ICS 35.030
CCS

中华人民共和国国家标准

GB/T XXXXX—XXXX

数据安全技术 个人信息安全规范

Data security technology — Personal information security specification

（工作组讨论稿）

（本草案完成时间：2026-06-01）

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
国家标准化管理委员会　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。本标准代替GB/T 35273-2020《信息安全技术 个人信息安全规范》，与GB/T 35273-2020相比，主要技术变化如下：

——修改了“敏感个人信息”（见3.2）；

——增加了“单独同意”（见3.8）；

——增加了“保证质量原则”（见4）；

——增加了“个人信息处理合法性基础”（见5）；

——增加了“敏感个人信息的收集”（见6.6）；

——增加了“人工智能类产品或服务的收集”（见6.7）；

——增加了“终端类产品或服务的收集”（见6.8）；

——增加了“统一账号体现的使用”（见8.6）；

——增加了“海外法律管辖判定与冲突处理”（见11）；

——增加了“个人信息保护负责人”（见13.1）；

——增加了“个人信息保护工作机构与人员”（见13.2）；

——增加了“个人信息保护合规审计”（见13.8）。

本文件由全国网络安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：中国电子技术标准化研究院、北京理工大学、赛西（深圳）电子信息产品标准化工程中心有限公司、中央网信办（国家网信办）数据与技术保障中心、国家信息技术安全研究中心、中国网络安全审查认证和市场监管大数据中心、华为技术有限公司、荣耀终端股份有限公司、中兴通讯股份有限公司、蚂蚁科技集团股份有限公司、北京抖音信息服务有限公司、深圳市腾讯计算机系统有限公司、北京三快科技有限公司、北京快手科技有限公司、阿里巴巴（北京）软件服务有限公司、国网江苏省电力有限公司信息通信分公司、北京小桔科技集团有限公司、中国联合网络通信集团有限公司、杭州萤石软件有限公司、西安交通大学、唯品会（中国）有限公司、阿里云计算有限公司、腾讯云计算（北京）有限责任公司、北京抖音科技有限公司等。

本文件主要起草人：姚相振、洪延青、高超、胡影、郝春亮、刘行、何延哲、国震寰、高月、杨韬、刘曦泽、魏昊、张敏、衣强、郑云文、闫金保、赵晓娜、梅傲婷、白晓媛、李海英、李昳婧、马硕、张亚男、武杨、朱玲凤、田喜清、落红卫、王昕、顾伟、刘艾婧、赵新建、张颂、李媛、黄如鑫、胡文慧、孙艺、郑鸿咚、范铭、罗丹、黄天宁、刘阳璐、杨骁涵等。

引　言

近年来，随着新技术的广泛应用，个人信息处理活动呈现场景多元、业务多样、链条复杂、跨境交互频繁的特征，个人信息保护面临新的风险与挑战。全球数据治理规则趋严、数据出海需求持续增长、新技术新业态不断涌现，个人信息非法收集、滥用、泄露等安全问题更加突出，对个人合法权益、社会公共利益乃至国家安全构成潜在威胁。

为适应新形势下个人信息保护与数据安全治理需要，本标准依据《中华人民共和国网络安全法》《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》《网络数据安全管理条例》等相关法律，聚焦个人信息全生命周期安全，完善处理规则、细化安全要求、强化主体责任，支撑各方有效遏制个人信息安全乱象，规范组织在收集、存储、使用、加工、传输、提供、公开、删除等处理活动中的行为，提升个人信息保护水平，保障数字经济健康有序发展。

对标准中的涉及的要求，法律法规另有规定的，需遵照其规定执行。

数据安全技术 个人信息安全规范

1 范围

本文件规定了开展收集、存储、使用、加工、传输、提供、公开、删除等个人信息处理活动应遵循的原则和安全要求。

本文件适用于规范各类组织个人信息处理活动，也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、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 25069—2022 信息安全技术 术语

GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

GB/T 42574—2024 信息安全技术 个人信息处理中告知和同意的实施指南

GB/T 45574—2025 数据安全技术 敏感个人信息处理安全要求

GB 46864—2025 数据安全技术 电子产品信息清除技术要求

GB/T 46903—2025 数据安全技术 个人信息保护合规审计要求

GB/T AAAA—AAAA 数据安全技术 未成年人产品和服务个人信息保护要求

GB/T AAAA—AAAA 数据安全技术 数据提供、委托处理、共同处理安全指南

3 术语和定义

GB/T 25069—2022 中界定的以及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。

注 1：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。

注 2：关于个人信息的判定方法和类型可参见附录 A。

注 3：个人信息处理者通过个人信息或其他信息加工处理后形成的信息，例如用户画像或特征标签，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，属于个人信息。

3.2

敏感个人信息 sensitive personal information

一旦遭到泄露或非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。

注1：敏感个人信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息和不满十四周岁未成年人的个人信息。

注2：关于敏感个人信息的识别和界定可参考附录B以及GB/T 45574-2025。

注3：多项个人信息汇聚后达到定义条件的，应将汇聚后的个人信息整体按照敏感个人信息进行识别与保护。

3.3

个人信息主体 personal information subject

个人信息所识别或者关联的自然人。

3.4

个人信息处理者 personal information processor

在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

注1：自然人因个人或者家庭事务处理个人信息的，相关自然人无需承担个人信息处理者的法定义务，但仍可依据实际处理活动判断其是否构成个人信息处理者并适用相应的安全要求。

注2：代表组织从事个人信息处理活动的个人不认定为个人信息处理者。

注3：应针对具体的个人信息处理活动确定所对应的个人信息处理者。产品或服务涉及多项个人信息处理活动的，产品或服务的提供者可能在部分处理活动中构成个人信息处理者，在其他处理活动中构成受托人。

注4：可以通过参与方约定、生效的规则等方式明确个人信息处理活动中的角色，在没有反面证据的情况下，可以按照约定和规则内容认定相关主体在个人信息处理活动中定性。

3.5

收集 collect

获得个人信息的控制权的行为，包括由个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等直接采集行为，通过接收其他个人信息处理者提供、转移，或搜集已公开个人信息等间接获取个人信息。

3.6

同意 consent

个人信息主体对其个人信息进行自愿、明确作出授权的行为。

注1：包括通过积极行为作出授权（即明示同意），或者通过自主行为推定作出授权。

注2：明示同意指个人信息主体通过书面、口头等方式对其个人信息处理作出的肯定性授权动作，如个人主动勾选或主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

注3：自主行为推定授权如信息采集区域内的个人信息主体在被告知信息收集行为后没有离开该区域等。

3.7

单独同意 separate consent

个人针对其个人信息进行特定处理而专门作出具体、明确授权的行为，不包括一次性针对多种目的或方式的个人信息处理活动作出的同意。

注：单独同意的告知内容与取得同意的方式需与其他处理活动予以区分。

3.8

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。

3.9

个人信息保护影响评估 personal information protection impact assessment

针对个人信息处理活动，检验其是否合法合规，分析其对个人信息主体合法权益造成的侵害及相应的安全风险，以及评价保护个人信息的各项措施有效性的过程。

3.10

删除 delete

将个人信息从其存储的所有系统中去除，使其达到不可被检索、访问或恢复的状态。

3.11

公开 publicize

向社会或不特定人群发布信息的行为。

注：在社交媒体平台中向非特定数量的个人发布信息的，即使发布者对可见范围设置了限制，若该信息的实际或潜在接收者数量较大且超出发布者的可控范围，宜参照本定义评估其公开属性。

3.12

转移 transfer of control

将个人信息控制权由一个个人信息处理者向另一个个人信息处理者转移的过程。

3.13

提供 providing

个人信息处理者向其他个人信息处理者提供个人信息，且双方分别对个人信息拥有独立控制权的过程。

注：委托第三方处理个人信息的，不属于向其他个人信息处理者提供个人信息的行为。

3.14

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。

3.15

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。

注：去标识化建立在个体基础之上，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对个人信息的标识。

3.16

个性化展示 personalized display

基于特定个人信息主体的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息，向该个人信息主体展示信息内容、提供商品或服务的搜索结果等活动。

3.17

业务功能 business function

满足个人信息主体的具体使用目的的功能。

注：常见的业务功能包括地图导航、网络约车、即时通讯、社区社交、网络支付、新闻资讯、网上购物、快递配送、交通票务等。

3.18

设备信息 device information

描述设备基本属性、唯一标识、运行状态的信息，包括设备制造商在生产阶段写入的硬件参数、序列号、唯一设备识别码。

3.19

统一账号 unified account

同一集团下不同无股权关系的实体之间提供的统一账号体系，用户可使用统一账号访问相关联的所有产品。

示例：同一集团下设A、B、C三家无股权关系的公司，分别运营不同的产品和服务，通过一个账号可以登录和使用A、B、C三家公司运营的多款产品和服务。

3.20

委托处理 commissioned processing

个人信息处理者委托个人、组织按照约定的目的和方式开展的个人信息处理活动。

4 个人信息安全基本原则

个人信息处理者开展个人信息处理活动应遵循合法、正当、必要、诚信原则，具体包括：

a） 权责一致——采取技术和其他必要的措施保障个人信息的安全，对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任。

b） 目的明确——具有明确、清晰、具体的个人信息处理目的。

c） 授权同意——向个人信息主体明示个人信息处理目的、方式、范围、规则等，在处理个人信息前取得个人信息主体同意或具备其他合法性基础。

d） 最小必要——处理个人信息应当具有合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。

e） 公开透明——以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督。

f） 保证质量——通过提醒、校验、核实等手段，保证收集的个人信息的真实性和准确性，发现个人信息存在错误时，及时告知个人信息主体并提供更正渠道，避免因信息不准确导致决策偏差或权益损害。

g） 确保安全——具备与所面临的安全风险相匹配的安全能力，并采取足够的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。

h） 权利保障——向个人信息主体提供能够查询、更正、删除其个人信息，以及撤回同意、注销账号、投诉等方法。

5 个人信息处理的合法性基础与合规要求

5.1 基本要求

个人信息处理者应：

a） 在个人信息处理活动开始前识别并记录相应的合法性基础，形成可核验、可追溯、可审计的证据链；合法性基础一经确定，不应以规避义务为目的随意变更；

b） 确保合法性基础的适用应遵循合法、正当、必要、最小影响原则；当存在多种可选基础时，应选择对个人权益影响更小的方式，并保持与告知信息一致；

c） 确保合法性基础与告知、处理活动记录、个人信息保护影响评估、个人信息保护合规审计之间应保持一致，并在处理目的、范围或情形发生重大变更时同步更新；

d） 宜妥善记录个人信息处理活动的合法性基础，记录的内容包括但不限于适用基础、适用性说明、审批流程和记录、时间戳与证据材料。

注：证明材料通常包括合同条款、法条号、系统配置截图等。

5.2 取得个人同意

个人同意作为合法性基础的要求包括：

a） 收集敏感个人信息，应取得个人信息主体的单独同意；

b） 收集不满 14 周岁未成年人个人信息，应取得其父母或其他监护人的单独同意；

c） 法律、行政法规规定处理个人信息应当取得个人书面同意的，应取得个人书面同意；

d） 取得个人信息主体同意前应向个人信息主体告知个人信息的相应处理规则；

e） 同意应基于清晰的告知并通过明确的主动行为作出；默认同意、被动同意、以继续使用为条件强迫同意等均不应视为有效同意，同意的实施参照 GB/T 42574-2023 的 9.1~9.4；

f） 个人信息处理者应当提供便捷的撤回同意的方式，个人撤回同意不影响撤回前基于个人同意已进行的个人信息处理活动的效力，撤回同意后，个人信息处理者应立即停止基于该使用目的的除存储和采取必要的安全保护措施之外的处理；

