ICS 03 100 20号
A10

团　　体　　标　　准

T/ CAB 0101—2021

市场研究 个人信息安全保护要求

Marketing Research—personal Information Security Protection Requirements

2021-04-01 发布　　2021-04-01 实施

中 国 产 学 研 合 作 促 进 会 发 布

目　次

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

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这些专利的责任。

本标准由中国信息协会市场研究业分会提出。

本标准由中国信息协会市场研究业分会归口。

本标准起草单位：北京零点有数数据科技股份有限公司、立信（重庆）数据科技股份有限公司、北京数字一百信息技术有限公司、央视市场研究股份有限公司、艾斯艾国际市场调查咨询（北京）有限公司、广州市卓越市场研究有限公司、北京百分点信息科技有限公司（极速洞察）、中国信息协会市场研究业分会、中国标准化研究院。

本标准主要起草人：张军、曹阳、冯卫、熊伟国、张彬、张鸿翔、左云鹏、李晶华、方茜、翁瑞光。

市场研究 个人信息安全保护要求

1 范围

本标准规定了市场研究从业者为完成市场研究在个人信息生命周期内处理受访者或其他个人的个人信息时应遵循的原则和要求。

本标准适用于市场研究中个人信息的处理活动。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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—2010 信息安全技术 术语

GB/T 26315—2010 市场、民意和社会调查 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

市场研究 marketing research

基于特定目的，按照一定规范收集、整理信息，进行分析和呈现的过程。

3.2

研究服务提供者 research service provider

按照客户或资助者要求，实施市场研究项目的机构或个人。

注：市场研究项目包括总项目中的部分研究任务。

[来源：GB/T 26315—2010，3.9，有修改]

3.3

客户 client

要求研究服务提供者提供市场研究服务的委托人。

注：包括公司、政府、非政府组织和个人。

[来源：GB/T 26315—2010，3.7，有修改]

3.4

受访者 respondent

接受访问的人。

[来源：GB/T 26315—2010，3.16]

3.5

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。

注：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

[来源：GB/T 35273—2020，3.1，有修改]

3.6

个人生物识别信息 personal biometric information

包括个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等可识别自然人的生理特性与行为特征的信息。

3.7

个人敏感信息 personal sensitive information

一旦泄露或者非法使用，可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息，包括种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等信息。

注：个人敏感信息包括个人身份信息（身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等）、个人生物识别信息（个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等）、个人财产信息（银行账户、鉴别信息、存款信息、 房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息）、个人健康生理信息（个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、 手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、 以往病史、诊治情况、家族病史、现病史、传染病史等）、其他信息（性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等）、14 岁以下（含）儿童的个人信息等。

[来源：GB/T 35273—2020，3.2，有修改]

3.8

个人信息生命周期 personal information lifecycle

个人信息从收集到彻底销毁的全生命历程。

3.9

个人信息处理者 personal information processor

自主决定处理目的、处理方式等个人信息处理事项的组织或个人。

3.10

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过程。

注：直接使用特定自然人的个人信息，形成该自然人的特征模型，称为直接用户画像。使用来源于特定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型，称为间接用户画像。

[来源：GB/T 35273—2020，3.8]

3.11

个人信息安全影响评估 personal information security impact assessment

针对个人信息处理活动，检验其合法合规程度，判断其对个人合法权益造成损害的各种风险，以及评估用于保护个人的各项措施有效性的过程。

[来源：GB/T 35273—2020，3.9]

3.12

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。

3.13

去标识化 de-identification

个人信息经过处理，使其不借助额外信息的情况下无法识别特定自然人的过程。

3.14

个人信息处理 processing of personal information

对个人信息进行的任何操作或者一系列操作，无论其是否通过自动化手段进行，如个人信息收集、记录、存储、使用、加工、传输、提供、公开等操作。

3.15

个人信息出境 cross-border transfer of personal information

个人信息处理者通过网络或其他等方式，将其在中华人民共和国境内收集和产生的个人信息，通过直接提供服务、产品等方式提供给境外的机构、组织或个人的一次性活动或连续性活动。

