流通服务平台协议等
授权相关补充说明	个人信息主体授权同意相关证明	例如：同意页面、工作流程、同意行为的记录（如日志）以及告知内容
	个体认证方式相关证明	客户界面截图/照片、业务协议（扫描件）、技术接口、平台服务记录等证明材料
	授权审计模式说明文件	审计报告

参 考 文 献

[1] GB/T 25069-2010 信息安全技术 术语

[2] GB/Z 28828-2012 信息安全技术 公共及商用服务信息系统个人信息保护指南

[3] GB/T 35273-2020 信息安全技术 个人信息安全规范

[4] GB/T 37932-2019 信息安全技术 数据交易服务安全要求

[5] GB/T 37964-2019 信息安全技术 个人信息去标识化指南

[6] GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南

[7]《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第 24 号令公布)

[8]《信息安全技术 个人信息告知同意指南》(国家标准 GB/T 征求意见稿)

[9]《中华人民共和国数据安全法》

[10]《中华人民共和国个人信息保护法》