注：如个人信息存在向第三方提供情形，则撤回同意后提供行为需立即终止。

g） 应留存同意的证据，记录同意的内容、时间、方式、载体、证明材料及撤回轨迹等，记录方式参照 GB/T 42574-2023 的 9.7；

h） 在处理不满十四周岁未成年人或其他无民事行为能力人、限制民事行为能力人等依法需取得监护人同意的个人信息时，依法取得监护人同意并保留记录。

5.3 订立、履行合同所必需

订立、履行合同所必需作为合法性基础的要求包括：

a） 仅限于实现合同的核心目的，或应个人请求、履行所适用的法律、行政法规规定等客观原因而在订立前采取措施所必需时方可适用；

b） 不应将与合同核心目的无直接关联的处理活动纳入本项，包括但不限于以商业营销为目的的个性化化广告、超出合同必要范围的行为分析、非实现合同义务所需的用户画像等。合同履约所必需的风险评估、质量改进等活动，应能证明其与合同目的的直接关联性；

c） 应评估个人信息处理活动与合同核心义务之间的关联与可替代性；

d） 应在处理活动记录中标注合同条款/要约要素与个人信息字段的对应关系；

e） 如合同变更导致处理目的或范围变化，应在变更生效前重新评估个人信息处理活动的合法性基础。

5.4 劳动合同所必需

按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需作为合法性基础的要求包括：

a） 仅限于劳动用工、人力资源管理、劳动纪律管理、薪酬福利、绩效考核、劳动争议处理等管理目的所必需的个人信息处理活动；
b） 应以依法制定的劳动规章制度、依法签订的集体合同或劳动合同等为依据，并在处理活动记录中标明对应依据；
c） 不应将商业营销、员工画像、与劳动管理无直接关系的行为监测等处理目的纳入本项；
d） 涉及敏感个人信息、自动化决策、公开、对外提供、出境等情形的，还应符合本文件相应章节要求。

5.5 为履行法定职责或者法定义务所必需

履行法定职责或者法定义务所必需作为合法性基础的要求包括：

a） 仅当存在明确的法律、行政法规或具有法律效力的规范性文件要求并指向具体处理义务时方可适用；
b） 个人信息处理范围应仅限于履行法定义务所必需的最小范围，并不应用于与该义务无关的其他目的；
c） 应在记录中标注明确的法律、行政法规或具有法律效力的规范性文件要求；
d） 如将基于法律合规收集的个人信息用于其他目的时，应重新评估其他目的适用的合法性基础。

5.6 公共卫生事件或紧急情况下为保护生命健康、财产安全所必需

公共卫生事件或紧急情况下为保护生命健康、财产安全所必需作为合法性基础的要求包括：

a） 仅当突发、紧迫场景下用于保护自然人的生命健康或重大财产安全时方可适用；
b） 依法由公共卫生主管机关开展疾病监测、报告、干预所需处理，可在未获授权情况下进行；
c） 应评估个人信息处理活动的紧急性与不可替代性，并保留授权与决定链条。

5.7 为公共利益实施新闻报道、舆论监督等行为

公共利益实施新闻报道、舆论监督作为合法性基础的要求包括：

a） 应仅为新闻报道、舆论监督或其他公共利益相关表达；
b） 不应以“公共利益”为名实施与报道目的无关、过度或侮辱性的处理，尤其不应对未成年人、受害者等弱势群体造成二次伤害；
c） 应开展个人信息保护影响评估，综合考量信息公共性和新闻性、对个人权益的影响、处理方式与范围、可替代性等因素，并采取去标识化、数据最小化等控制，实现公共利益与个人信息权益的平衡；
d） 建立新闻报道、舆论监督所涉及的个人信息处理行为及拟公开内容建立审核机制，保存编辑与法务审查记录；
e） 对事实错误、断章取义或已失时效的信息，应及时更正与更新。

5.8 在合理范围内处理个人自行公开或其他合法公开的个人信息

合理范围内处理个人自行公开或其他合法公开的个人信息作为合法性基础的要求包括：

a） 应确认个人信息来源的公开具有合法依据；

b） 应用于公开个人信息的原始目的，不应将已公开个人信息用于用户画像、商业营销等其他目的；
c） 仅处理为实现目的必需的公开个人信息，不宜绕过技术限制实施抓取或聚合；
d） 对于公开的敏感个人信息，不应仅因敏感个人信息已公开而降低对其的保护强度；
e） 应建立处理已公开个人信息清单，明确信息来源、获取时间、公开依据、限制条件、处理目的与范围、必要性评估与去标识化措施等；
f） 批量抓取或聚合使用前应开展个人信息保护影响评估，采取合理措施并设置个人权利响应通道。

5.9 法律、行政法规规定的其他情形

法律、行政法规规定的其他情形作为合法性基础的要求包括：
a） 仅在明确的法律、行政法规就特定处理目的、范围、条件作出规定时适用；
b） 不应自行以“其他情形”为由扩大解释，或以部门内部制度、行业自律文件替代法律依据；
c） 在记录中载明法律依据名称、条款、适用场景与效力层级；
d） 定期复核外部规范变化，必要时启动重评与更新告知。

6 个人信息的收集

6.1 最小必要

对个人信息处理者的要求包括：
a） 收集的个人信息的类型、字段、时机、粒度、范围应与实现产品或服务的业务功能直接相关，并采取对用户权益影响最小的方式；扩展功能需证明与基本功能存在合理关联性。

注 1：如产品或服务只需特定类型个人信息时，不应收集其他类型个人信息；如只需某一类型个人信息的部分字段内容时，不应收集所有字段内容；如只需特定功能场景收集，不应在其他无关功能场景收集；如只需粗粒度个人信息，不应收集细粒度个人信息；如只需向指定用户收集，或只收集特定范围个人信息，不应向所有用户默认收集或收集全部个人信息；

注 2：直接相关是指没有上述个人信息的参与，产品或服务的基本功能或扩展功能无法实现。

b） 自动采集个人信息的频率应是对个人权益影响最小且实现产品或服务的业务功能所必需的最低频率；
c） 间接获取个人信息的数量应是对个人权益影响最小且实现产品或服务的业务功能所必需的最少数量；
d） 收集个人信息用于人工智能产品或服务数据预处理、模型训练时，应限于实现业务所需的最小必要范围，并采取有效安全技术手段降低个人信息泄露的可能性；
e） 人工智能产品或服务宜设置输入端的用户提醒和过滤机制以实现个人信息收集的最小必要，并可通过过滤机制阻断非必要的敏感个人信息；

注 3：如产品或服务识别到用户输入敏感个人信息，可设置提示“请注意隐私风险，谨慎输入敏感个人信息”。

f） 人工智能产品或服务不应提前收集超出其功能或者服务所需的个人信息，应在用户首次启用相关功能时告知对应个人信息收集情况并申请所需权限；
g） 个人信息处理者宜优先采用隐私增强技术实现最小化收集。采用隐私增强技术的，应向个人信息主体告知技术原理及对个人信息权益的影响；
h） 定期评估收集个人信息的必要性，并在业务功能、技术环境或法律法规发生变化时重新进行验证。

6.2 自主选择

当产品或服务提供多项需收集个人信息的业务功能时，个人信息处理者不应违背个人信息主体的自主意愿，强迫个人信息主体接受产品或服务所提供的业务功能及相应的个人信息收集请求。对个人信息处理者的要求包括：

a） 不应通过捆绑产品或服务各项业务功能的方式，要求个人信息主体一次性接受并授权同意其未申请或使用的业务功能收集个人信息的请求；

注 1：需要连续自动执行的任务，如自动化人工智能助手类应用，在经过个人信息保护影响评估和充分告知用户的前提下，可以在开始自动化任务前一次性告知所要收集的个人信息和所要申请的权限，并取得个人信息主体的同意。

b） 应把个人信息主体自主作出的肯定性动作，如主动点击、勾选、填写等，作为产品或服务的特定业务功能的开启条件。个人信息处理者应仅在个人信息主体开启该业务功能后，开始收集个人信息；

注 2：实现方法可参考附录 C。

c） 关闭或退出业务功能的途径或方式应与个人信息主体选择使用业务功能的途径或方式同样方便。个人信息主体选择关闭或退出特定业务功能后，个人信息处理者应停止该业务功能的个人信息收集活动；

d） 个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应频繁征求个人信息主体的授权同意；

e） 个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应暂停个人信息主体自主选择使用的其他业务功能，或降低其他业务功能的服务质量；

f） 不应以改善服务质量、提升个人信息主体体验、研发新产品、增强安全性等为由，强制要求个人信息主体同意收集个人信息；

g） 产品或服务的扩展功能使用人工智能技术的，应允许个人信息主体关闭人工智能相关扩展功能。

6.3 告知和同意

对个人信息处理者的要求包括：

a） 收集个人信息，应向个人信息主体告知个人信息处理者的名称或者姓名和联系方式，个人信息的处理目的、处理方式，处理的个人信息种类、保存期限，个人行使权利的方式和程序，并取得个人信息主体的同意；

注 1：如产品或服务仅提供一项收集、使用个人信息的业务功能时，个人信息处理者可通过个人信息处理规则的形式，实现向个人信息主体的告知；产品或服务提供多项收集、使用个人信息的业务功能的，除个人信息处理规则外，个人信息处理者宜在实际开始收集特定个人信息时，向个人信息主体提供收集、使用该个人信息的目的、方式和范围，以便个人信息主体在作出具体的同意前，能充分考虑对其的具体影响。

注 2：告知和同意的实施方法见 GB/T 42574-2023 第 8 章和第 9 章。

a） 通过部署自动化设备收集现场个人信息且未事先取得个人同意的，应使用具有明显外形特征的采集设备，或通过播放语音提示、张贴标识、开启设备提示灯等可以使个人信息主体意识到其个人信息正在被收集的方式；

b） 具备生物识别功能的设备，应根据产品使用场景限制识别的范围，仅允许授权用户在限定范围内被识别或检测；

c） 收集敏感个人信息前，应取得个人信息主体的单独同意，并应确保个人信息主体的单独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；

d） 收集年满 14 周岁未成年人的个人信息前，应征得未成年人或其监护人的同意；收集不满 14 周岁未成年人的个人信息前，应征得其父母或其他监护人的单独同意；

e） 间接获取个人信息时：

1） 对于公开渠道收集个人信息时，应遵循个人信息提供方设定的公开个人信息处理规则；

2） 通过采购第三方服务收集个人信息时，应通过合同等方式要求个人信息提供方对其提供的个人信息来源及后续对外提供的合法性负责，个人信息处理者应仅对接收个人信息后的使用过程合法性负责；

3） 个人信息处理者应与个人信息提供方确认数据来源的合法性及对外提供的合法性；

4） 个人信息提供方对外提供个人信息前宜先经过第三方法律服务机构数据合规评估或者自评估且评估结论为通过。

6.4 个人信息处理规则

对个人信息处理者的要求包括：

a） 应制定个人信息处理规则，内容应包括但不限于：

1） 个人信息处理者的基本情况，包括名称或者姓名和有效的联系方式；

2） 收集、使用个人信息的业务功能，以及各业务功能分别收集的个人信息的目的、方式、种类，调用权限名称、频度，收集使用敏感个人信息的必要性以及对个人权益的影响。涉及敏感个人信息的，需明确标识或突出显示；

3） 个人信息收集方式、存储期限、涉及数据出境情况等；

4） 对外提供、转移、公开个人信息的目的、涉及的个人信息种类、接收个人信息的第三方类型，以及各自的安全和法律责任；

5） 嵌入软件开发工具包的，应以结构化清单形式列明使用的第三方服务或嵌入的软件开发工具包名称（包名）、版本、主要功能、运营者名称或者姓名、收集使用个人信息的种类和完整的软件开发工具包个人信息收集使用规则链接；

6） 个人信息主体的权利和实现机制，如查询方法、更正方法、删除方法、注销账号的方法、撤回授权同意的方法、获取个人信息副本的方法、对信息系统自动决策结果进行投诉的方法等；

7） 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；

8） 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；

9） 处理个人信息主体询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式。

b） 个人信息处理规则所告知的信息应真实、准确、完整；

c） 个人信息处理规则的内容应清晰易懂，符合通用的语言习惯，使用标准化的数字、图示等，避免使用有歧义的语言；

d） 个人信息处理规则应公开发布且易于访问，例如，在网站主页、移动应用程序安装页、交互界面或设计等显著位置设置链接；采用隐私清单的方式辅助个人信息主体理解等；

e） 个人信息处理规则应逐一送达个人信息主体。当成本过高或有显著困难时，可以公告的形式发布；

注 1：面向个人提供服务的互联网应用程序在首次启动时，宜通过弹窗等显著方式向用户告知个人信息收集使用规则，并在用户充分知情的前提下，取得用户同意规则的明确表示。

f） 在本条 a）所载事项发生变化时，应及时更新个人信息处理规则并重新告知个人信息主体；

注 2：许多组织将个人信息处理规则命名为个人信息保护政策、隐私政策。

注 3：个人信息处理规则内容的撰写方法和相关内容结构可参考 GB/T 44588-2024，不满十四周岁未成年人专门的个人信息处理规则可参考 GB/T AAAA-AAAA。