注 1：以下情形属于数据出境:

a） 向本国境内，但不属于本国司法管辖或未在境内注册的主体提供个人信息；

b） 个人信息未转移存储至本国以外的地方，但被境外的机构、组织、个人访问查看的（公开信息、网页访问除外）；

c） 个人信息处理者把个人信息由境内转移至境外，涉及其在境内收集和产生的个人信息的。

注 2：非在境内收集和产生的个人信息经由本国出境，未经任何变动或加工处理的，不属于个人信息出境。

注 3：非在境内收集和产生的个人信息在境内存储、加工处理后出境，不涉及境内收集和产生的个人信息的，不属于个人信息出境。

4 个人信息保护原则

4.1 合法性

处理个人信息应当采用合法、正当的方式，遵循诚实信用原则，不得通过欺诈、诱骗、误导、强迫等方式处理个人信息，不得通过非法渠道处理个人信息，不得违反法律、行政法规的规定处理个人信息，不得从事危害国家安全、公共利益的个人信息处理活动。

4.2 权责一致

采取技术和其他必要的措施保障所处理的个人信息安全，并对个人信息处理活动负责，对其个人信息处理活动对受访者或其他个人合法权益造成的损害承担责任。

4.2 目的明确

具有明确、合理的的个人信息处理目的。

4.4 最小必要

处理个人信息应当限于实现处理目的的最小范围，不得进行与处理目的无关的个人信息处理。

4.5 公开透明

以明确、易懂和合理的方式明示个人信息处理规则，并接受外部监督。

4.6 准确性

为实现处理目的，所处理的个人信息应当准确，并及时更新。

5 个人信息来源合法性要求

5.1 客户提供个人信息的合法性要求

研究服务提供者接收客户提供的个人信息以完成市场研究需要的情况下，应将个人信息匿名化后再接收。

特殊情况下必须接收未匿名化个人信息的，应以合同或其他形式先向客户确认个人信息来源合法性以及对个人信息的使用未超出个人授权同意的范围内。同时个人信息的传输和存储应采取加密措施。

5.2 自行收集个人信息的合法性要求

5.2.1 收集个人信息的告知同意

收集受访者或其他个人的个人信息前，应向其告知收集、使用个人信息的目的、方式和范围，并征得受访者或其他个人的授权同意。

以线下形式（包括但不限于问卷调查、座谈会、深访等形式）完成对受访者或其他个人的个人信息的收集前，可将收集、使用个人信息的目的、方式和范围明示在《授权告知书》中，并将《授权告知书》附于问卷或张贴在信息收集区域内，并征得受访者或其他个人的授权同意。

以线上形式（包括但不限于电脑端、移动端等形式）完成对受访者或其他个人的个人信息的收集前，应采用交互界面形式，向受访者或其他个人明示《授权告知书》以告知收集、使用个人信息的目的、方式和范围，例如弹窗、文字说明、提示框等，并征得受访者或其他个人的授权同意。

5.2.2 隐私政策/个人信息保护政策内容

受访者或其他个人应能够随时了解并获得研究服务提供者提供的隐私政策/个人信息保护政策。隐私政策/个人信息保护政策所告知的信息应真实、准确、完整。隐私政策/个人信息保护政策的内容应清晰易懂，符合通用的语言习惯，使用标准化的文字、数字、图示等，避免使用有歧义的语言。内容应包括但不限于：

