目　次

前　　言

本文件按照GB/T1.1——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。

本文件是T/SHAA0002《数字广告》的第5部分。

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。

本文件由上海市广告协会提出并组织实施。

本文件由上海市广告协会归口。

本文件起草单位：上海市广告协会、上海广告研究院、上海大学、利欧集团数字科技有限公司、上海新分众广告传播有限公司、互诚信息技术（上海）有限公司。

本文件主要起草人：孔秀祥、周崧弢、陈岩。

本文件首批承诺执行单位：

1.承诺执行企业：上海美术设计有限公司、分众传媒信息技术股份有限公司、先恩环境艺术发展集团有限公司、互诚信息技术（上海）有限公司、上海广播电视台、上海广告有限公司、德高广告（上海）有限公司、上海唐神广告传播有限公司、东方航空传媒股份有限公司、上海飞帆广告有限公司、上海铁路文化广告发展有限公司、凤凰卫视都市传媒（上海）有限公司、携程旅游信息技术（上海）有限公司、上海雅仕维广告有限公司、上海映巷文化传播有限公司、上海亚通文化传播有限公司、中广国际广告创意产业基地发展有限公司、利欧集团数字科技有限公司、上海不只广告有限公司、上海企创信息科技有限公司、上海辰源企业形象设计有限公司、上海惠亨智能科技有限公司、上海剧星传媒股份有限公司。

2.承诺执行团体：上海市广告协会展览陈列分会、上海市广告协会品牌服务分会、上海市广告协会互联网分会、上海市广告协会交通分会、上海市广告协会融媒体分会、上海市广告协会户外分会、上海市广告协会招牌标识分会、上海市广告协会摄影分会、上海市广告协会生态专业委员会、上海市广告协会园区专业委员会、上海市广告协会学术法律专业委员会

引　言

数字广告经过近20年的发展，不断开挖互联网技术的潜力、拓宽大数据技术的应用场景、结合人工智能技术并予以发展。数字广告是对商业价值深入挖掘而发展起来的新兴营销传播模式，通过对数据的密集使用，频繁使用数据收集、加工、交换、建模等手段来发挥数据对广告效益的提升。特别是近年来广告行业引入机器学习算法和神经网络算法，并日益加强这些算法的应用权重，不断拓宽其应用场景。数据已经成为广告行业的重要基础资源，数据技术的应用和探索成为了广告行业的核心竞争力之一、引发广告企业的积极尝试并引发一定的投资热潮。

数字广告领域对数据收集、加工、交换和应用的供需两旺，数据相关的新理论、新技术和新应用层出不穷，处于一种不断探索、不但突破的欣欣向荣的态势。在一派繁荣的背后，也有隐忧，在跑马圈地粗放式成长之际，国家为了规范数字营销的乱象，出台了一系列政策法规，给出了不能触碰的高压线，并同时努力突破阻碍数据资源有效利用的垄断性屏障。乱象沉底套上合法性马甲继续做一些灰色的业务，法规也绑住了部分企业的手脚。如何在法律法规下，高效有序地开发数据资源的价值，给广告赋能？

为了更精准地消除数字广告领域数据应用中的灰色地带，把牢数据安全的大门，高效有序开发数据潜能，需要制定一套完整的面向数字广告的数据应用与安全的规范和标准。这样的规范与标准能够帮助解决广告主、媒体、用户、代理商、第三方监测机构之间在数据的收集、加工、交换和使用中出现的矛盾与错位，以期解决行业内存在的数据一致性、操作规范性、商业数据安全性、个人信息保护等方面的问题。

数字广告的数据应用与安全标准，围绕数字广告行业的数据收集、使用、存储、传输和删除等行为，在法律规章许可的先决前提条件下，既守住安全合规的底线，又充分满足市场日益增长的需求，把握好两者的平衡，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，由上海市广告协会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，向上海市广告协会反映。

第5部分：数据应用和安全

1 范围

本文件规定了数字广告相关的数据应用和安全的规范与要求，界定了数据应用的范围与场景，对数据应用的合法合规与应用效率的平衡制定了相应的规范性要求。

本文件适用于所有参与数据广告业务的公司与机构，包括广告主、广告媒体和流量平台、用户、广告代理公司、广告技术公司、广告监测公司、广告数据技术服务公司和其他第三方组织（如专业化的MCN机构、数字广告软件服务商、虚拟数字人制作公司、AI广告公司）等，规范在数字广告活动策划创意与计划的准备期间、媒体购买投放与反馈评估的执行期间以及活动结束后的总结分析期间，涉及到的数字广告相关的数据收集、应用、交换、存储、传输、验证和删除等活动，也适用在其他领域开展的相关活动。