注 4：在个人信息主体首次打开产品或服务、注册账号等情形时，宜通过弹窗等形式主动向其展示个人信息处理规则的主要或核心内容，帮助个人信息主体理解该产品或服务的个人信息处理范围和规则，并决定是否继续使用该产品或服务。不涉及收集或处理用户个人信息的节点除外。

注 5：若业务功能涵盖多个关联产品（如同一主体运营的不同 App、小程序、网站或服务模块），各产品的个人信息处理规则需保持内容与其产品功能的一致性和准确性，避免产生由功能差异导致的个人信息处理规则矛盾，如共用一份个人信息处理规则，需要进行差异化说明。

g） 智能终端的个人信息处理规则在网络或产品说明书等渠道上可以便捷查询；

h） 保留个人信息处理规则的历史版本供个人信息主体查阅。

6.5 同意的例外

存在本标准 5.3 至 5.8 规定的其他合法性基础时，个人信息处理者收集个人信息不必取得个人信息主体的同意。

6.6 敏感个人信息的收集

个人信息处理者在收集敏感个人信息前，除符合上述个人信息收集要求外，应符合 GB/T 45574-2025 第 5 章、第 6 章中敏感个人信息收集相关要求。

6.7 人工智能类产品或服务的收集

收集的要求包括：

a） 人工智能产品或服务如提供人脸、人声等生物识别信息编辑类深度合成功能的，应显著提示个人信息主体并取得其单独同意；

b） 人工智能产品或服务使用个人信息开展预训练、优化训练的，应显著告知处理目的、方式和影响范围，并取得个人同意。法律法规要求应取得单独同意的，应取得个人的单独同意，用户拒绝不应影响产品或服务基本功能的正常使用。人工智能产品或服务应提供撤回同意的途径或方式；

c） 人工智能产品或服务调用其他服务实现功能的：

1） 其他服务提供主体与人工智能服务为同一主体的，可直接通过人工智能产品或服务界面取得个人信息主体同意；

2） 其他服务提供主体为第三方主体的，根据业务场景判定数据处理关系和各方法律责任，具体可参考 GB/T XXXX-XXXX《数据安全技术 数据提供、委托处理、共同处理安全指南》国家标准，其他服务个人信息处理者应在首次提供服务时获取个人信息主体授权同意。

6.8 终端类产品或服务的收集

收集的要求包括：

a） 对于本身无用户交互界面或用户交互界面有限的产品（如智能监控摄像头、门锁、音箱、手表、手环等），如有配套使用的应用程序或在线网页，应在用户首次使用前通过配套使用的应用程序或在线网页，通过弹窗等显著方式呈现个人信息处理规则，并引导用户阅读；如没

有配套使用的应用程序或在线网页等，可通过用户手册等使用说明线下呈现个人信息处理规则；

b） 应在安装图像采集设备的公共区域设置显著的提示标识，告知个人信息主体该区域正在进行视频图像信息收集；

c） 在使用智能终端的过程中，采集到非必要个人信息或者未能取得个人信息主体同意的，个人信息处理者应当及时删除个人信息或者进行匿名化处理。

7 个人信息的存储

7.1 个人信息存储时间最小化

对个人信息处理者的要求包括：

a） 个人信息的保存期限应当为实现处理目的所必要的最短时间，且应根据处理目的的变更、业务需求的变化以及法律法规的更新等因素，动态评估并适时调整存储期限。当处理目的已达成或无法达成时，应及时删除个人信息或匿名化处理；

b） 超出 7.1 a)中个人信息存储期限的，应对个人信息进行删除或匿名化处理；

c） 存储个人信息的电子产品应具备循环覆盖、格式化、控制删除等清理数据的能力，电子产品的数据清除能力应符合 GB 46864-2025 的相关要求。

7.2 去标识化处理

个人信息处理者在收集个人信息后，应根据个人信息的类型、敏感程度以及后续处理目的，在个人信息用于统计分析、学术研究、提供披露或超出原始收集目的等场景前，应及时进行去标识化处理，以降低个人信息被直接或间接识别的风险，确保处理后的信息在不借助额外信息的情况下无法识别或关联到特定个人信息主体。

a） 应建立规范的去标识化流程，包括确定处理目标、识别标识符、选择技术方法、实施处理以及验证效果等步骤；

b） 应根据数据类型、业务场景和安全需求，选择适当的去标识化技术；

c） 在选择和应用去标识化技术时，应充分考虑其对数据可用性和分析价值的影响，及抵御潜在的攻击的有效性；

d） 对处理后的数据集进行系统性的效果评估，以验证其是否达到预期的去标识化目标；

e） 应根据评估结果，判断重标识风险是否在可接受的水平，若风险超出阈值，应重新选择或组合使用去标识化技术，并再次进行评估，直至风险降至可接受范围；评估过程和结果应形成书面记录，并妥善保存；

f） 应采取严格的技术和管理措施，将可用于恢复识别个人的信息（如密钥、映射表等）与去标识化后的信息分开存储。对恢复信息的访问应建立严格的访问控制策略，遵循最小必要原则，仅授权给因业务需要确需访问的特定人员，并对所有访问行为进行详细记录和审计；

g） 应建立去标识化处理活动的完整记录，记录内容至少应包括：处理的数据集、采用的技术方法及参数、处理的时间、操作人员、效果评估报告以及后续的任何变更记录；

h） 应定期对去标识化处理的有效性进行内部审计，检查技术措施是否按预期执行、访问控制策略是否得到遵守、评估结果是否准确等。审计发现的问题应及时整改，并留存整改记录。

7.3 敏感个人信息的传输和存储

个人信息处理者应在符合 GB/T 45574-2025 中 5.5 节要求的基础上，符合以下要求：

a） 传输和存储敏感个人信息时，应采用加密等安全措施；
b） 存储个人生物识别信息时，应采用技术措施确保信息安全后再进行存储，例如将个人生物识别信息的原始信息和摘要分开存储，或仅收集、存储、使用摘要信息。

7.4 个人信息处理者停止运营

当个人信息处理者停止运营其产品或服务时，应：
a） 及时停止继续收集个人信息；
b） 将停止运营的通知以逐一送达或公告的形式通知个人信息主体；
c） 对其所持有的个人信息进行删除或匿名化处理；
d） 法律、行政法规另有规定的，从其规定。

8 个人信息的使用

8.1 个人信息使用的目的限制

对个人信息处理者的要求包括：
a） 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。因业务需要确需超出原处理目的、处理方式或处理范围使用个人信息的，应重新确定合法性基础，依法重新告知个人信息主体。以个人同意作为合法性基础的，应重新取得个人同意，法律法规要求单独同意或书面同意的，从其规定；
b） 如所收集的个人信息进行加工处理而产生的信息，能够单独或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，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敏感个人信息的，对其处理应符合 GB/T 45574 的要求。

8.2 个人信息访问控制措施

对个人信息处理者的要求包括：
a） 对被授权访问个人信息的人员，应建立最小授权的访问控制策略，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；
b） 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；
c） 对安全管理人员、数据操作人员、审计人员的角色进行分离设置；
d） 确因工作需要，需授权特定人员超权限处理个人信息的，应经个人信息保护负责人或个人信息保护工作机构或对应的审批流程进行审批，并记录在册；
e） 对敏感个人信息的访问、修改等操作行为，宜在对角色权限控制的基础上，按照业务流程的需求触发操作授权。例如，当收到客户投诉，投诉处理人员才可访问该个人信息主体的相关信息。

8.3 个人信息的展示限制

涉及通过界面展示个人信息的（如显示屏幕、纸面），个人信息处理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。对个人信息处理者的要求包括：
a） 面向大范围公众展示个人信息的，应仅展示业务所需最小范围的个人信息字段，对个人姓名、身份证件号码、电话号码等直接标识符进行去标识化展示；

b） 面向个人信息主体展示个人信息的，应对敏感个人信息去标识化展示，完整个人信息仅个人信息主体选择展示后呈现，默认关闭截屏、录屏或对敏感信息复制、打印等功能或操作；

c） 面向个人信息处理者内部展示用户个人信息的，应根据业务场景和个人信息保护影响评估结果采取相应的去标识化措施。

8.4 基于不同业务目的所收集的个人信息的汇聚融合

对个人信息处理者的要求包括：

a） 遵守本标准 8.1 的要求；

b） 根据汇聚融合后个人信息所用于的目的，开展个人信息保护影响评估，采取有效的个人信息保护措施；

c） 将个人自行公开或者其他已经合法公开的个人信息汇聚融合用于模型训练前，应对其来源和内容进行审查与风险评估，并采取去标识化措施；

d） 对于可直接识别特定自然人身份的个人信息，应进行去标识化处理；

e） 应建立健全模型输出审核机制，降低模型输出或被诱导输出真实、可识别的个人信息。

8.5 自动化决策和人工智能的使用

8.5.1 用户画像的使用限制

对个人信息处理者的要求包括：

a） 用户画像中对个人信息主体的特征描述，不应：

1） 包含淫秽、色情、赌博、迷信、恐怖、暴力的内容；

2） 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，不应：

1） 侵害公民、法人和其他组织的合法权益；

2） 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。

c） 除为达到个人信息主体授权同意的使用目的所必需外，使用用户画像时应消除明确身份指向性，避免精确定位到特定个人。例如，为准确评价个人信用状况，可使用直接用户画像，而用于推送商业广告目的时，则宜使用间接用户画像。

8.5.2 个性化展示的使用

对个人信息处理者的要求包括：

a） 在向个人信息主体提供业务功能的过程中使用个性化展示的，应显著区分个性化展示的内容和非个性化展示的内容；

注 1：显著区分的方式包括但不限于：标明“定推”等字样，或通过不同的栏目、版块、页面分别展示等。

b） 在向个人信息主体提供电子商务服务的过程中，根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的个性化展示的，应当同时向该消费者提供不针对其个人特征的选项；

注 2：基于个人信息主体所选择的特定位置进行展示、搜索结果排序，且不因个人信息主体身份不同展示不一样的内容和搜索结果排序，则属于不针对其个人特征的选项。

a） 在向个人信息主体推送新闻信息服务的过程中使用个性化展示的，应：

1） 为个人信息主体提供简单直观的退出或关闭个性化展示模式的选项；

2） 当个人信息主体选择退出或关闭个性化展示模式时，向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。

b） 在向个人信息主体提供业务功能的过程中使用个性化展示的，应建立个人信息主体对个性化展示所依赖的个人信息（如标签、画像维度等）的管理机制，保障个人信息主体对个性化展示相关程度进行调控的能力。