— 研究服务提供者的基本情况，包括主体身份、联系方式；

— 收集、使用个人信息的类型。涉及个人敏感信息的，需明确标识或突出显示；

— 个人信息收集方式、存储期限、涉及数据出境情况等个人信息处理规则；

— 对外提供个人信息的目的、涉及的个人信息类型、接收个人信息的第三方类型，以及各自的安全和法律责任；

— 个人的权利和实现机制，如查询方法、更正方法、删除方法、注销账户的方法、撤回授权同意的方法、获取个人信息副本的方法等；

— 提供个人信息后可能存在的安全风险及不提供个人信息可能产生的影响；

— 遵循的个人信息安全基本原则，具备的数据安全能力，以及采取的个人信息安全保护措施，必要时可公开数据安全和个人信息保护相关的合规证明；

— 处理个人询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式。

5.2.3 隐私政策/个人信息保护政策形式

研究服务提供者应以明确、易懂、合理的方式公开隐私政策/个人信息保护政策，并接受外部监督，具体包括：

— 以易于访问的方式公开展示。例如，在网站主页、移动互联网应用程序安装页、交互界面或设计等显著位置设置链接；

— 规则应逐一送达个人，并获得个人确认。当成本过高或有显著困难时，可以公告的形式发布，并公布如个人信息泄露时可采取的投诉渠道及方式；

— 在隐私政策/个人信息保护政策所载事项发生变化时，应及时更新隐私政策/个人信

息保护政策并重新告知个人。

5.2.4 收集个人信息时征得授权同意的例外

以下情形中，研究服务提供者收集、使用个人信息不必征得个人的授权同意：

— 与研究服务提供者履行法律法规规定的义务相关的；

— 与国家安全、国防安全直接相关的；

— 与公共安全、公共卫生、重大公共利益直接相关的；

— 与刑事侦查、起诉、审判和判决执行等直接相关的；

— 出于维护个人或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；

— 所涉及的个人信息是个人自行向社会公众公开的，且使用收集符合该个人信息被公开时的用途；

— 根据个人要求签订和履行合同所必需的；

— 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道。

— 个人信息处理者为学术研究机构，出于公共利益开展统计或学术研究所必要， 且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的。

5.3 数据供应商提供个人信息的合法性要求

5.3.1 供应商遴选及入库审查

研究服务提供者在与供应商合作前，应对其完成供应商遴选以及入库审查，审查内容包括但不限于：

— 供应商的基本信息的真实性、准确性和完整性，如营业执照、行政许可或备案(如需)、银行开户、税务登记等；重点审查供应商是否为中国法律合法成立并有效存续的法人或其他组织；

— 供应商是否有相关资质证明，其经营范围是否满足合作需求；

— 供应商内部是否有相关数据安全管理制度及数据安全保护技术措施；

— 供应商收集使用个人信息是否符合《中华人民共和国网络安全法》、《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》、《信息安全技术个人信息安全规范》等法律法规和司法解释的要求。具体包括是否制定并公开数据收集使用规则，是否违反收集使用规则使用个人信息的情况，是否明示收集使用个人信息的目的、方式和范围，是否经个人同意收集使用个人信息，是否发生过数据泄露等方面；

— 供应商是否有行政处罚的信息，是否曾被列入经营异常名录；

— 供应商作为被告的涉诉情况，是否被列入严重违法失信企业名单；

— 供应商以往项目完成质量，配合度等。

5.3.2 承诺函

研究服务提供者在与供应商合作时，应要求供应商说明个人信息来源，并以合同或者承诺函形式对其个人信息来源的合法性进行声明。

5.3.3 授权同意范围

研究服务提供者在与供应商合作时，应了解供应商已获得的个人信息处理的授权同意范围，包括使用目的，个人是否授权同意对外提供、公开披露、删除等。

如市场研究所需进行的个人信息处理超出已获得的授权同意范围的，应在获取个人信息后的合理期限内或处理个人信息前，征得受访者或者其他个人的明示同意，或通过供应商征得受访者或其他个人的明示同意。

6 个人信息的保留

6.1 个人信息的分类存储

研究服务提供者应将市场研究中收集的个人信息进行妥善分类，不同来源、不同类型的个人信息应分别存储，避免数据混淆。

对所存储的分类个人信息应采取安全管理措施，建立使用权的分级制度，形成使用登记记录，并定期进行安全审核。

6.2 个人信息存储时间最小化

个人信息存储期限应为实现个人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个人另行授权同意的除外。

超出上述个人信息存储期限后，应对个人信息进行删除或匿名化处理。

6.3 去标识化处理

收集受访者或其他个人的个人信息后，宜立即进行去标识化处理，并采取技术和管理方面的措施，将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。