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。其中标注日期的引用文件，仅该日期对应的版本适用于本文件；不标注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 34090.2 互动广告第2部分：投放验证要求

GB/T 35273-2020 信息安全技术个人信息安全规范

GB/T 37964-2019 信息安全规范 个人信息去标识化指南

T/CAAAD 001-2021，T/CCSA 329-2021 互联网广告数据应用和安全技术要求

T/CAAD 002-2020 中国互联网广告投放监测及验证要求

T/CAAAD 003-2020 移动互联网广告标识技术规范

T/CANA 001-2020 电子商务数权评价标准

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1 一手数据 primary data

称为原始数据，是指通过用户许可获得的用户网络访问行为、网络交流、交易行为等数据，通过监测获得的广告相关的数据等。

3.1.2 二手数据 secondary data

由其他机构收集、整理出来的数据，通过查找或购买等方式获取。二手数据可分为第一方数据、第二方数据、第三方数据。

3.1.3 第一方数据 first party data

是指企业直接从受众(包括客户、网站访问者和社交媒体关注者）那里收集的数据。

3.1.4 第二方数据 second party data

来自于其他源的第一方数据。

3.1.5 第三方数据 third party data

来自于其他源的非第一方数据。数源提供方不一定是数据的原始采集者，可能是多方数据的聚合者。

3.1.6 敏感数据 Sensitive Data

可直接识别特定用户，是与具体用户之间有特定相关性的数据。

3.1.7 脱敏数据 masked data

去标识，匿名化之后获得的数据。

3.1.8 数据脱敏 data masking

又称数据漂白、数据去隐私化或数据变形。指对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。

3.1.9 重要数据 Critical Data

可从中得知产品商业价值，企业经营秘密等，是需谨慎使用的用户或客户相关数据、产品核心数据等。

3.1.10 一般数据 General data

支撑业务逻辑及运行的数据，通过统计、分级、加工等处理不会对用户或公司利益产生影响。

3.1.11 直接标识符 direct identifier

可在特定环境下单独识别个人信息主体。姓名、身份证号码、护照号等就是直接标识符。

3.1.12 准标识符 quasi-identifier

需要结合其他属性才能识别到具体个人，比如性别、出生日期或年龄、职业、婚姻状况等。

3.1.13 匿名化 Anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别，且处理后的信息不能被复原的过程。匿名化处理后所得的信息不属于个人信息。

3.1.14 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，无法识别个人信息主体的过程。去标识化的信息还保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代个人信息标识。

3.1.15 广告标识符或 ID identifier for advertising

可理解为广告标识符，在同一个设备上的所有App都会取到相同的值，是苹果专门给各广告提供商用来追踪用户而设的。广告标示符是由系统存储着的。适用于对外：例如广告推广，换量等跨应用的用户追踪等。

3.1.16 程序化购买 programmatic buying

基于自动化系统（技术）和数据来进行的广告投放。该方式支持根据广告主定义的期望受众，系统帮其找出优选的媒体来购买受众，为广告主提出最优媒介采买计划，运用计算机软件进行自动化购买的方式执行，并按照期望的周期反馈监测结果，并对后续投放进行优化。

3.1.17 需求方平台 demand side platform

帮助广告主执行广告投放策略的平台，可设定投放金额、单价、数量、物料等执行策略。

3.1.18 供给方平台 supply side platform

帮助媒体进行广告资源销售的平台，记录了媒体销售的广告位、物料尺寸、售卖金额、库存等信息。

3.1.19 数据管理平台 data management platform

整合各方数据并提供数据分析、数据管理、数据调用等，通过数据调用向需求方平台、供给方平台、广告主和媒体提供数据服务的平台。

3.1.20 广告交易市场 advertising exchange

联系广告主和媒体，或者需求方平台和供给方平台，组织竞价、撮合交易的市场平台。

3.1.21 用户画像 user profiling

通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如职业、经济、健康、教育、个人喜好、信用、行为等方面作出分析或预测，形成其个人特征模型的行为。

3.1.22 数据安全事件 data security event

有关数据处理时出现的规模性异常，即为数据安全事件。包括但不限于：数据泄漏、数据泄密、数据篡改、数据丢失、黑客攻击、人为破坏、软硬件灾难性事故等。

3.2 缩略语

下列缩略语适用于本文件。

ADX Advertising Exchange广告交易市场
CTR Click Through Rate点击率
DMP Data Management Platform数据管理平台
DSP Demand Side Platform需求方平台
IDFA Identifier For Advertising广告标识符
IVT Invalid Traffic无效流量
RTB RealTime Bidding实时竞价
SSP Supply Side Platform供给方平台
TD Trading Desk交易桌面