8.5.3 信息系统自动决策机制的使用

个人信息处理者业务运营所使用的信息系统，具备自动决策机制且能对个人信息主体权益造成显著影响的（例如自动决定个人征信及贷款额度，或用于面试人员的自动化筛选等），应符合 GB/T 45392，并符合以下要求：

a） 保证决策的透明度和结果公平、公正，不应对个人在交易价格等交易条件上实行不合理的差别待遇；

b） 在规划设计阶段或首次使用前开展个人信息保护影响评估，并依据评估结果采取有效的保护个人信息主体的措施；

c） 在使用过程中定期开展个人信息保护影响评估，并依据评估结果改进保护个人信息主体的措施；

d） 向个人信息主体提供针对自动决策结果的投诉渠道，并对自动决策结果进行人工复核。

8.5.4 生成式人工智能的使用

个人信息处理者业务运营所使用的信息系统，接入大语言模型或使用大语言模型提供服务的智能体处理个人信息，且可能会对个人信息主体权益重大影响活动（如输出个人信息）的，要求包括：

a） 应事先并定期开展个人信息保护影响评估，确保采取的安全措施和风险程度相适应；

b） 应建立便捷的反馈渠道，接收可能受影响的个人信息主体要求，删除或限制信息系统输出相关信息。收到个人信息主体请求后 15 个工作日内，应完成核验及删除工作；

c） 应建立健全输出内容审核及风险监测措施，降低输出不当内容的风险；

d） 宜建立识别和过滤机制，对训练数据中无授权或个人信息主体明确拒绝的个人信息进行识别和过滤，并能优化参数防止输出。

8.6 统一账号体系的使用

个人信息处理者使用统一账号体系，应符合以下要求：

a） 应制定专门的个人信息处理规则，并在具体产品或服务的个人信息处理规则中向个人信息主体告知统一账号关联的个人信息的种类、目的、处理方式等，敏感个人信息、统一账号间个人信息提供情况应采用明确标识或突出显示；

b） 基于统一账号的单独产品或服务收集、处理的个人信息宜分开存储；

c） 应在产品或服务中提供单独产品或服务账号信息的查询、复制、修改等响应能力或入口；

d） 个人信息主体对统一账号的信息关联展示、处理提出质疑的，应向个人信息主体做合理说明；

e） 除注销统一账号外，应为个人信息主体提供删除单独产品或服务上的使用数据、注销单独产品或服务账号的途径；

f） 个人信息主体申请删除单独产品或服务数据的，不影响统一账号下的其他数据继续保留；

g） 两个及以上账号间提供个人信息的，应遵循本标准第 4 章的基本原则，超出原有范围或改变处理目的的，应按照本标准 6.3 要求取得个人信息主体同意；

h） 应定期对账号间提供的个人信息情况进行审查，及时调整个人信息使用策略。

9 个人信息主体的权利

9.1 个人信息查询

个人信息处理者应向个人信息主体提供查询下列信息的方法：

a） 基于所持有的关于该主体的个人信息或个人信息的类型；

b） 上述个人信息的来源、所用于的目的；

c） 已经获得上述个人信息的第三方身份或类型。

注：个人信息主体提出查询非其主动提供的个人信息时，个人信息处理者可在综合考虑不响应请求可能对个人信息主体合法权益带来的风险和损害，以及技术可行性、实现请求的成本等因素后，作出是否响应的决定，并给出解释说明。

9.2 个人信息更正

个人信息主体发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。个人信息处理者收到请求后，应核对个人信息来源，确认存在错误或不完整的，应及时更正、补充；无法核对的，应告知个人无法更正的原因。个人信息主体应提供准确的更正信息及相关证明，个人信息处理者应在15个工作日内完成更正，并告知个人更正结果。

9.3 个人信息删除

对个人信息处理者的要求包括：

a） 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） 处理目的已实现、无法实现或者为实现处理目的不再必要；

2） 个人信息处理者停止提供产品或者服务，或者保存期限已届满；

3） 个人撤回同意；

4） 个人信息处理者违反法律法规规定，收集、使用个人信息的；

5） 个人信息处理者违反与个人信息主体的约定，收集、使用个人信息的。

b） 个人信息处理者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提供、转移个人信息，个人信息处理者应立即停止提供、转移的行为，并通知第三方及时删除；

c） 个人信息处理者违反法律法规规定或违反与个人信息主体的约定，公开个人信息，个人信息处理者应立即停止公开的行为，并发布通知要求相关接收方删除相应的信息。

d） 个人信息处理者需使用个人信息继续为个人信息主体提供产品或服务的，当个人信息主体要求删除个人信息时，个人信息处理者应向个人信息主体说明。如个人信息主体仍要求删除，可引导个人信息主体注销产品或服务。

e） 当符合以上情形依法进行删除时，应采用以下方法之一或其组合，确保个人信息不可恢复：

1） 对存储媒体按照GB46864-2025要求进行信息清除；

2） 对于备份、容灾或归档数据，可通过备份周期覆盖、数据隔离或去标识化等技术方式确保其无法被重新使用；

3） 对个人信息进行匿名化处理，完成后对匿名化处理效果进行评估。

9.4 个人信息主体撤回授权同意

对个人信息处理者的要求包括：

a） 应向个人信息主体提供撤回收集、使用其个人信息的授权同意的方法。撤回授权同意后，个人信息处理者在获得合法依据前不应再处理相应的个人信息；
b） 应按照收集个人信息情况，提供撤回授权同意的途径和方式，且撤回同意的途径和方式与收集个人信息的打开方式同样便捷；
c） 应保障个人信息主体拒绝接收基于其个人信息推送商业广告的权利。对外提供、转移、公开个人信息，应向个人信息主体提供撤回授权同意或删除个人信息的方法。

注：撤回授权同意不影响撤回前基于授权同意的个人信息处理。

9.5 个人信息主体注销账号

对个人信息处理者的要求包括：

a） 通过注册账号提供服务的个人信息处理者，应向个人信息主体提供注销账号的方法，且该方法应简便易操作；
b） 宜设置便捷的注销功能交互式页面，及时响应个人信息主体注销请求；
c） 受理注销账号请求后，需要人工处理的，在满足注销条件下，应在承诺时限内（不超过 15 个工作日）完成核查和处理；
d） 注销账号过程中进行身份核验需要个人信息主体重新提供的个人信息不应多于注册、使用等服务环节收集的个人信息；
e） 注销账号过程不应设置不合理的条件或提出额外要求增加个人信息主体义务，如注销单个账号强制注销多个产品或服务的账号，要求个人信息主体填写精确的历史操作记录作为必要注销条件等；
f） 注销账号的过程需收集敏感个人信息核验身份时，应明确对收集敏感个人信息后的处理措施，如达成目的后立即删除或匿名化处理等；
g） 个人信息主体注销账号后，应及时删除其个人信息或做匿名化处理；
h） 同一个人信息处理者或关联公司、集团内多个服务采用统一账号进行一体化管理的，应在个人信息处理规则中明确账号服务提供方，账号服务处理个人信息的目的、方式、范围；
i） 个人信息主体使用统一账号服务登录具体产品的，应允许个人信息主体选择注销统一账号，或者允许用户选择关闭统一账号在该产品的使用权限、删除仅用于此产品的用户数据等方式实现账号注销同等效果；
j） 法律、行政法规规定需要保存相应个人信息的，从其规定。

9.6 个人信息主体获取个人信息副本

根据个人信息主体的请求，个人信息处理者应在验证个人真实身份后，为个人信息主体提供获取以下类型个人信息副本的方法，或在技术可行的前提下直接将以下类型个人信息的副本传输给个人信息主体指定的第三方，个人信息副本应是便于个人信息主体阅读的数据格式。

a） 本人的基本资料、身份信息；
b） 本人的健康生理信息、教育工作信息。

9.7 响应个人信息主体的请求

对个人信息处理者的要求包括：

a） 在验证个人信息主体身份后，应及时响应个人信息主体基于本标准 9.1 至 9.6 提出的请求，应在 15 个工作日内或法律法规规定的期限内作出答复及合理解释，并告知个人信息主体外部纠纷解决途径；

b） 直接在产品或服务提供的界面中设置专门的功能或选项，便于个人信息主体在线行使其访问、更正、删除、撤回授权同意、注销账号等权利；
c） 直接实现个人信息主体的请求需要付出高额成本或存在其他显著困难的，个人信息处理者应向个人信息主体提供替代性方法，以保护个人信息主体的合法权益；
d） 以下情况可不响应个人信息主体基于本标准 9.1 至 9.6 提出的请求，包括：
   1） 与个人信息处理者履行法律法规规定的义务相关的；
   2） 与国家安全、国防安全直接相关的；
   3） 与公共安全、公共卫生、重大公共利益直接相关的；
   4） 与刑事侦查、起诉、审判和执行判决等直接相关的；
   5） 个人信息处理者有充分证据表明个人信息主体存在主观恶意或滥用权利的；
   6） 出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；
   7） 响应个人信息主体的请求将导致个人信息主体或其他个人、组织的合法权益受到严重损害的；
   8） 所采集信息的范围与场地为私人环境，或影响私人隐私等。
e） 如决定不响应个人信息主体的请求，应向个人信息主体告知该决定的理由，并向个人信息主体提供投诉的途径。
f） 自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使查阅、复制、更正、删除等权利，但死者生前另有安排的除外。近亲属行使权利时，应提供死亡证明、亲属关系证明等材料，个人信息处理者应在 15 个工作日内响应，无法响应的需告知延迟原因及预计处理时间。

9.8 投诉管理

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。

10 个人信息的委托处理、提供、转移、公开

10.1 委托处理

个人信息处理者委托第三方处理个人信息时，应符合以下要求：
a） 个人信息处理者作出委托行为，不应超出已征得个人信息主体授权同意的范围或应遵守本标准 6.5 所列情形；
b） 个人信息处理者应对委托行为进行个人信息保护影响评估，确保受委托者达到本标准 13.6 的数据安全能力要求；
c） 受委托者应：
   1） 严格按照个人信息处理者的要求处理个人信息。受委托者因特殊原因未按照个人信息处理者的要求处理个人信息的，应及时向个人信息处理者反馈；
   2） 受委托者确需再次委托时，应事先征得个人信息处理者的授权。受委托者发生变更时应及时告知个人信息处理者；
   3） 协助个人信息处理者响应个人信息主体基于本标准 9.1 至 9.6 提出的请求；
   4） 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，应及时向个人信息处理者反馈；
   5） 在委托关系解除时删除个人信息或匿名化处理。

d） 个人信息处理者应对受委托者进行监督，方式包括但不限于：
   1） 通过合同等方式规定受委托者的责任和义务；
   2） 对受委托者开展检查。
e） 个人信息处理者应准确记录和存储委托处理个人信息的情况；
f） 个人信息处理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安全保护责任的，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（例如更改口令、回收权限、断开网络连接等）控制或消除个人信息面临的安全风险。必要时个人信息处理者应终止与受委托者的委托关系，并要求受委托者及时删除从个人信息处理者获得的个人信息。

10.2 个人信息提供

个人信息处理者提供个人信息时，应充分评估风险。提供个人信息，非因收购、兼并、重组、破产等原因的，应符合以下要求：

a） 事前开展个人信息保护影响评估，并依评估结果采取有效的保护个人信息主体的措施；
b） 基于个人同意处理个人信息的，向个人信息主体告知提供个人信息的目的、接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类以及可能产生的后果，并取得个人信息主体的单独同意。提供经去标识化处理的个人信息，且确保接收方无法重新识别或者关联个人信息主体的除外；
c） 接收方应在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应按照本标准 6.3 要求取得个人同意；
d） 通过合同等方式规定接收方的责任和义务；具体可参考 XXXX-XXXX《数据安全技术 数据提供、委托处理、共同处理安全指南》国家标准；
e） 准确记录和存储个人信息的提供情况，包括提供、转移的日期、规模、目的，以及接收方基本情况等；
f） 因提供个人信息发生安全事件而对个人信息主体合法权益造成损害的，个人信息处理者应承担相应的责任；
g） 个人信息处理者发现接收方违反法律法规要求或双方约定处理个人信息的，应立即要求数据接收方停止相关行为，且采取或要求数据接收方采取有效补救措施（例如更改口令、回收权限、断开网络连接等）控制或消除个人信息面临的安全风险；必要时个人信息处理者应解除与数据接收方的数据合作关系，并要求数据接收方及时删除从个人信息处理者获得的个人信息。

10.3 收购、兼并、重组、破产时的个人信息转移

当个人信息处理者发生收购、兼并、重组、破产等变更时，个人信息处理者应：

a） 向个人信息主体告知有关情况；
b） 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，应重新取得个人信息主体的明示同意；
c） 如破产且无承接方的，应删除个人信息或匿名化处理。

10.4 个人信息公开

个人信息原则上不应公开。个人信息处理者经法律授权或具备合理事由确需公开时，应符合以下要求：

a） 事前开展个人信息保护影响评估，并依评估结果采取有效的保护个人信息主体的措施；
b） 向个人信息主体告知公开个人信息的目的、类型，并取得个人信息主体单独同意；
c） 公开敏感个人信息前，除 10.4 b）中告知的内容外，还应通过明显提示的方式向个人信息主体告知涉及的敏感个人信息的内容；
d） 准确记录和存储个人信息公开情况，包括公开的日期、规模、目的、公开范围等；
e） 承担因公开个人信息而对个人信息主体合法权益造成损害的相应责任；
f） 不应公开个人生物识别信息；
g） 不应公开我国公民的种族、民族、政治观点、宗教信仰等敏感个人信息的分析结果。