7 个人信息的使用

7.1 个人信息的访问

7.1.1 专人负责

不同来源，不同类型的个人信息应指派专人负责对其管理并形成管理日志，记录管理人员、授权人员及权限、个人信息的访问情况、下载情况等。

应当只将对于个人信息的访问权限授权给受其管理并对其负有保密义务的人员。

7.1.2 最小授权

研究服务提供者对被授权访问个人信息的人员，应建立最小授权的访问处理策略，使其只能访问职责所需的最小必要的个人信息，且仅具备完成职责所需的最少的数据操作权限。

7.1.3 内部审批

研究服务提供者在市场研究中对于个人信息处理活动应实行内部审批制度，对其要求包括：

— 对个人信息的重要操作设置内部审批流程，如进行批量修改、拷贝、下载等重要操作；

— 对安全管理人员、数据操作人员、审核人员的角色进行分离设置；

— 确因工作需要，需授权特定人员超权限处理个人信息的，应经个人信息保护责任人或个人信息保护工作机构进行审批，并记录在册；

— 对个人敏感信息的访问、修改等操作行为，需在对角色权限处理的基础上，按照业务流程的需求触发操作授权。例如，当收到受访者投诉，投诉处理人员才可访问该个人的相关信息。

7.1.4 人员离职

人员离职时，研究服务提供者应检查其全部个人信息处理活动，及时删除其访问权限，要求其删除已下载的个人信息数据，并以合同或其他形式确认其保密义务。

7.2 个人信息的使用限制

7.2.1 已结项项目的个人信息使用

已结项或已关闭的市场研究项目中的个人信息原则上不可查询或调取，如特殊情况需要查询和调取的，应设置内部审批流程并记录在册。

7.2.2 使用范围

使用个人信息时，不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围。因市场研究需要，确需超出上述范围使用个人信息的，应再次征得个人明示同意；

注：将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，属于与收集目的具有合理关联的范围之内。但对外提供学术研究或描述的结果时，需对结果中所包含的个人信息进行去标识化处理。

7.2.3 新个人信息使用

如所收集的个人信息经过加工处理而产生的新个人信息，能够单独或与其他个人信息或信息结合能识别特定自然人身份或者反映特定自然人活动情况的，应将其认定为个人信息。对其处理应遵循收集个人信息时获得的授权同意范围。

注：加工处理而产生的个人信息属于个人敏感信息的，对其处理需符合对个人敏感个人信息的要求。

7.2.4 界面展示个人信息

涉及通过界面展示个人信息的（如屏幕显示、纸面），研究服务提供者应对需展示的个

人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险，被访者及个人同意展示的除外。

7.3 用户画像的使用限制

7.3.1 特征描述的合法性要求

用户画像中对受访者或者其他个人的特征描述，不应：

— 包含淫秽、色情、赌博、迷信、恐怖、暴力的内容；

— 表达对民族、种族、宗教、残疾、疾病歧视的内容。

7.3.2 用户画像使用要求

在市场研究或其他对外合作中使用用户画像的，不应：

— 侵害公民、法人和其他组织的合法权益；

— 危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、 民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序。

— 除为实现受访者或个人授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。

7.4 使用目的变更时的告知同意

研究服务提供者因市场研究需要需变更使用目的的，需向个人告知涉及的个人信息类型、变更原因、变更后的处理目的，并再次征得个人的明示同意。使用目的变更包括但不限于以下情形：