4 数据应用原则

数字广告数据的应用原则包括但不限于：

4.1 合法性原则

数字广告数据应用的参与方应严格按照法律法规的要求开展数据收集、应用、交换、存储、传输、验证和删除等活动；

4.2 完整可用原则

数字广告数据应用的参与方应保证数据使用、交换、存储、传输活动中的数据完整性和可用性；

4.3 数据等级分类及授权管理原则

数字广告业务中产生或应用的数据应该划分为敏感数据、重要数据和一般数据等类别，并进行分别授权管理，在数据使用、交换、存储、传输活动中，确保各类数据有足够的安全性和保密性；

4.4 透明可验证原则

数字广告数据应用的参与方在开展数据使用和交换活动的过程中，应当记录数据使用和交换情况，实现可查看与可追溯，以验证合规性和安全性。

4.5 最小数据原则

该原则要求数据控制者收集、使用的个人数据类型、范围、期间对于数字广告活动应当是适当的、相关的和必要的。最明确的“用户同意”、最少化的信息要素采集、最安全的存储和传输。在数字广告活动中很少或基本不再使用的数据要进行删除、封存或脱敏处理，提高访问权限。

4.6 伦理原则

数字广告数据应用的参与方在开展收集、应用、交换、存储、传输、验证和删除等活动时要尊重数据所有权，保护数据相关人的个人隐私，做好无害化处理。

4.7 公平原则

数字广告数据应用的参与方在开展收集、应用、交换、存储、传输、验证和删除等活动时，避免制造数字鸿沟，编织信息茧房，大数据杀熟和自我优待等有失公平的行为。在数据的使用和处理中要落实“告知—同意”原则。

4.8 效率原则

数字广告数据应用的参与方在收集数据采用非必要不使用的最小化原则，交换与传输时优先采用统一接口与标准。在深入数据挖掘时，要强调“有限、适度”原则

5 数据应用环节与应用场景的安全要求规范

5.1 应用环节规范

5.1.1 总体要求

数据使用方应当遵守以下总体要求：

遵守《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》，坚持将最小化原则应用于数据采集、存储、传输、处理、使用、共享开放、删除的全部流程。存储数据要做脱敏处理，尽量使用协会推荐的广告标识来分享、传输与交换数据。做好数据事故的预案，实施谁泄密谁负责原则。本节的数据处理安全主要关涉个人信息数据和非个人信息数据在使用过程中的安全保障。

a）处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理；

b）用于处理信息系统中的数据以赋能数字广告的系统，应当遵守数据分等级保护的要求对数据传播、处理、交换和存储等环节进行安全保护。

5.1.2 数据收集

数据收集可分为一手数据收集，二手数据收集。一手数据收集，即原始数据的收集，数字广告业中多指广告主营销活动中收集到的客户或潜在客户的数据。原始数据中可能包含有较多与隐私相关的信息。原始数据收集应让用户知情并取得用户许可，用户对数据还必需有退出与取消权保障。

二手数据通过交易或交换等手段合法获得。数字广告业的数据交易应遵循只交易价值，不交易原始数据的原则。数据拥有者和使用者要围绕数据的全生命周期做好安全防护，有效控制流转过程带来的风险。

数据接收方收集数据，具体要求包括：

a） 数据接收方收集数据，不应：

1） 从非法渠道获取数据；

2） 通过误导、欺诈、胁迫等非法方式获取数据；

3） 隐瞒产品或服务所具有的获取数据的真实功能；

4） 获取法律法规明令禁止获取的数据；

5） 以其他违反法律法规的方式收集数据。

b） 一手数据接收方直接向用户收集数据，应当：

1） 直接向用户收集数据时，应当遵循合法、正当、必要和诚信的原则收集数据。如涉及收集个人信息，应向用户告知收集个人信息用于数字广告服务的目的、方式和范围，并获得用户同意。此外，应符合 GB/T35273 第 5 章的要求规范数据收集行为；

2） 可与用户直接交互的数据接收方，如媒体、终端设备等，宜以简洁清晰、通俗易懂的方式（可包含文字和图示）告知关键内容，同时提供完整版告知内容的链接；

3） 不具备直接告知渠道的，应在媒体、终端设备的告知文本中披露个人信息收集处理的详细情况，并以简单直观的方式向用户提供“退出”或“关闭”选项。披露相关说明的媒体和终端设备应予以配合，并且宜在信息收集者的官方渠道（网站、公众账号等）告知收集、使用个人信息的情况，并提供退出、删除机制。

c） 二手数据接收方间接从其他数据提供方处获取数据，应当：

1） 间接收集数据时，数据接收方应通过合法、正当的途径，采用合法、正当、必要的方式收集数据。如涉及间接收集个人信息，应要求数据提供方出示个人信息来源合法合规性的证明并进行确认，且数据接收方应了解数据提供方已获得的个人信息处理的单独同意的范围，包括授权使用的目的、方式、范围以及用户是否授权同意进一步转让、共享、公开披露等；