10.5 提供、转移、公开个人信息时的其他合法事由

以下情形中，个人信息处理者提供、转移、公开个人信息不必事先征得个人信息主体的授权同意：

a） 与个人信息处理者履行法律法规规定的义务相关的；
b） 与国家安全、国防安全直接相关的；
c） 与公共安全、公共卫生、重大公共利益直接相关的；
d） 与刑事侦查、起诉、审判和判决执行等直接相关的；
e） 出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；
f） 个人信息主体自行向社会公众公开的个人信息；
g） 从合法公开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。

10.6 共同个人信息处理者

对个人信息处理者的要求包括：

a） 个人信息处理者应在个人信息处理规则中说明共同处理个人信息的情况；
b） 当个人信息处理者与第三方为共同个人信息处理者时，个人信息处理者应通过合同等形式与第三方共同确定应符合的个人信息安全要求，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，并向个人信息主体明确告知；
c） 如未向个人信息主体明确告知第三方身份，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，个人信息处理者应承担因第三方引起的个人信息安全责任。

注： 如个人信息处理者在提供产品或服务的过程中部署了收集个人信息的第三方插件（例如网站经营者在其网页或应用程序中部署统计分析工具、软件开发工具包 SDK、调用地图 API 接口），且该第三方并未单独向个人信息主体征得收集个人信息的授权同意，则个人信息处理者与该第三方在个人信息收集阶段为共同个人信息处理者。

10.7 第三方接入管理

当个人信息处理者在其产品或服务中接入具备收集个人信息功能的第三方产品或服务且不适用本标准 10.1、10.5 和 10.6 的，对个人信息处理者的要求包括：

a） 建立第三方产品或服务接入管理机制和工作流程，必要时应建立安全评估等机制、设置接入条件；

注： 如独立的第三方服务提供者，其独立于个人信息处理者，有自己的个人信息处理目的、方式和规则。其收集和处理个人信息的行为不受个人信息处理者的直接控制，但需要遵循相关法律法规以及与个人信息处理者约定的安全保护义务等。

b） 应与第三方产品或服务提供者通过合同等形式明确双方的安全责任及应实施的个人信息安全措施；
c） 应向个人信息主体明确标识产品或服务由第三方提供；
d） 应妥善留存平台第三方接入有关合同和管理记录，确保可供相关方查阅；
e） 应要求第三方根据本标准相关要求向个人信息主体征得处理个人信息的授权同意，核验其实现的方式；
f） 应要求第三方产品或服务建立响应个人信息主体请求和投诉等的机制，并告知用户、及时更新，以供个人信息主体查询、使用；
g） 应督促第三方产品或服务提供者加强个人信息安全管理，发现第三方产品或服务没有落实安全管理要求和责任的，应及时督促整改，必要时停止接入；
h） 涉及第三方嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包、小程序等）的，宜：
   1） 开展技术检测确保其个人信息收集行为符合约定要求；
   2） 对第三方嵌入或接入的自动化工具收集个人信息的行为开展检查，发现超出约定的行为，及时切断接入。

10.8 个人信息跨境传输

个人信息处理者将在中华人民共和国境内运营中收集和产生的个人信息向境外提供的，应按照相关法律、行政法规、部门规章、强制性国家标准等的要求，健全个人信息出境安全相关技术和管理措施，及时防范、处置个人信息违法违规出境安全风险和威胁。

11 海外法律管辖判定与冲突处理

11.1 海外法律管辖判定

11.1.1 管辖判定要素

个人信息处理活动涉及境外个人信息主体、境外实体、境外存储或计算资源、境外投放、境外监测、向境外提供个人信息，或者可能触发境外法律域外适用的，个人信息处理者应开展目标法域管辖判定，判定要素至少应包括：

a） 属地要素：关键处理环节发生地（收集、存储、使用、对外提供）、本地实体或雇员、数据中心或云计算结算地域；
b） 效果要素：是否有意针对目标法域的个人信息主体，典型标志包括使用当地语言、币种、配送承诺，在当地投放广告或提供售后，持续跟踪定位等；
c） 属人要素：处理者或其实际控制的境外实体与目标法域公司的设立与经营关联；
d） 行业专项规则：金融、电信、商业交易等特定场景的域外规定。

11.1.2 综合判定与记录

当属地、效果、属人等多种要素同时存在时，个人信息处理者应基于当地法律要求，识别需要考虑的要素，必要时综合各要素权重进行判定，并形成书面论证，作为个人信息处理活动记录与个人信息保护影响评估的前置条件和上线放行依据。

11.1.3 排除情形

除非当地法律明确规定，个人信息处理者不应仅以“未在当地设立实体”或“未直接收取对价”为由，否定目标法域的域外适用。

11.2 法律冲突识别与分层处置

11.2.1 法律冲突类型

个人信息处理者应建立法律冲突识别机制，至少识别以下类型冲突：

a） 直接对立型，例如一方法域强制传输或提供个人信息与他方法域禁止出境或限制提供之间的冲突；

b） 标准不一致型，例如敏感信息定义、同意门槛、跨境机制、存证要求等存在差异；

c） 程序性差异型，例如报告时限、在地代表或代理、备案登记等流程性差异。

11.2.2 法律冲突处置的优先顺序与措施

个人信息处理者在识别法律冲突后：

a） 在不违反中华人民共和国法律、行政法规以及主管机关要求的前提下，宜按照以下处置顺序：优先考虑当地强制性法律规范的要求处理相关事务；当当地法律规范不明确或存在模糊空间时，优先考虑可能导致显著处罚或禁令风险的规范；如前述两种情况均无法适用时，可考虑通过合同约束或行业自律承诺解决冲突；当以上方式均无法提供明确指引时，宜参考国际标准或行业最佳实践。

b） 可考虑综合采取以下措施：

1） 地域差分与隔离：逻辑或物理地域实例化或分区，将数据处理活动在地化，数据本地加工后聚合输出，避免不必要的跨境传输；

2） 最小化与去标识化：实施数据最小化原则，降低数据粒度，对非必须识别的数据进行去标识化或假名化处理，以降低数据敏感度和风险；

3） 机制替代与多轨并行：针对不同目标法域，分别选择适用的跨境传输机制，并准备必要的补充措施；

4） 政府请求应对：建立明确的跨境数据政府请求评估流程，包括政府请求合法性审查、请求范围的最小化审查、合作方及个人信息主体的通知义务以及必要时的救济措施；

5） 第三方风险管理：对第三方提供的数据处理服务和技术工具（如 SDK、API 等）进行风险评估，建立第三方合规审计和监控机制，确保第三方行为符合目标法域要求；

6） 透明度与沟通：发布透明度报告，明确跨境数据处理情况、相关法律风险与冲突处置方案，向利益相关方和公众公开；

7） 合规证据留存：建立跨境数据处理合规管理台账，系统记录法律冲突识别、评估与处置全过程，形成完整证据链。

11.3 合规流程与证明

11.3.1 专项评估

对于首次进入目标法域、重大变更或新增对外提供或监测行为的活动，个人信息处理者应在上线前完成管辖判定、法律冲突识别与跨境适配方案的一体化评估，并纳入个人信息保护影响评估报告。

11.3.2 记录与一致性

合法性基础、管辖判定、跨境机制、补充措施与政府请求应对策略，应在个人信息处理活动记录中结构化、版本化保存，并与个人信息处理规则、合同条款保持一致。

11.3.3 评估与监控

个人信息处理者对关键处理活动应定期评估；对高风险跨境活动宜至少每年评估一次，并在目标法域规则更新或执法趋势变化时及时触发重新评估与整改。

11.4 组织与职责

个人信息处理者应：

a） 指定跨境合规负责人，确定法务、数据、安全具体职责，建立个人信息处理情况记录，包括：目标法域、业务、数据、机制、证据等；

b） 涉及第三方或 SDK、广告网络的，落实第三方接入管理、合同约束与审计，发现超范围处理应及时终止接入；

c） 建立政府数据请求响应机制与透明度报告制度，保存法律依据、请求范围、响应决定与技术处置证据。

12 个人信息安全事件处置

12.1 个人信息安全事件应急处置和报告

对个人信息处理者的要求包括：

a） 应制定个人信息安全事件应急预案；

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） 发生个人信息安全事件后，个人信息处理者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，涉及的个人信息及人数，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） 按照国家网络安全事件相关法律法规及时上报，报告内容包括但不限于：涉及个人信息主体的类型、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） 个人信息安全事件可能会给个人信息主体的合法权益带来严重危害的，如敏感个人信息的泄露，按照本标准 12.2 的要求实施安全事件的告知。

d） 根据相关法律法规变化情况，以及事件处置情况，及时更新应急预案。

12.2 安全事件告知

对个人信息处理者的要求包括：

a） 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个人信息主体。难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息；

b） 告知内容应包括但不限于：

1） 安全事件的内容和影响；

2） 已采取或将要采取的处置措施；

3） 个人信息主体自主防范和降低风险的建议；
4） 针对个人信息主体提供的补救措施；
5） 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。

13 组织的个人信息安全管理要求

13.1 个人信息保护负责人

对个人信息保护负责人的要求包括

a） 满足以下条件之一的组织，应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督：
1） 被认定为大型网络平台的；
2） 主要业务涉及个人信息处理，且相关业务从业人员规模大于 200 人；
3） 处理超过 100 万人的个人信息；
4） 处理超过 10 万人的敏感个人信息的。

注 1：大型网络平台，是指注册用户 5000 万以上或者月活跃用户 1000 万以上，业务类型复杂，网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响的网络平台。

注 2：处理方式简单可不包括在内，如以保管为目的的学校或用人单位的人事档案管理情形。

b） 大型网络平台个人信息保护负责人的任职条件应符合相关法律法规、规章及监管要求。其他个人信息处理者指定个人信息保护负责人的，应由公司法定代表人或主要负责人担任，宜确保其具备个人信息保护专业知识、履职经验、组织协调能力和独立履职条件；法律法规另有规定的，从其规定。

c） 个人信息保护负责人的任职条件应包括但不限于：
1） 具有中华人民共和国国籍；
2） 不存在可能影响其独立、公正履行个人信息保护职责的违法犯罪记录或重大失信记录；
3） 与个人信息处理者之间存在具有法律效力的雇佣或委任协议；
4） 具备个人信息处理与保护的专业知识，熟悉相关法律法规，具有履行个人信息保护职责相关的管理经验；
5） 熟悉个人信息处理者的组织架构、股权结构、主营业务，掌握处理个人信息的信息系统、数据中心、传输链路情况、个人信息情况等；
6） 具有较强的综合分析、文字表达和沟通协调能力。

d） 个人信息保护负责人的职责应包括但不限于：
1） 全面统筹实施组织内部的个人信息保护工作，对个人信息保护负直接责任；
2） 组织制定个人信息保护工作计划并督促落实；
3） 制定、签发个人信息处理规则和个人信息保护规程；
4） 负责个人信息保护影响评估、个人信息处理者的个人信息保护合规审计工作；
5） 与履行个人信息保护职责的部门保持沟通，通报或报告个人信息保护和事件处置等情况；
6） 对其履行职责过程中掌握的信息保密；
7） 配合履行个人信息保护职责部门开展调查研究，为推进个人信息保护工作提出建议。

e） 个人信息保护负责人的基本权力和义务包括不限于：
1） 应参与有关个人信息处理活动的重要决策，直接向组织主要负责人报告工作；
2） 具有充分的权限协调个人信息处理者内部相关部门与人员完成个人信息保护工作；