— 研究服务提供者收集受访者或其他主体个人信息后，超出原有授权范围使用的；

— 研究服务提供者间接获取个人信息后，进行加工处理形成新的个人信息并用于其他目的；

— 研究服务提供者进行收购、兼并等，将获取的个人信息超出原有授权范围使用的；

— 研究服务提供者收集后涉及重大处理规则变化的，例如需要将个人信息传输到境外进行处理的。

8 个人信息的对外提供

8.1 个人信息的委托处理

8.1.1 委托者要求

研究服务提供者在市场研究中委托第三方处理个人信息时，应符合以下要求：

— 研究服务提供者作出委托行为，不应超出已征得个人授权同意的范围或应遵守 5.2.4 所列情形；

— 研究服务提供者应对委托行为进行个人信息安全影响评估，确认受委托者的数据安全能力；

— 研究服务提供者应对受委托者的个人信息处理进行监督；

— 研究服务提供者应准确记录和存储委托处理个人信息的情况；

— 研究服务提供者得知或者发现受委托者未按照委托要求处理个人信息，或未能有效履行个人信息隐私保护责任的，应立即要求受托者停止相关行为，且采取或要求受委托者采取有效补救措施（如更改口令、回收权限、断开网络连接、现场销毁等）处理或消除个人信息面临的安全风险。必要时研究服务提供者应终止与受委托者的业务关系，并要求受委托者及时删除从研究服务提供者获得的个人信息。

8.1.2 受委托者要求

受委托者应符合以下要求：

— 严格按照研究服务提供者的要求处理个人信息。受委托者因特殊原因未按照研究服务提供者的要求处理个人信息的，应及时向研究服务提供者反馈；

— 未经研究服务提供者同意，受托方不得转委托他人处理个人信息；

— 协助研究服务提供者保障受访者或其他个人的权利；

— 受委托者在处理个人信息过程中无法提供足够的安全保护水平或发生了安全事件的，应及时向研究服务提供者反馈；

— 在委托关系解除时将个人信息返还个人信息处理者或者予以删除。

8.2 个人信息的第三方提供

8.2.1 个人信息第三方提供限制

研究服务提供者在市场研究中应仅向客户及其他第三方提供匿名化处理后的受访者或其他个人的个人信息，或仅提供统计分析结果，除非：

— 已向受访者或其他个人告知第三方的身份、个人信息的处理目的、处理方式和个人信息的种类，并事先征得受访者或其他个人的授权同意；

— 提供经去标识化处理的个人信息，且确保个人信息接收方无法重新识别或者关联个人。

8.2.2 个人信息提供者要求

研究服务提供者在市场研究中对外提供个人信息时，应充分重视风险。对外提供个人信息，非因收购、兼并、重组、破产原因的，应符合以下要求：

— 事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人的措施；

— 通过合同等方式规定双方的责任和义务；

— 准确记录和存储个人信息的对外提供情况，包括对外提供的日期、规模、目的，以及个人信息接收方基本情况等；

— 研究服务提供者发现个人信息接收方违反法律法规要求或双方约定处理个人信息的，应立即要求个人信息接收方停止相关行为，且采取或要求个人信息接收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）处理或消除个人信息面临的安全风险；必要时研究服务提供者应解除与个人信息接收方的业务关系，并要求个人信息接收方及时删除从研究服务提供者获得的个人信息；