2） 开展业务所需进行的个人信息处理活动超出提供方已获得的同意范围的，应重新征得用户同意；

3） 数据接收方应对数据或个人信息的来源、共享、转让、公开批露、安全保障措施等情况通过官方渠道在隐私政策等文本中向用户进行告知。

4） 发送方需要确认接收方的使用范围，防止接收方超限使用。提倡遵从只交易价值，不交易原始数据的原则。

5.1.3 数据使用

数据使用方，包括数据收集者、数据提供方，使用数据，包括但不限于加密存储、处理、运算、映射、标签分类、定向等方式，具体要求包括：

a）针对定向、重定向和程序化创意等方式的广告技术所使用的受众标识的限制：应优先使用符合T/CAAAD003-2020标准要求的广告标识符；

b） 使用目的限制：

1） 不应超出与数据提供方的约定范围使用数据，或违反约定将数据提供给其他数据接收方；

2） 如涉及使用个人信息，还不应超出与收集或获取个人信息时所声称或约定的目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得用户授权同意。

c） 数据使用完整性要求：

1） 数据使用方应具备完善的数据等级分类及授权管理制度与管理策略，支持权限最小化原则、合理授权数据使用的权限范围；

2） 数据使用过程中，数据使用方应具备完整的用户信息访问、处理、删除等操作的记录，以备数据审计；

3） 数据使用的整个过程中，数据使用方应保证使用操作合理合法，不得滥用、篡改、非法出售和故意毁损数据。

d） 数据使用安全保密要求：

1） 应对数据进行分类并根据类别需要采取适合的保密、脱敏等处理措施，保障敏感数据的使用安全；

2） 应对数据严格保密，建立健全数据保护制度，综合使用各类技术手段保护数据使用安全，如权限管控、访问认证/鉴权、隔离、审计、加密、脱敏等；

3） 用于数据保密应采用行业通用加密方式，应符合国家密码管理相关要求。

5.1.4 数据存储

a） 数据存储应设置加密、备份与恢复机制。应采用加密技术或去标识化技术在数据存储过程中隐藏敏感数据。

b） 数据存储应采取安全措施，及时进行备份，在数据遭遇入侵或者硬件损坏等不可抗力被损坏后，在符合一定条件时可及时恢复；

c） 数据存储应设计数据的完整性检测方案以对数据进行完整性检测，保证数据的真实性和完整性，不得篡改和伪造数据，尤其是敏感数据；

d） 存储时间最小化要求

1） 数据存储期限应为实现数据主体授权使用的目的所必需的最短时间，法律法规另有规定或者数据主体另行授权同意的除外；

2） 超出上述存储期限后，应对数据进行删除或匿名化处理。

5.1.5 数据访问

数据应采取完整有效的访问控制策略，确保无权访问存储数据的个人或其他组织，不可访问或者通过其他间接手段访问存储的数据。

a）供相应的身份认证和访问控制机制，确保只有合法的用户或应用程序才能发起数据处理请求；
b）用认证系统和机制，进行权限设置、认证以及审计；
c）用符合国家密码管理相关要求的密码技术保证数据存储的保密性，包括但不限于鉴别数据、业务数据和个人信息等；