3） 在个人信息处理重大事项决策前应有权提出相关意见和建议；
4） 应有权对个人信息处理者内部个人信息处理的不合规操作进行制止和采取必要的纠正措施；
5） 围绕个人信息保护工作开展向履行个人信息保护职责的部门提出意见建议；
6） 向内部个人信息保护工作人员提供接受专业培训的资源渠道和机会；
7） 参加履行个人信息保护职责的部门组织的个人信息保护有关学习培训、座谈研讨活动；

f） 个人信息保护负责人不设定任期，因工作需要或个人辞职等原因需更换个人信息保护负责人，个人信息处理者应在 30 个工作日内补任符合本标准 13.1a)-d)要求的个人信息保护负责人。

g） 个人信息处理者应为个人信息保护负责人开展工作提供必要的保障，包括不限于：
1） 个人信息处理者应明确其法定代表人或主要负责人对个人信息保护负有全面领导责任，包括为个人信息保护工作提供人力、财力、物力保障；
2） 个人信息处理者应为个人信息保护负责人和个人信息保护工作提供必要的资源，保障其独立履职；
3） 个人信息处理者应确保个人信息保护负责人以适当方式及时参与所有涉及个人信息保护的事宜；
4） 参与有关个人信息处理活动的重要决策直接向组织主要负责人报告工作。

h） 个人信息处理者应确保个人信息保护负责人的独立性：
1） 个人信息处理者应确保个人信息负责人在履行职责时不受个人信息处理者的任何指示或干涉；
2） 个人信息保护负责人不应因合法履行职责而被个人信息处理者解雇或处罚，个人信息保护负责人应直接向个人信息处理者的最高机构负责；
3） 个人信息保护负责人在同时承担其他职务时，应当确保相关职责不能影响其履行个人信息保护的职责，个人信息保护负责人不应担任与个人信息保护存在利益冲突的职务。

i） 非必须设立个人信息保护负责人的组织可参照 13.1.b)~h)的要求执行。

13.2 个人信息保护工作机构与人员

对个人信息处理者的要求包括：

a） 应明确其法定代表人或主要负责人对个人信息安全负全面领导责任，包括为个人信息安全工作提供人力、财力、物力保障等；

b） 应建立健全个人信息保护管理架构，设立个人信息保护工作机构，负责个人信息保护工作。各业务部门应根据业务规模、处理个人信息量级、敏感程度等因素合理配置本部门负责个人信息保护工作人员数量、能力，鼓励个人信息保护从业人员参与个人信息保护专项培训；

c） 满足以下条件之一的组织，应设立专职的个人信息保护工作机构：
1） 被认定为大型网络平台的；
2） 主要业务涉及个人信息处理，且相关业务从业人员规模大于 200 人；
3） 处理超过 100 万人的个人信息，或预计在 12 个月内处理超过 100 万人的个人信息；
4） 处理超过 10 万人的敏感个人信息的。

d） 个人信息保护工作机构的职责应包括但不限于：
1） 制定、实施、定期更新个人信息处理规则和相关规程；
2） 建立、维护和更新组织所持有的个人信息清单（包括个人信息的类型、数量、来源、接收方等）和授权访问策略；

3） 开展个人信息保护影响评估，提出个人信息保护的对策建议，督促整改安全隐患；
4） 定期组织开展个人信息保护培训，学习贯彻个人信息处理规则、文件；
5） 在产品或服务上线发布前进行检测，避免未知的个人信息收集、使用、提供等处理行为；
6） 公布投诉、举报方式等信息并及时受理投诉举报；
7） 定期进行个人信息保护合规审计；
8） 与监督、管理部门保持沟通，通报或报告个人信息保护和事件处置等情况。

e） 个人信息保护人员应定期接受个人信息保护教育培训。

13.3 个人信息安全工程

开发具有处理个人信息功能的产品和服务时，个人信息处理者宜按照 GB/T 41817 标准要求在需求、设计、开发、测试、发布等系统工程阶段考虑个人信息保护要求，保证在系统建设时对个人信息保护措施同步规划、同步建设和同步使用。

13.4 个人信息处理活动记录

13.4.1 一般要求

个人信息处理者应妥善记录个人信息处理活动，满足以下要求：

a） 个人信息处理活动记录覆盖个人信息处理活动的全生命周期；
b） 个人信息处理活动记录真实、准确、完整、及时更新，以实现可追溯、可审计、可证明。

13.4.2 适用范围

存在下列情形之一的，个人信息处理者应建立并维护个人信息处理活动记录：

a） 处理敏感个人信息；
b） 进行自动化决策；

注：如使用自动化决策对用户进行画像。

c） 委托处理个人信息、向其他个人信息处理者提供个人信息或公开个人信息；
d） 向境外提供个人信息；
e） 个人信息处理目的、处理方式、信息类型、处理场景发生重大变化；
f） 个人信息处理者内部人员查阅、复制个人信息；
g） 其他可能对个人权益产生重大影响的个人信息处理活动。

13.4.3 记录要求

个人信息处理活动记录应至少包括以下内容：

a） 个人信息处理者的名称或者姓名、联系方式；
b） 个人信息类别、处理目的、处理方式、处理的合法性基础和留存期限；
c） 涉及个人信息对外提供的，应记录接收方名称、联系方式和处理目的；
d） 涉及个人信息出境的，应记录出境的个人信息种类、处理目的、处理方式、接收国家或地区、接收方姓名或名称及联系方式、采用的出境机制（如安全评估、认证或标准合同）及备案情况；
e） 采取的安全技术措施和组织措施概述；
f） 涉及敏感个人信息的，应记录敏感个人信息的具体种类及必要性评估结果；

g） 涉及自动化决策或用户画像的，应记录决策或画像的逻辑、算法或模型类型及版本、公平性和透明性保障措施及申诉渠道；
h） 涉及个人信息委托处理的，应记录受托方名称、联系方式、合同编号、监督审计安排及受托方个人信息删除情况；
i） 涉及个人信息公开的，应记录个人信息公开的日期、规模、目的、范围、渠道和频率等；
j） 个人信息主体行使权利的途径和联系方式，以及个人信息投诉举报行权记录；
k） 个人信息保护影响评估报告、结论及风险处置措施；
l） 个人信息安全事件及处置措施；
m） 个人信息处理的审批记录；
n） 个人信息处理活动操作人员的姓名、职务、联系方式等；
o） 个人信息处理规则的历史版本和版本变更记录。

13.4.4 记录维护

个人信息处理者和受托处理个人信息的主体应：
a） 明确记录维护责任人，并采取适当的管理和技术措施，确保记录及时更新、准确完整；
b） 处理活动发生变更后，应在变更生效前及时更新相关记录。
c） 应每年至少复核一次记录，对高风险个人信息处理活动应每半年复核一次。

13.4.5 记录保存

个人信息处理活动记录的最新版本及历史版本应至少保存三年，法律法规另有规定的从其规定。

13.4.6 可用性

个人信息处理活动记录应采用电子化、结构化和可机读的方式保存，能够在监管检查或个人信息主体请求时及时提供。

13.5 个人信息保护影响评估

13.5.1 一般要求

个人信息处理者应建立个人信息保护影响评估制度，基于本标准 13.4 中的个人信息处理活动记录，将个人信息保护影响评估作为个人信息处理活动启动、重大变更和终止管理的前置条件，实现可核验、可追溯、可审计的合规证据链。

13.5.2 评估内容

个人信息保护影响评估应至少覆盖下列内容：
a） 合法性评估，个人信息处理活动是否符合本标准第 5 章的合法性基础；
b） 正当性评估，个人信息处理目的是否清晰、明确，不存在误导、诱导等情形，是否可以为个人信息主体创造价值，处理目的是否符合公序良俗，个人信息处理产生的其他正当利益是否与保护个人信息主体合法权益相冲突；

注：正当利益指对于维护其他主体或群体利益有正向帮助，如维护市场交易秩序、维护其他消费者重大利益、提高合法使用数据的价值。

c） 必要性评估，个人信息处理活动是否与处理目的直接相关，是否仅处理必要的个人信息，是否采取了最小影响的处理方式；

d） 风险源分析，从网络环境和技术措施、个人信息处理过程合规性、参与的人员、第三方和管理制度等方面，并结合业务特点、规模及安全态势，分析安全措施的有效性以及安全事件的可能性；

e） 权益影响分析，个人信息处理活动是否可能影响个人信息主体自主决定权、引发差别性待遇、名誉受损或遭受精神压力、人身与财产安全等方面，并描述影响和分析影响的程度；

f） 风险综合分析，结合权益影响分析、安全措施的有效性分析等结果，合理推断个人信息处理活动的风险。

13.5.3 评估场景

存在下列情形之一的，个人信息处理者应事前开展个人信息保护影响评估：

a） 处理敏感个人信息；

b） 利用个人信息实施自动化决策；

c） 委托处理、向其他个人信息处理者提供或公开个人信息；

d） 向境外提供个人信息；

e） 产品或服务发布前，或业务功能发生重大变更前；

f） 法律法规或监管要求发生变化；

g） 业务模式、信息系统或运行环境发生重大变更；

h） 发生重大个人信息安全事件或收到个人信息安全事件预警时。

如个人信息处理者已存在a）～d）的情形，但未事前开展个人信息保护影响评估的，应及时对当前个人信息处理活动进行评估。

13.5.4 评估管理

个人信息保护影响评估管理要求包括但不限于：

a） 个人信息保护负责人或工作机构识别应评估的个人信息处理活动，制定评估计划，对评估工作的完整性、有效性负责，并对评估过程实施监督；

b） 应根据GB/T 39335提出的方法制定评估方案、组建评估队伍，并实施个人信息保护影响评估；

c） 应保证评估工作的独立性、客观性、专业性，大型网络平台服务提供者、重要个人信息处理活动宜委托第三方实施个人信息保护影响评估；

注1：重要个人信息处理活动包括：处理1000万人个人信息、向第三方提供10万人个人信息、处理10万人敏感个人信息、处理1万人未成年人个人信息、向境外提供1万人个人信息等。

d） 评估结果显示存在严重风险、高风险情形的，个人信息保护负责人或工作机构应向相关方提出针对性的改进措施建议，并督促其及时改进；

e） 应形成个人信息保护影响评估报告，报告结果显示采取的安全措施与风险相适应的（如低风险或中风险但有明确改进和监督计划），个人信息保护负责人或工作机构方可批准产品或服务上线、变更或持续运行；

f） 应至少每年对生效的个人信息保护影响评估结论进行一次复核，触发13.5.3f）～g）时应立即对评估结论进行复核，复核应关注个人信息处理目的是否变化、权益影响分析准确性、控制措施有效性、风险状态变化、安全事件影响等；

g） 评估结论及改进措施建议宜经个人信息保护负责人或授权管理人批准后生效；

h） 个人信息保护影响评估报告及其相关证据应至少保存三年，并可供相关方查阅；对涉及面广、用户量大、社会关注度高或公共利益相关的处理活动，宜以适宜形式对外公开便于相关方了解评估工作开展情况。

注 2：公开形式包括评估报告的摘要或已开展评估的标识等。

i） 根据相关管理要求需将个人信息保护影响评估报告予以备案的，应将签章版报告予以备案；

j） 宜建立评估相关工具、系统，提升评估工作效率，并以电子化、结构化保存评估过程资料、证据文件及评估报告等，使其能够在监管检查或合规审计、个人信息主体权利请求处置中及时调用与出具。

13.6 数据安全能力

个人信息处理者应根据有关国家标准的要求，建立适当的数据安全能力，落实必要的管理和技术措施，防止个人信息的泄露、损毁、丢失、篡改。涉及敏感个人信息处理的个人信息处理者，宜符合 GB/T 37988 三级以上能力要求。

13.7 人员管理与培训

对个人信息处理者的要求包括：

a） 应与从事个人信息处理岗位上的相关人员签署保密协议，对大量接触敏感个人信息的人员进行背景审查，以了解其犯罪记录、诚信状况等；

b） 应明确内部涉及个人信息处理不同岗位的安全职责，建立发生安全事件的处罚机制；

c） 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；

d） 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；

e） 应建立相应的内部制度和政策对特殊岗位如个人信息保护负责人、法务、合规、产品、研发、测试等岗位人员提出产品/服务上线的个人信息保护的指引和要求；

f） 应定期（至少每年一次）或在个人信息保护相关法律法规、规章及规范性文件等要求发生重大变化时，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相关法律法规、规章及规范性文件等要求和相关规程。