— 因对外提供个人信息发生安全事件而对个人合法权益造成损害的，研究服务提供者应承担相应的责任；

— 帮助个人了解个人信息接收方对个人信息的存储、使用等情况，以及个人的权利。

8.2.3 个人信息接收者要求

客户及其他第三方在市场研究中作为接收方，接收个人信息时应符合以下要求：

— 履行合同约定的责任和义务；

— 在个人的授权同意范围内处理个人信息；

— 超出个人的授权同意范围处理个人信息的，应重新向个人告知并取得其同意；

— 接收匿名化或去标识化后个人信息的，接收者不得利用技术手段重新识别个人身份。

8.3 收购、兼并、重组、破产时的个人信息转让

当研究服务提供者发生收购、兼并、重组、破产等变更时，对研究服务提供者的要求包括：

— 向个人告知有关情况；

— 变更后的个人信息处理者应继续履行原个人信息处理者的责任和义务，如变更个人信息使用目的时，应重新取得个人的明示同意；

— 如破产且无承接方的，对个人信息作删除或销毁处理。

8.4 个人信息公开披露

个人信息原则上不应公开披露，研究服务提供者经法律授权或具备合理事由确需公开披露时，应符合以下要求：

— 事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人的措施；

— 向个人告知公开披露个人信息的目的、类型，并事先征得个人明示同意；

— 准确记录和存储个人信息的公开披露的情况，包括公开披露的日期、规模、目的、公开媒体/平台、公开范围等；

— 承担因公开披露个人信息对个人合法权益造成损害的相应责任。

8.5 对外提供个人信息不必征得个人的授权同意的情形

以下情形中，研究服务提供者不必征得个人的授权同意：

— 与个人信息处理者履行法律法规规定的义务相关的；

— 与国家安全、国防安全直接相关的；

— 与公共安全、公共卫生、重大公共利益直接相关的；

— 与刑事侦查、起诉、审判和判决执行等直接相关的；

— 出于维护个人或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；

— 个人自行向社会公众公开的个人信息，且对外提供符合该个人信息被公开时的用途；

— 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道。

9 儿童或弱势人群个人信息和个人敏感信息

9.1 儿童或弱势人群个人信息和个人敏感信息的收集

研究服务提供者在市场研究中收集儿童或弱势人群个人信息和个人敏感信息时对其额外要求包括：

— 具有特定的目的和充分的必要性；

— 收集年满 14 周岁未成年受访者或其他未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意；

— 收集弱势人群，即因精神、情绪、社会或身体原因可能限制其作出自愿和明智决定的能力，长期或暂时不能表达其自身利益的人群的个人信息前，应征得弱势人群及其监护人的明示同意；

— 收集受访者或其他个人的个人敏感信息前，应征得个人的明示同意，并应确保个人的明示同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示；

— 收集受访者或其他个人的个人生物识别信息前，应单独向个人告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人的明示同意；

— 法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

9.2 个人敏感信息的传输和存储

9.2.1 加密措施

在市场研究中传输和存储个人敏感信息时，应采用加密等安全措施。

9.2.2 分开存储

在市场研究中存储个人敏感信息时，个人生物识别信息应与个人身份信息分开存储。并且原则上不应存储原始个人生物识别信息（如样本、图像等），可采取的措施包括但不限于：

— 仅存储个人生物识别信息的摘要信息；

— 在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能；

— 在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。

9.3 个人敏感信息的对外提供

9.3.1 明示同意

研究服务提供者在市场研究中对外提供个人敏感信息前，除 8.2.1 中告知的内容外，还应向受访者或其他个人告知涉及的个人敏感信息类型、数据接收方的身份和数据安全能力，并事先征得个人的明示同意。法律、行政法规规定需取得书面同意的，从其规定。

9.3.2 个人生物识别信息的对外提供

个人生物识别信息原则上不应对外提供。因市场研究需要，确需对外提供的，应单独向受访者或其他个人告知目的、涉及的个人生物识别信息类型、数据接收方的具体身份和数据安全能力等，并征得个人的明示同意。法律、行政法规规定需取得书面同意的，从其规定。

9.4 个人敏感信息的公开披露

研究服务提供者公开披露个人敏感信息时对其额外要求包括：

— 公开披露个人敏感信息前，除 8.4 中告知的内容外，还应向受访者或其他个人告知涉及的个人敏感信息的内容；

— 不应公开披露个人生物识别信息；

— 不应公开披露我国公民的民族、政治观点、宗教信仰等个人敏感数据的分析结果。

10 个人在个人信息处理活动中的权利

10.1 选择权

市场研究中受访者或其他个人对个人信息的处理享有选择权，受访者或其他个人在市场研究中的对其个人信息的提供是完全自愿的，其有权选择同意或者拒绝。

10.2 保密权

受访者或其他个人有权要求研究服务提供者或客户采取必要的措施和手段对其收集到的个人信息承担保密义务，除非得到受访者或其他个人的授权同意，其他第三方无权知晓。

10.3 知情权

受访者或其他个人有权知晓如下事项：

— 受访者或其他个人向个人信息处理者查询其个人信息内容、类型、来源、目的和适用范围以及获得上述个人信息的第三方身份或类型的方法；

— 复制个人信息的方法；

— 个人信息处理者的隐私政策/个人信息保护政策。

10.4 更正权

受访者或其他个人发现个人信息处理者所持有的个人信息不准确或不完整的，或者受访者或其他个人想要撤回其对个人信息处理活动的授权同意，个人信息处理者应为其提供请求更正或补充信息或撤回授权同意的方法。