5.1.6 数据传输与交换

数据提供方和数据接收方之间传输数据，具体要求包括：

a） 数据提供方和数据接收方之间应以合法合规、正当的目的和方式传输数据；
b） 数据传输应优先使用符合T/CAAAD003-2020标准要求的广告标识符；
c） 传输与交换数据的双方在数字广告环境下，基本通过嵌入或接入自动化工具（如程序、脚本、接口、软件开发工具包等）进行数据传输：
d）传输与交换数据的双方应通过合同等形式明确双方的安全责任、应实施的数据安全措施及双方法律义务与责任；在自动化工具处理数据的方式、目的、期限等发生重大变更时，如原合同没有条款说明，应对合同进行更新或签订补充协议等，应妥善留存传输与交换的合同和管理记录，确保可供相关方查阅；
e）传输与交换数据的双方应优先采用标准所推荐的传输方式和控制机制。由数据提供方建立接入自动化工具提供数据的管理机制和工作流程，必要时应建立评估机制，设置接入条件，并对接入的自动化工具进行尽职调查和个人信息保护影响评估。数据接收方不应强迫任何单位或组织嵌入或接入可获取数据的自动化收集工具(如代码、脚本、接口、算法模型、软件开发工具包等）；
f）数据提供方应当：
1）在向数据接收方提供个人信息前进行个人信息保护影响评估，并进行记录，应要求数据接收方建立响应用户请求、申诉等的机制，并妥善留存、及时更新，以供用户查询、使用；
2）应向用户说明接入自动化工具的情况并明示该自动化工具由第三方提供，涉及收集处理个人信息的，应向用户告知数据接收方通过自动化工具收集处理个人信息的详细情况，并获得用户单独同意；
3）应督促和监督数据接收方加强数据安全管理，发现第三方产品或服务没有落实安全管理要求和责任的，应及时通知该数据接收方，督促整改，必要时停止接入；
4）宜开展技术检测，审查该自动化工具是否存在漏洞，确保其数据收集、使用行为符合约定要求。
e） 完整可用要求
1） 数据传输过程中应对数据提供完整性校验；
2）数据传输与交换的双方应具备检测相关网络数字设备在数据传输过程中完整性受到破坏的能力，并具备恢复数据完整性的能力；
3）数据传输渠道和方式应合法合规，传输的数据如果涉及个人信息或个人敏感信息，应确保征得用户单独同意或符合法律法规规定的正当法律事由，并应告知传输敏感个人信息的必要信息以及对其权益的影响；
4） 在传输过程中，应保证数据经过处理仍具有可用性。
f） 安全保密要求
1） 传输过程中应进行身份鉴别，确保交易双方身份真实可信、不可抵赖。在通过网络传输用户个人信息数据时，宜使用安全协议，如 https；
2） 在对数据信息进行传输时，应在风险评估的基础上，采用符合国家密码管理相关要

求的加密技术对数据进行加密传输，宜根据风险评估确定保护要求，并确定加密算法的类型、属性，以及所用密钥的长度；

3） 根据数据的保密要求，在传输过程中宜使用数字签名、消息验证码等技术，以确保信息的不可否认性和完整性。使用数字签名时应符合国家政策关于数字签名的技术要求。

g） 数据提供方宜对数据接收方收集处理数据的行为进行审计，发现超出约定行为，应及时通知该数据接收方，督促整改，必要时停止接入；

h） 在数据传输过程中，应有完整的数据处理的相关记录，用于数据验证和核查。

5.1.7 数据删除

数据使用方使用数据，具体要求包括：

a） 数据使用目的达成后，应对数据进行删除或匿名化处理；

b） 涉及个人信息，符合以下情形，个人信息主体要求删除的，应及时删除个人信息：

1） 数据使用方违反法律法规规定，收集、使用个人信息的；

2） 数据使用方违反与个人信息主体的约定，收集、使用个人信息的。

c） 数据使用方违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息，且个人信息主体要求删除的，数据使用方应立即停止共享、转让的行为，并通知第三方及时删除；

d） 数据使用方 违反法律法规规定或违反与个人信息主体的约定，公开披露个人信息，且个人信息主体要求删除的，数据使用方应立即停止公开披露的行为，并发布通知要求相关接收方删除相应的信息。

5.2 应用场景安全要求

5.2.1 场景描述

有关数字广告数据应用场景，包括但不限于程序化广告购买、广告监测、广告效果评估、异常流量排查和反作弊、用户画像、数据汇聚融合、委托处理等。

5.2.2 程序化购买

程序化购买场景中数据安全要求如下：

a）接入程序化购买平台的各方，首先应签订数据安全协议，明确各方的数据安全责任和义务；

b） 程序化购买活动期间：

1）供给方平台(SSP）和广告交易市场（ADX）应对信息收集过程向用户进行充分披露，并保存相应的证据。广告投放服务（Ad Serving）和需求方平台（DSP）可要求供给方平台（SSP）和广告交易市场（ADX）提供相应的授权证明；

2）数据提供方应优先使用符合 T/CAAAD003-2020 标准要求的广告标识符，遵循最小数据原则，只传递已授权的最小必要用户信息，不能泄漏用户的固定唯一标识符；