13.8 个人信息保护合规审计

个人信息处理者应按照 GB/T 46903-2025《数据安全技术 个人信息保护合规审计要求》开展个人信息保护合规审计，个人信息保护合规审计流程包括审计准备、审计实施、审计报告、问题整改、归档管理 5 个阶段，对个人信息处理者的要求包括：

a） 应按照法律、行政法规要求定期对个人信息处理活动是否遵守法律、行政法规的情况进行个人信息保护合规审计，个人信息保护合规审计开展频率参考 GB/T 46903-2025 的要求；

b） 应保证提供的审计相关证明材料真实、完整、有效；

c） 提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应成立主要由外部成员组成的独立机构对个人信息保护合规审计情况进行监督；

d） 制定个人信息保护合规审计管理制度，明确开展个人信息保护合规审计的组织人员、方式方法、内容依据、范围频率等，以及合规审计人员的职责及权限；

e） 确保个人信息保护合规审计具备必要的资源及权限，包括合理的合规审计预算和人力资源计划，以及必要的办公场地、系统、设备等；

f） 确保个人信息保护合规审计活动的独立性，审计人员不应参与被审计对象的管理或决策，审计报告宜直接向董事会或安全合规委员会报告；自审计场景可通过成立独立的实体部门或虚拟项目组等方式执行，吸纳未直接参与业务个人信息保护相关业务工作的专业人员；

g） 建立健全个人信息保护管理制度、安全技术措施、处理情况记录、操作行为日志、监督检查记录、测试评价报告等合规审计证据体系，以供个人信息保护合规审计进行审查和评价；

h） 宜建立健全个人信息保护合规审计管理体系，及时发现和消除安全风险和弥补合规差距，在组织范围内对涉及的业务场景开展合规审计并进行持续监督；

i） 宜使用个人信息保护合规审计相关工具，提高个人信息保护合规审计工作效率和质量。

附 录 A
（资料性附录）个人信息示例

个人信息是指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，如姓名、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。个人信息的常见类型示例参见表 A.1。

判定某项信息是否属于个人信息，应考虑以下两条路径：

一是识别，即从信息到个人，持有、接收数据的一方，在现有技术条件下考虑到所有可合理使用的手段，由信息本身的特殊性识别出特定自然人，个人信息应有助于区分出特定个人。现有的技术条件，应当综合考虑法律法规与监管部门要求，相关国家标准的规定，以及实际识别的成本。如果持有、接收数据的一方，在现有技术条件下考虑到所有可合理使用的手段，都无法识别区分出特定自然人，则不适用识别的方法。

例如，可用于识别个人的信息示例，包括但不限于姓名、身份证号码、护照号码或生物识别数据。相反，如果一个列表仅包含信用评分，而没有关于这些评分所对应个人的任何附加信息，则该列表无法提供足够信息来识别特定个人。

二是与个人有实质关联的关联，即从个人到信息。当某项信息与特定个体关联时，即可认定该信息与该个体“有关”，可以通过信息的内容、目的、结果等要素判断是否关联：

a）内容要素：当信息的内容直接涉及特定自然人时，满足关联条件；

b）目的要素：当信息的使用目的旨在评估、影响特定自然人的状态或行为时，满足关联条件；

c）结果要素：当信息的使用可能对特定自然人的权益产生影响时，满足关联条件。

例如，可用于关联个人的信息示例，例如已知某个人，则该个人的位置信息、个人浏览记录等与其关联的信息也是个人信息。相反，如果一个列表仅包含有位置信息、浏览记录，而没有关于这些位置、记录所对应个人的任何附加信息，则该列表无法提供足够信息来关联特定个人。

符合上述两种情形之一的信息，均应判定为个人信息。

需说明的是，仅用于商业沟通、业务联络、企业间合作等合法商业目的的商业联系信息，不属于识别特定自然人身份或者反映特定自然人活动情况的个人信息。

具体包括：

（1）自然人在履行企业职务或个体经营过程中仅用于标识其职业身份职务或职称；

（2）用于企业间联系的固定办公电话、办公传真号码及其他专门用于商业联络的通讯账号；

（3）以企业域名为后缀的电子邮箱地址（如 name@company.com）；

（4）企业注册地址、官网链接等公开的企业联络信息。

前款所列信息若与其他可识别特定自然人的信息结合使用，导致可直接或间接识别自然人身份的，仍应适用个人信息保护的规定。

表 A.1 个人信息举例

个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮箱等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等

表 A.1 个人信息举例（续）

个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征、步态、眼纹等
网络身份标识信息	个人信息主体账号、单独可识别自然人的 IP 地址、邮箱地址、个人信息主体个人数字证书、用户标识符（用户 ID）等
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、医疗就诊记录、生育信息、既往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况产生的相关信息，以及体重、身高、体温、肺活量等
个人教育工作信息	个人职业、职位、职称、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等
个人财产信息	银行、证券等账户的账号、鉴别信息（密码、口令等）、存款信息（包括资金数量、支付收款记录等），个人收入状况、房产信息、信贷记录、征信信息、交易和消费记录（交易订单、交易金额等）、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
身份鉴别信息	账号口令、数字证书、短信验证码等用于个人身份鉴别的数据
个人通信信息	通信记录和内容、短信、彩信、话音、电子邮件、即时通信等通信内容（如文字、图片、音频、视频、文件等），以及描述个人通信的数据（通常称为元数据）等
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网页浏览记录、软件使用记录、点击记录、用户使用某业务的行为记录（如优秀业务中的用户游戏登陆时间、最近充值时间）、与智能系统的对话记录等
个人设备信息	指包括硬件序列号、设备 MAC 地址、可变更的唯一设备识别码（Android ID、广告标识符（IDFA）等）、不可变更的唯一设备识别码（如国际移动设备识别码（IMEI）等）、用户在终端上安装的应用程序列表（如每款应用软件的名称、版本等）等在内的描述个人常用设备基本情况的信息
个人位置信息	包括仅能定位到行政区、县级等的位置信息（如地区代码、城市代码等），与个人所处地理位置、活动地点和活动轨迹等相关信息，个人住宿信息，及乘坐飞机、火车、汽车、轮船等交通出行信息等，行踪轨迹、精准定位信息、住宿信息、经纬度等
个人标签信息	基于个人上网记录等加工产生的个人用户标签、画像信息，如行为习惯、兴趣偏好等
个人运动信息	步数、步频、运动时长等
其他个人信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等

附 录 B
（资料性附录）敏感个人信息判定

敏感个人信息是指一旦遭到泄露或非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。通常情况下，不满 14 周岁未成年人的个人信息和自然人的隐私信息属于敏感个人信息。可从以下角度判定是否属于敏感个人信息：

泄露：个人信息一旦泄露，将导致个人信息主体及收集、使用个人信息的组织和机构丧失对个人信息的控制能力，造成个人信息扩散范围和用途的不可控。某些个人信息在泄露后，被以违背个人信息主体意愿的方式直接使用或与其他信息进行关联分析，可能对个人信息主体权益带来重大风险，应判定为敏感个人信息。例如，个人信息主体的身份证复印件被他人用于手机号卡实名登记、银行账户开户办卡等。

非法提供：某些个人信息仅因在个人信息主体授权同意范围外扩散，即可对个人信息主体权益带来重大风险，应判定为敏感个人信息。例如，性取向、存款信息、传染病史等。

滥用：某些个人信息在被超出授权合理界限时使用（如变更处理目的、扩大处理范围等），可能对个人信息主体权益带来重大风险，应判定为敏感个人信息。例如，在未取得个人信息主体授权时，将健康信息用于保险公司营销和确定个体保费高低。

表 B.1 给出了敏感个人信息的示例。

表 B.1 敏感个人信息举例

类别	描述
生物识别信息	个人基因[a]、人脸[b]、声纹[c]、步态[d]、指纹、掌纹、眼纹、耳廓和虹膜等生物识别信息
宗教信仰信息	个人信仰的宗教、加入的宗教组织、宗教组织中的职位、参加的宗教活动和特殊宗教习俗等个人信息
特定身份信息	残障人士身份信息、不适宜公开的职业身份信息等个人信息
医疗健康信息	——与个人的身体或心理的伤害、疾病、残疾和疾病风险或隐私有关的健康状况信息[e]，如病症、既往病史、家族病史、传染病史、体检报告和生育信息等； ——在疾病预防、诊断、治疗、护理和康复等医疗服务过程中收集和产生的个人信息，如医疗就诊记录（如医疗意见、住院志、医嘱单、手术及麻醉记录、护理记录和用药记录）、检验检查数据（如检验报告和检查报告）等
金融账户信息	个人的银行、证券、基金、保险和公积金等账户的账号及密码，公积金联名账号、支付账号、银行卡磁道数据（或芯片等效信息）和基于账户信息产生的支付标记信息和个人收入明细等个人信息
行踪轨迹信息	连续精准定位轨迹信息、车辆行驶轨迹信息和人员连续的活动轨迹信息等个人信息
不满十四周岁未成年人个人信息	不满十四周岁未成年人的个人信息
其他敏感个人信息	精准定位信息[f]、居民身份证照片、性取向、性生活、征信信息、犯罪记录信息[g]和显示个人身体私密部位的照片或视频信息等个人信息
a 具体可参考 GB/T41806。 b 具体可参考 GB/T41819。 c 具体可参考 GB/T41807。 d 具体可参考 GB/T41773。 e 个人的体重、身高、血型、血压和肺活量等基本体质信息，如与个人的疾病和医疗就诊无关，则可认为不属于敏感个人信息范畴。	

表 B.1 敏感个人信息举例

f 通过调用个人移动通信终端精准位置权限采集的位置信息是精准定位信息，通过网络地址等测算的粗略位置信息不是精准定位信息，连续采集的精准定位信息可用于生成行踪轨迹。 g 犯罪记录，是指我国国家专门机关对犯罪人员的客观记载，如罪名和刑罚等记录。

附 录 C
（资料性附录）实现个人信息主体自主意愿的方法

保障个人信息主体自主意愿包括两个方面：一是不强迫个人信息主体接受多项业务功能；二是保障个人信息主体对个人信息收集、使用的知情权和授权同意的权利。个人信息处理者，尤其是移动应用程序运营者，可通过以下方式实现：

C.1 区分基本业务功能和扩展业务功能

保障个人信息主体选择同意的权利，首先需划分产品或服务的基本业务功能和扩展业务功能，划分的方法如下：

a） 应根据个人信息主体选择、使用所提供产品或服务的根本期待和最主要的需求，划定产品或服务的基本业务功能；

注 1：个人信息主体之所以识别或挑选某项产品或服务，主要依据个人信息处理者对所提供产品或服务开展的市场推广和商业定位、产品或服务本身的名称、在应用商店中的描述、所属的应用类型等因素。因此，个人信息处理者应根据一般个人信息主体对上述因素的最可能的认识和理解，而非自身想法来确定个人信息主体的主要需求和期待来划定基本业务功能。一般来说，如果产品或服务不提供基本业务功能，个人信息主体将不会选择使用该产品或服务。

注 2：随着产品或服务的迭代、拓展、升级等，基本业务功能可能需要随之重新划分。个人信息处理者仍应根据一般个人信息主体最可能的认识和理解，来重新划定基本业务功能。但个人信息处理者不应短时间内大范围改变基本业务功能和扩展业务功能的划分。在重新划分后，个人信息处理者应再次告知并征得个人信息主体对基本业务功能收集、使用其个人信息的明示同意。

b） 不应将改善服务质量、提升个人信息主体体验、研发新产品单独作为基本业务功能；

c） 将产品或服务所提供的基本业务功能之外的其他功能，划定为扩展业务功能。

C.2 基本业务功能的告知和明示同意

基本业务功能的告知和明示同意的实现方法如下：

a） 在基本业务功能开启前（如个人信息主体初始安装、首次使用、注册账号等），应通过交互界面或设计（如弹窗、文字说明、填写框、提示条、提示音等形式），向个人信息主体告知基本业务功能所必要收集的个人信息种类，以及个人信息主体拒绝提供或拒绝同意收集将带来的影响，并通过个人信息主体对信息收集主动作出肯定性动作（如勾选、点击“同意”或“下一步”等）征得其明示同意；