10.5 删除权

受访者或其他个人有权要求个人信息处理者停止对其个人信息的处理活动，并要求个人信息处理者删除其个人信息。

10.6 投诉权

市场研究中受访者或其他个人对个人信息的处理享有投诉权，个人信息处理者应建立投诉管理机制和投诉跟踪流程，并在合理的时间内对投诉进行响应并形成记录。记录内容可包括投诉的日期、投诉的原因、投诉的受访者或其他个人的身份、投诉的内容以及投诉的解决过程及结果等。

11 个人信息安全保护措施

11.1 安全保护的技术措施

研究服务提供者应当采取一定的技术措施以确保合理应对风险的安全水平，防止个人信息的泄露、损毁、丢失、篡改，包括但不限于下列措施：

— 应采取防范计算机病毒和网络攻击、网络侵入等危害个人信息安全行为的技术措施以保护个人信息；

— 个人信息的匿名化和加密处理；

— 实时监测数据系统的运行情况，遇异常登录或异常下载情况时应断开链接并立即预警；

— 确保数据系统和服务持续具备保密性、完整性、可用性和可复原性；

— 在发生实体事故或技术事故时，及时恢复个人信息的可用性和可访问性的能力；

— 技术措施成效应定期测试和评估。

11.2 安全影响评估

11.2.1 适用条件

出现以下任意一种情况时，研究服务提供者应进行个人信息安全影响评估：

— 当一种处理活动可能对个人信息产生高风险时，研究服务提供者应当在处理前完成个人信息安全影响评估；

— 在个人信息对外提供前，或市场研究项目发生重大变化时，应进行个人信息安全影响评估；

— 在法律法规有新的要求时，或在业务合作、信息系统、运行环境发生重大变更时，

或发生重大个人信息安全事件时，应进行个人信息安全影响评估。

11.2.2 评估内容

个人信息安全影响评估应主要评估处理活动遵循个人信息安全基本原则的情况，以及个人信息处理活动对个人合法权益的影响，内容包括但不限于：

— 个人信息收集环节是否遵循目的明确、选择同意、最小必要等原则；

— 个人信息处理是否可能对个人合法权益造成不利影响，包括是否会危害人身和财产安全、损害个人名誉和身心健康、导致差别性待遇等；

— 个人信息安全措施的有效性；

— 匿名化或去标识化处理后的数据集重新识别出个人或与其他数据集汇聚后重新识别出个人的风险；

— 对外提供、公开披露个人信息对个人合法权益可能产生的不利影响；

— 发生安全事件时，对个人合法权益可能产生的不利影响。

11.2.3 评估报告

研究服务提供者应形成个人信息安全影响评估报告，并以此采取保护个人的措施，使风险降低到可接受的水平，同时应妥善留存个人信息安全影响评估报告，确保可供相关方查阅，并以适宜的形式对外公开。

11.3 安全保护的人员管理

研究服务提供者承担个人信息安全保护责任，对其要求包括：

— 明确责任部门和人员对个人信息安全负直接责任；

— 应明确内部涉及个人信息处理不同岗位的职责，并与其签署保密协议，对大量接触个人敏感信息的人员进行背景审查，以了解其犯罪记录、诚信状况等；

— 应要求个人信息处理岗位上的相关人员在调离岗位或终止劳动合同时，继续履行保密义务；

— 应明确可能访问个人信息的外部服务人员应遵守的个人信息安全要求，与其签署保密协议，并进行监督；

— 应建立相应的内部制度和政策对员工提出个人信息保护的指引和要求；

— 应定期（至少每年一次）或在隐私政策/个人信息保护政策发生重大变化时，对个人信息处理岗位上的相关人员开展个人信息安全专业化培训和考核，确保相关人员熟练掌握个人信息保护政策和相关规程。