3）参与各方可使用分布式记账方式等手段签注数字签名、唯一时间戳等多种不可更改的标记以确保交易关键信息不被篡改；

4）各方产生的交易记录应安全保存，以备审计；

c） 程序化购买过程结束，各方均应遵照数据安全协议约定执行相应数据安全程序。

d） 程序化创意：遵守公序良俗，避免庸俗。避免引起广告用户的负面情绪。

e） 程序化广告投放内容数据合法合规性，由DSP审核素材、SSP和ADX审核全稿，实行多级管理，全流程监管。应该设置内容安全应急程序和处置联系方式。

5.2.3 广告监测

广告监测场景中数据安全要求如下：

a） 如果媒体/广告主植入监测公司的SDK，监测公司应将SDK收集数据所需要的权限告知媒体/广告主，并取得媒体/广告主授权同意；

b） 媒体/广告主应在隐私政策中预先将广告监测可能索要的权限向用户进行告知，并取得用户授权同意；

c） 媒体、广告主应在隐私政策中将广告监测需要收集的数据，以及收集数据的目的、方式、范围向用户进行告知，并取得用户授权同意；如果媒体/广告主使用监测SDK的，还应将监测SDK名称向用户告知；

d）监测方应当在其隐私政策中明确告知用户可撤回收集、使用其个人信息同意授权的方法。若用户撤回同意后，监测公司后续不得再处理相应的个人信息；撤回同意不影响撤回前基于同意的个人信息处理；

e） 监测公司不得收集与提供广告投放监测服务无关的个人信息，符合本条要求收集的数据类型和用途；

f） 监测公司的数据收集、存储、处理、计算系统应满足以下要求：

1） 广告监测数据应以数据传输原始格式分别在媒体平台及监测公司系统中至少保存 2 年，法律、行政法规另有规定的，从其规定；

2） 若广告主、媒体或相关方应个人信息主体请求，要求监测公司删除原始监测数据，应出示个人信息主体要求删除个人信息的证明；注：根据 GB/T35273 的定义，此处“删除”是指在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

3） 监测公司应在媒体配合下，遵循数据安全要求对数据进行收集，应保证数据准确、完整地传输、存储、处理、计算。避免因监测数据信息不准确、不完整对企业或相关利益方的权益造成不利影响。

5.2.4 广告效果评估

广告效果评估场景，收集和处理数据应尽量避免涉及个人信息，优先使用人群化的广告标签。其数据安要求如下：

a） 收集数据：

1）埋点数据收集广告投放数据与广告互动数据，涉及个人信息的，效果评估机构或媒体方在信息收集前应向个人信息主体明示信息收集的类型及用途，并应获得个人信息主体授权同意后方可进行；

2）采用监测渠道收集到的数据进行效果评估的，应是对个人信息进行脱敏后的数据，或者应有个人信息主体为数据用于效果评估使用的授权同意证明：

b） 数据处理与分析包含数据存储、数据传输及数据计算等应用，效果评估机构与数据处理方应该遵循数据等级分类及授权管理原则，建立相应的审批与数据安全管理机制，宜预先采用加密技术或去标识化技术对数据进行脱敏处理，防止用户信息泄露及随意扩大商业用途；

c） 效果评估报告的数据应以细粒度数据聚合方法呈现给广告主。

d） 处理广告效果数据应当保证数据的质量，避免因数据不准确、不完整对相关企业或个人权益造成不利影响。

5.2.5 异常流量排查和反作弊

异常流量排查和反作弊场景中数据安全要求如下：

a） 异常流量的识别：异常流量的原始数据均应保留至少2年，应标记出无效流量，以备复核时作为判定依据。

b） 异常流量的复核：复核异常流量，监测机构、媒体、广告主三方应提取异常流量数据样本或全部流量数据进行复核，样本提取应遵守最少够用的原则，各方对所涉及的数据和判定依据负有保密义务。

c） 异常流量特征的提炼：鼓励通过分析异常流量以完善反作弊算法。新的反作弊算法和规则不宜公布，应实施分级严格保护，设置严格的权限机制。

d） 鼓励制作、管理和使用行业公共异常流量库所定义的数据。行业协会组织成员企业可制作本企业使用的异常流量定义名单数据，允许成员企业使用移动设备和智能电视等用于广告用途的识别标识的原始数据值，该原始数据值可加密或未加密，以满足甄别无效流量的目的。数据提供、加工、使用的各方应本着最小化的使用场景原则使用数据，并限制上述数据仅在本企业范围内使用。

5.2.6 用户画像

用户画像场景中数据安全要求如下：

a） 用户画像中对用户的特征描述，应符合公序良俗，不应包含：淫秽、色情、赌博、迷信、恐怖、暴力的内容以及表达对民族、种族、宗教、残疾、疾病歧视的内容；

b） 在业务运营或对外业务合作中使用用户画像的，应合法合规，满足以下要求：

1）应避免侵害公民、法人和其他组织的合法权益；

2）个人信息匿名化，应消除明确身份指向性，避免精确定位到特定个人；

3）应结合用户画像所用于的目的，采取有效的数据保护措施；

4）在业务运营或对外业务合作中使用用户画像的，应事前进行个人信息保护影响评估，业务出现重大调整时，应重新进行评估，对评估报告和处理情况应予记录，并至少保存三年。

c） 用于广告目的的用户特征组合应消除明确身份指向性，降低重新被标识的风险，避免精确定位到特定个人，保证特征组合所限定的用户数量不少于规模下限，规模下限应当不少于特征组中最多特征值的50倍。