注 1：当产品或服务所提供的基本业务功能无需一次性全部开启时，应根据个人信息主体的具体使用行为逐步开启基本业务功能，并即时完成本条 a）的告知要求。

注 2：AI 助手个人信息收集的告知除以上方式外，还可采用语音、视频告知的方式，个人信息主体对信息收集也可通过语音、视频的方式进行反馈。

b） 个人信息主体不同意收集基本业务功能所必要收集的个人信息的，个人信息处理者可拒绝向个人信息主体提供该业务功能；

c） 本条 a）所要求的交互界面或设计应方便个人信息主体再次访问及更改其同意的范围。

注 3：上述要求的实现方式可参考附录 C.4。

C.3 扩展业务功能的告知和明示同意

扩展业务功能的告知和明示同意的实现方法如下：

a） 在扩展业务功能首次使用前，应通过交互界面或设计（如弹窗、文字说明、填写框、提示条、提示音等形式），向个人信息主体逐一告知所提供扩展业务功能及所必要收集的个人信息，并允许个人信息主体对扩展业务功能逐项选择同意；

b） 个人信息主体不同意收集扩展业务功能所必要收集的个人信息的，个人信息处理者不应反复征求个人信息主体的同意。除非个人信息主体主动选择开启扩展功能，在 24 小时内向个人信息主体征求同意的次数不应超过一次；

c） 个人信息主体不同意收集扩展业务功能所必要收集的个人信息的，不应拒绝提供基本业务功能或降低基本业务功能的服务质量；

d） 本条 a）所要求的交互界面或设计应方便个人信息主体再次访问及更改其同意的范围。

注：上述要求的实现方式可参考附录 C.4。

附 录 D
（资料性附录）合法性基础示例场景

个人信息处理者处理个人信息前应确定个人信息处理合法性基础，并向个人信息主体告知个人信息处理规则。处理个人信息的合法性基础场景示例如表 D.1 所示。

表 D.1 合法性基础示例场景

合法基础	示例场景	场景描述
为订立、履行个人作为一方当事人的合同所必需	电子商务合同订立和履行场景下的个人信息处理	卖家（电子商务经营者）发布的商品或者服务信息符合要约条件的，买家（用户）选择该商品或者服务并成功提交订单，买家与电子商务平台经营者的电子商务合同成立。为完成合同的订立与履行，电子商务平台经营者需处理用户的个人信息，并在必要范围内向相关第三方提供信息。 具体而言： —— 向卖家提供信息：包括订单信息、收件人信息、物流信息等，用于完成商品的发货与交付； —— 向电子支付服务提供者提供信息：包括支付账户信息、支付金额、支付时间等，用于完成交易支付； —— 向快递物流服务提供者提供信息：包括收件人信息、物流信息等，用于完成商品的运输与配送。
	机票预订服务场景下的个人信息处理	用户通过第三方票务平台选择航班、填写乘机人信息并成功提交订单，用户与第三方票务平台的电子商务合同成立。为完成合同订立与履行，第三方票务平台需处理用户的个人信息，并在必要范围内向相关第三方提供信息。 具体而言： —— 向卖家（机票渠道商）及航空公司提供信息：包括乘机人姓名、身份证件信息、联系方式、航班信息等，用于完成机票出票等服务。 —— 向支付服务提供者提供相应的支付信息，用于完成票款支付。 —— 向保险服务提供者提供信息（如适用）：在用户购买旅行保险的情况下，需提供乘机人信息、航班信息、保单信息等，用于保险承保与理赔。
	在线医疗服务预约与诊疗服务	用户通过互联网医疗平台预约医生、填写基本健康信息、提交就诊需求并完成订单支付，即构成用户与互联网医疗平台之间的服务合同关系。为完成合同的订立与履行，互联网医疗平台需依法处理用户的个人信息，并在必要范围内向相关第三方提供信息。 具体而言： —— 向医疗机构提供信息：包括用户姓名、联系方式、预约时间、就诊需求、健康状况等，用于安排医生接诊、匹配诊疗资源； —— 向支付服务提供者提供信息：包括支付账户信息、支付金额、支付时间等，用于完成服务费用的支付； —— 向快递物流服务提供者提供信息（如适用）：在用户购买药品的情况下，需提供收件人信息、物流信息等，用于完成药品配送。
按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需	处理员工的考勤记录	公司根据依法制定的劳动规章制度和依法签订的劳动合同，处理员工的考勤记录，属于实施人力资源管理所必需的个人信息处理行为。 该行为旨在判断员工是否存在迟到、早退等违反工作纪律的情形，有助于维护正常的工作秩序和劳动管理秩序。

表 D.1 合法性基础示例场景（续）

	处理员工的工作文档、邮件、和消息	公司根据依法制定的劳动规章制度和依法签订的劳动合同，对员工在公司配发的办公设备和办公软件中处理的工作文档、邮件和消息进行必要的监控，属于实施人力资源管理所必需的个人信息处理行为。 该行为旨在保障企业商业秘密和敏感信息的安全，防止员工在履行职责过程中向第三方泄露公司重要数据或信息。
	处理员工的绩效考核信息	公司根据依法制定的劳动规章制度和依法签订的劳动合同，对员工的绩效考核信息进行收集、评估和分析，属于实施人力资源管理所必需的个人信息处理行为。 该行为旨在客观评价员工的工作表现，作为薪酬调整、晋升、奖惩等管理决策的依据，有助于提升组织效能和员工发展。
为履行法定义务所必需	互联网平台保障网络安全稳定运行义务	为履行《中华人民共和国网络安全法》等法律法规规定的网络安全保障义务，互联网平台在提供网络服务过程中，依照法定要求采取技术措施和其他必要措施，对网络运行状态、异常行为、安全事件等进行监测、分析和处置，以保障网络的安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。 在此过程中，平台可能需要处理用户的设备信息、登录行为、IP 地址、访问日志等个人信息，属于履行法定职责或者法定义务所必需的个人信息处理行为。
	互联网平台履行用户身份核验义务的个人信息处理	为履行《中华人民共和国网络安全法》《互联网用户账号信息管理规定》等法律法规规定的用户身份核验义务，互联网平台在提供网络服务过程中，需依法对用户进行实名认证，核实用户身份信息，以防止网络违法和不良信息传播，维护网络空间清朗环境。 在此过程中，平台可能需要处理用户的手机号等个人信息，属于履行法定职责或者法定义务所必需的个人信息处理行为。
	互联网平台履行网络内容安全审核义务的个人信息处理	为履行《中华人民共和国网络安全法》《网络信息内容生态治理规定》等法律法规规定的网络内容安全审核义务，互联网平台在提供内容发布、评论、转发等服务过程中，需对用户发布的内容进行审核，以防范违法和不良信息传播，维护网络空间清朗环境。 在此过程中，平台可能需要处理用户的账号信息、发布内容、IP 地址、设备信息、行为日志等个人信息，用于识别内容来源、判断内容合规性、追溯违规行为。上述处理行为属于履行法定职责或者法定义务所必需的个人信息处理行为。
	互联网平台履行反网络诈骗风险防控义务的个人信息处理	为履行《中华人民共和国反电信网络诈骗法》《中华人民共和国网络安全法》《互联网信息服务管理办法》等法律法规规定的反网络诈骗风险防控义务，互联网平台在提供支付、社交、交易等服务过程中，需对用户行为进行风险识别和异常监测，以防范网络诈骗、虚假交易、恶意注册等违法行为，保障用户财产安全和平台秩序。 在此过程中，平台可能需要处理用户的账号信息、交易记录、登录行为、IP 地址、设备信息等个人信息，用于识别高风险行为、预警诈骗活动、配合执法机关调查。上述处理行为属于履行法定职责或者法定义务所必需的个人信息处理行为。
为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需	突发公共卫生事件中的疫情防控	在突发公共卫生事件期间，为有效控制疫情传播、保障公众生命健康安全，政府相关部门或指定机构可依法处理相关人员的个人信息，包括：个人身份信息、行程轨迹、健康状况、核酸检测结果等。该处理行为是为应对突发公共卫生事件所必需的，用于开展流行病学调查、风险人群筛查、隔离管控、医疗资源调配等防控措施。
	自然灾害或事故中的紧急救援	在发生自然灾害（如地震、洪水）或重大安全事故（如火灾、爆炸）等紧急情况下，为及时开展救援、保障人民群众生命健康和财产安全，应急管理部门、医疗机构或相关救援组织可依法处理相关人员的个人信息，包括：个人身份信息、联系方式、位置信息、受伤情况、家庭成员信息等。 该处理行为是为保护自然人的生命健康和财产安全所必需的，用于实施紧急救援、医疗救助、安置转移等应急处置措施。
为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息	媒体机构对公共事件进行新闻报道中的个人信息处理	某地发生一起涉及公共安全的交通事故，造成多人受伤，引发社会广泛关注。为履行新闻报道职责、保障公众知情权，某新闻媒体机构在调查和报道该事件过程中，依法采集并公开了涉事人员的部分个人信息，包括：（在不侵犯隐私权的前提下）事故当事人基本信息、事故现场照片、医院就诊信息、事故目击者或相关人员的陈述内容； 该处理行为是为公共利益实施新闻报道所必需的，且在合理范围内，用于向公众传递真实、客观、及时的新闻信息，促进社会监督和公共安全意识的提升。

表 D.1 合法性基础示例场景（续）

在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息	学术研究机构基于公开论文分析科研人员成果	某学术研究机构为评估科研人员的学术影响力，开展学术成果分析研究。该机构从学术数据库（如 CNKI、Web of Science、Google Scholar）中获取科研人员发表的论文、研究方向、引用次数等信息，用于构建学术影响力评估模型。 这些信息属于科研人员自行公开或合法公开的个人信息，处理行为仅用于学术研究、数据统计和成果分析，未超出合理范围，也未对个人造成实质性影响。
	企业基于公开信息进行市场调研分析	某市场调研公司为客户提供行业分析研报，从公开渠道（如企业官网、新闻报道、政府公示信息、行业白皮书）中收集企业高管信息、公司业务范围、市场表现等数据，用于行业趋势分析、竞争格局研究等商业用途。 这些信息属于企业或个人合法公开的个人信息，处理行为仅用于市场研究、行业分析等合理用途，未超出公开信息的原始用途，也未对信息主体造成实质性影响。
	大模型训练中基于合法公开数据的个人信息处理	某人工智能企业为训练语言模型，从合法公开的互联网数据源中用不违反法律法规要求的自动化采集方法采集文本数据。为确保数据处理行为符合《中华人民共和国个人信息保护法》相关规定，企业在数据采集和训练前，对数据中涉及的个人信息进行了系统性的辨析与去标识化处理。

参 考 文 献

[1] GB/T 32921—2016 信息安全技术信息技术产品供应方行为安全准则

[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] 《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

[4] 《全国人大常委会关于维护互联网安全的决定》2000 年 12 月 28 日第九届全国人民代表大会常务委员会第十九次会议通过

[5] 《全国人大常委会关于加强网络信息保护的决定》2012 年 12 月 28 日第十一届全国人民代表大会常务委员会第三十次会议通过

[6] 《中华人民共和国电子商务法》2018 年 8 月 31 日第十三届全国人民代表大会常务委员会第五次会议通过

[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令第 24 号公布，自 2013 年 9 月 1 日起施行

[8] 《中华人民共和国刑法修正案（七）》2009 年 2 月 28 日第十一届全国人民代表大会常务委员会第七次会议通过

[9] 《中华人民共和国刑法修正案（九）》2015 年 8 月 29 日第十二届全国人民代表大会常务委员会第十六次会议通过

[10] ISO/IEC 29100-2011Information technology Security techniques Privacy framework

[11] EU General Data Protection Regulation2015-05-24

[12] CWA 16113-2012Personal Data Protection Good Practices

[13] ISO/IEC 29101-2013Information technology Security techniques Privacy architecture framework

[14] ISO/IEC FDIS 29134Information technology Security techniques Privacy impact assessment2017-02-20

[15] ISO/IEC FDIS 29151Information technology Security techniques Code of practice for personally identifiable information protection 2016-12-16

[16] ISO/IEC 2nd WD 29184Information technology Security techniques Guidelines for online privacy notices and consent2016-12-04

[17] EU-U.S. Data Privacy Framework, 2023

[18] The OECD Privacy Framework OECD2013

[19] APEC Privacy FrameworkAPEC2005-12

[20] Consumer Privacy Bill of Rights Act of 2015 (Administration Discussion Draft)White House2015-02