12 个人信息境外提供

12.1 境外提供要求

12.1.1 境外提供的前提条件

研究服务提供者因市场研究需要，需确向境外提供个人信息的，应当至少具备下列一项条件：

— 依照相关法律规定通过国家网信部门组织的安全评估；

— 按照国家网信部门的规定经专业机构进行个人信息保护认证；

— 与境外接收方订立合同，约定双方的权利义务，并监督其个人信息处理活动符合中华人民共和国境内法律、行政法规规定以及本标准规定的个人信息保护标准；

— 法律、行政法规或者国家网信部门规定的其他条件。

12.1.2 获得授权同意

个人信息出境，应向个人说明个人信息数据出境的目的、范围、内容、接收方及接收方所在的国家或地区，并经其同意。未成年人个人信息出境须经其监护人同意。

12.1.3 完成出境安全评估

研究服务提供者在中华人民共和国境内运营中收集和产生的个人信息，应当在境内存储。因特定市场研究需要，确需向境外提供的，应当进行安全评估，并对评估结果负责。个人信息出境安全评估应重点评估以下内容：

— 个人信息出境的必要性，以及是否符合法律、行政法规的规定；

— 涉及个人信息情况，包括个人信息的数量、范围、类型、敏感程度，以及个人是否同意其个人信息出境等；

— 个人信息接收方是否有损害个人合法权益的历史、是否发生过重大安全事件；

— 个人信息接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等；

— 个人信息出境及再转移后被泄露、毁损、篡改、滥用等风险；

— 个人信息出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险；

— 其他需要评估的重要事项。

12.1.4 禁止出境的情况

存在以下情况之一的，个人信息不得出境：

— 个人信息出境未经受访者或其他个人同意，或可能侵害个人利益；

— 个人信息出境可能给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益；

— 其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。

12.2 个人信息出境记录

个人信息出境应当建立个人信息出境记录，并且至少保存 5 年，记录内容包括：

— 向境外提供个人信息的日期时间；

— 接收者的身份，包括但不限于接收者的名称、地址、联系方式等；

— 向境外提供的个人信息的类型及数量、敏感程度；

— 国家网信部门、公安部门、安全部门等有关部门规定的其他内容。

12.3 个人信息跨境传输

研究服务提供者在中华人民共和国境内收集和产生的个人信息向境外提供的，应遵循国家相关规定和相关标准的要求。

13. 个人信息安全事件处置

13.1 个人信息安全事件应急处置和报告

13.1.1 安全事件应急预案

研究服务提供者应制定个人信息安全事件应急预案，同时应定期（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。

13.1.2 安全事件应急处置

发生个人信息安全事件后，研究服务提供者应根据应急响应预案进行以下处置：

— 记录安全事件内容，包括但不限于：发现安全事件的人员、时间、地点，涉及的个人信息及人数，发生安全事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门；

— 评估安全事件可能造成的影响，并采取必要措施处理事态，消除隐患；

— 按照《国家网络安全事件应急预案》等有关规定及时上报，报告内容包括但不限于：涉及个人的类型、数量、内容、性质等总体情况，安全事件可能造成的影响，已采取或将要采取的处置措施，安全事件处置相关人员的联系方式；

— 个人信息泄露安全事件可能会给个人的合法权益造成严重危害的，如个人敏感信息的泄露，按照 13.2 的要求实施安全事件的告知。

— 根据相关法律法规变化情况，以及安全事件处置情况，及时更新应急预案。

13.2 安全事件告知

13.2.1 安全事件告知要求

研究服务提供者应及时将安全事件相关情况以邮件、信函、电话、推送通知等方式任选其一告知受影响的个人。难以逐一告知个人时，应采取合理、有效的方式发布与公众有关的警示信息。

13.2.2 安全事件告知内容

安全事件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；

— 个人自主防范和降低风险的建议；

— 针对个人提供的补救措施；

— 个人信息保护负责人和个人信息保护工作机构的联系方式。