5.2.7 数据的汇聚融合

数据的汇聚融合场景中数据安全要求如下：

a） 数据使用方，如DSP、监测机构、效果评估机构等，在遵循合法合规和正当必要原则的前提下，可汇聚融合基于不同业务场景所收集来的数据并加以使用；

b） 汇聚融合的数据如涉及个人信息，应满足以下要求：

1） 汇聚融合的数据应不包含具有指向性的个人信息数据；

2） 在与用户或数据提供方之间明确约定的目的与范围内使用、交换与交易数据；

3） 汇聚融合后要开展个人信息合规影响评估，采取有效的个人信息保护措施。

5.2.8 委托处理数据

委托处理数据场景中数据安全要求如下：

a） 委托方在委托之前，应当进行信息保护的影响评估，并记录评估报告及处理情况，记录至少保存三年；

b） 受委托方应严格按照委托方的要求处理数据，不得超出约定的处理目的、处理方式等处理数据。受委托方因特殊原因未按委托方的要求处理个人信息的，应及时向委托方报告；
c） 委托方应对受委托者进行监督，方式包括但不限于：通过合同等方式规定受委托者的责任和义务；对受委托者的处理过程和处理结果等进行审计；
d） 委托方应准确记录和保存委托处理数据的情况；
e） 委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得备份，不得保留。
f） 委托方得知或者发现受托方未按照委托要求处理数据，或未能有效履行数据安全保护责任的，应立即要求受托方停止相关行为，且采取或要求受托方采取有效补救措施（如更改口令、回收权限、断开网络连接等）控制或消除数据面临的安全风险。必要时委托方应终止与受托方的业务关系，并要求受托方及时删除从委托方获得的数据；
g） 如涉及个人信息的，委托方应与受托方约定委托处理的目的、方式、个人信息种类、保护措施、双方权利义务等，并对委托方的个人信息处理活动进行监督，受托方应当协助委托方响应用户提出的相关请求；受托方在处理个人信息过程中无法提供足够的安全保护水平或者发生了安全事件的，应及时向委托方报告；
h） 未经委托方同意和用户单独告知同意，受托方不应转委托他人处理数据；
i） 宜在委托方平台进行的委托处理，非在委托方平台进行的委托处理，应满足本文件5.1.5数据传输环节规范，宜预先采用加密技术或去标识化技术使得数据对被委托方为匿名。

5.2.9 安全事件处置

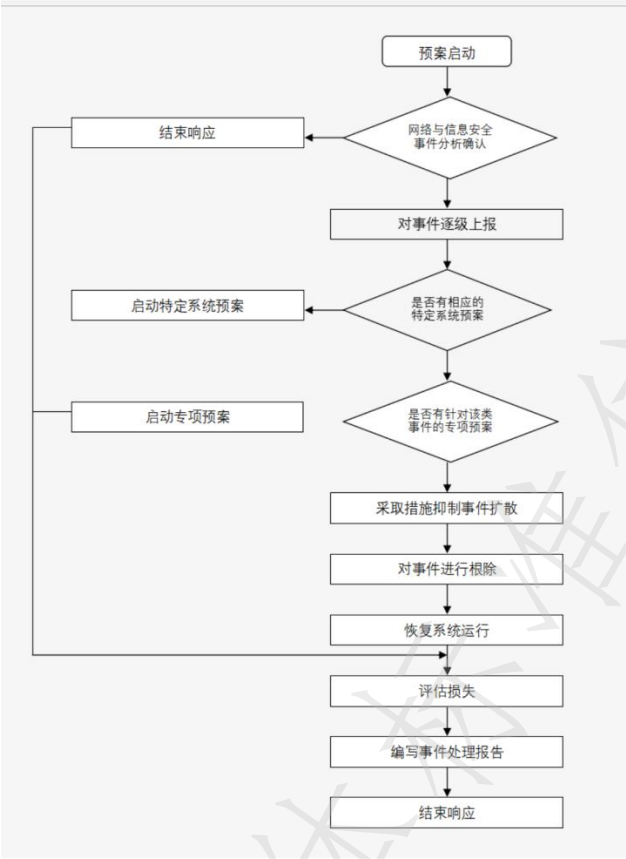
安全事件处置场景中数据安全要求如下：

参与方应具备安全事件处置能力，具体包括：

a） 应制定数据安全事件应急预案；
b） 应定期(至少每年一次）组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责和应急处置策略和规程；
c） 发生数据安全事件后，数据使用和传输主体应根据应急响应预案进行以下处置：
   1） 记录事件内容，包括但不限于：发现事件的人员、时间、地点，涉及的数据及规模，发生事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门；
   2） 评估事件可能造成的影响，并采取必要措施控制事态，消除隐患；
   3） 按照有关规定及时上报，报告内容包括但不限于：涉及用户的类型、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式；
   4） 当法律法规变化或事件处置情况有变化时，应及时更新应急预案。
d） 安全事件告知除采取措施能够有效避免信息泄露、篡改、丢失造成危害的以外，发生或者可能发生个人信息泄露、篡改、丢失的，应当立即采取补救措施，并通知履行数据或个人信息保护职责的部门和个人：
   1） 应及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的用户。难以逐一告知用户时，应采取合理、有效的方式发布与公众有关的警示信息；
   2） 告知内容应包括但不限于：安全事件的内容和影响；已采取或将要采取的处置措施；用户自主防范和降低风险的建议；针对用户提供的补救措施；数据处理者的联系方式。

附录 A

A.1 数据安全事件应急响应流程图



A.2 应用数据交换接口定义

（该部分参照T/CAAAD 001-2021，T/CCSA 329-2021互联网广告数据应用和安全技术要求6 数字广告应用数据交换接口定义）

参 考 文 献

[1]《中华人民共和国网络安全法》（自2017年6月1日起施行）
[2]《中华人民共和国数据安全法》（2021年9月1日起施行）
[3]《中华人民共和国个人信息保护法》（2021年11月1日起施行）
[4]《中华人民共和国广告法》（2021年4月29日全国人民代表大会常务委员会第二次修订）
[5]《互联网广告管理暂行办法》（2016 年 9 月 1 日起施行）
[6]《网络交易监督管理办法》(国家市场监督管理总局2021年3月15日发布，自2021年5月1日起施行)
[7]《电信和互联网用户个人信息保护规定》（工业和信息化部，2013年9月1日起施行）
[8]《互联网广告管理暂行办法》（国家工商行政管理总局，2016年9月1日起施行）
[9]《国家网络安全事件应急预案》（国家互联网信息办公室，2017年1月10日起施行）
[10]《App违法违规收集使用个人信息行为认定方法》（国家互联网信息办公室、工业和信息化部、公安部、市场监管总局联合制定，2019年11月28日施行）
[11]《数据安全管理办法（征求意见稿）》（国家互联网信息办公室，2019年5月28日发布）
[12]《网络数据安全管理条例（征求意见稿）》（国家互联网信息办公室，2021年11月14日发布）
[13]《中国互动网络广告行业自律守则》（中国广告协会互动网络委员会制定，2007年6月13日起施行）
[14]《上海市数据条例》上海市人大常务委员会于2021年11月25日通过，2022年1月1日旅行。
[15]GB/T 34090.2 互动广告第2部分：投放验证要求
[16]GB/T 35273-2020 信息安全技术个人信息安全规范
[17]GB/T 37964-2019 信息安全技术 个人信息去标识化指南
[18]DB33/T 2178-2019 广告经营单位业务管理规范
[19]DB33/T 2179-2019 互联网广告标注与传输技术规范
[20]T/CAAAD 003-2020 移动互联网广告标识技术规范
[21]T/CAAAD 002-2020 中国互联网广告投放监测及验证要求
[22]T/CAAAD 003-2020 移动互联网广告标识技术规范
[23]T/CAAAD 001-2021，T/CCSA 329-2021 互联网广告数据应用和安全技术要求
[24]T/CAAD 002-2020 中国互联网广告投放监测及验证要求
[25]T/CAAAD 003-2020 移动互联网广告标识技术规范
[26]T/CANA 001-2020 电子商务数权评价标准
[27]OpenRTB Dynamic Native Ads API Specification（https://www.iab.com/wp-content/uploads/2016/03/OpenRTB-API-Specification-Version-2-5-FINAL.pdf?fbclid=IwAR2_Q65gOz4wKs3hh1tSi_vmC9YeOOkxRrgbBx5S94ZxjGl7HHfsTIs08-c）。
[28]Openrtb3.0
（https://github.com/InteractiveAdvertisingBureau/openrtb/blob/047a177d5f284a85c3b9ddb7efffd8c8697c7c2e/OpenRTB%20v3.0%20FINAL.md）