ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 42574—2023

信息安全技术　个人信息处理中告知和同意的实施指南

Information security technology—Implementation guidelines for notices and consent in personal information processing

2023-05-23 发布　　2023-12-01 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。

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。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国电子技术标准化研究院、深圳市腾讯计算机系统有限公司、中国信息通信研究院、北京理工大学、同盾科技有限公司、北京字节跳动科技有限公司、完美世界控股集团有限公司、北京百度网讯科技有限公司、北京小米移动软件有限公司、华为技术有限公司、全知科技(杭州)有限责任公司、贝壳找房(北京)科技有限公司、阿里巴巴(北京)软件服务有限公司、北京邮电大学、北京奇虎科技有限公司、荣耀终端有限公司、北京京东尚科信息技术有限公司、OPPO广东移动通信有限公司、重庆邮电大学、北京小桔科技有限公司、公安部第一研究所、中国电子信息产业发展研究院、讯联智付网络有限公司、上海腾桥信息技术有限公司、国家信息技术安全研究中心、用友网络科技股份有限公司、泰康保险集团股份有限公司、顺丰速运有限公司、天翼电子商务有限公司、湖南财信数字科技有限公司、深圳法大大网络科技有限公司、中国人民银行数字货币研究所、飞利浦(中国)投资有限公司、蚂蚁科技集团股份有限公司、中电长城网际系统应用有限公司、京东科技控股股份有限公司、中国网络安全审查技术与认证中心、中国石油兰州石化自动化研究院、财付通支付科技有限公司、中国石油大庆油田信息技术公司、中信银行股份有限公司。

本文件主要起草人：何延哲、赵冉冉、葛鑫、洪延青、薛颖、胡影、陈湉、周晨炜、田申、衣强、刘笑岑、朱玲凤、刘俊河、谭礼格、娜迪娅·尼亚孜、张朝、邓婷、陈松、王艳红、彭骏涛、庄子骏、赵晓娜、张灵子、刘熙君、朱通、张向拓、闵京华、徐彩曦、符薇、张屹、李腾、张娜、王枞、李昳婧、陈绍良、严少敏、张有科、康琼、马可、樊华、蔡明阳、周顿科、姚一楠、王维、孟靖卓、付伟、史广龙、刘晓霞、王磊、魏书音、苏亚林、徐雨晴、王劲松、封莎、王昕、焦伟、李靖、王芳、刘明杨、袁扬民、宋杰、何云云、王超、刘元兴、汪巍、吴甜。

信息安全技术　个人信息处理中告知和同意的实施指南

1　范围

本文件给出了处理个人信息时，向个人告知处理规则、取得个人同意的实施方法和步骤。

本文件适用于个人信息处理者在开展个人信息处理活动时保障个人权益，也可为监管、检查、评估等活动提供参考。

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 35273—2020　信息安全技术　个人信息安全规范

GB/T 39335—2020　信息安全技术　个人信息安全影响评估指南

3　术语和定义

GB/T 25069—2022 和 GB/T 35273—2020 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。

［来源：GB/T 35273—2020，3.1，有修改］

3.2

敏感个人信息　sensitive personal information

一旦泄露或者非法使用，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：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，以及不满 14 周岁未成年人的个人信息。

3.3

个人信息处理者　personal information handler

在个人信息处理活动中自主决定处理目的、处理方式的组织或个人。

注：与 GB/T 35273—2020 中的“个人信息控制者”所指一致。

3.4

告知　notice

使个人知晓其个人信息处理活动及其有关规则的行为。

注：个人信息处理活动包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

3.5

同意　consent

个人对其个人信息进行处理自愿、明确作出授权的行为。

注：包括通过积极的行为作出授权(即明示同意)，或者通过个人的行为而推定其作出授权。

[来源：GB/T 35273—2020，3.7，有修改]

3.6

明示同意　explicit consent

个人通过书面、口头等方式主动作出声明，或者自主作出肯定性动作，对其个人信息进行处理作出明确授权的行为。

注：肯定性动作包括个人主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

[来源：GB/T 35273—2020，3.6，有修改]

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

提供　provision

个人信息处理者通过共享、转移等方式将个人信息传输或披露给其他个人信息处理者的行为。

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。

3.9

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。

注：个人信息保护影响评估也称“个人信息安全影响评估”。

[来源：GB/T 39335—2020，3.4，有修改]

4　缩略语

下列缩略语适用于本文件。

API：应用程序编程接口(Application Programming Interface)

App：移动互联网应用程序(Mobile Internet Application)

IoT：物联网(Internet of Things)

IP：互联网协议(Internet Protocol)

SDK：软件开发工具包(Software Development Kit)

5　告知的适用情形

5.1　收集个人信息

个人信息处理者收集个人信息包括但不限于以下情形。

a)　通过个人填写、勾选、上传等方式收集个人信息。

b)　通过软件程序或硬件设备等自动采集个人信息。

注 1：包括 SDK、API、浏览器、智能终端、传感器、摄像头等。

c） 与个人交互并记录个人的行为。

注 2：包括记录个人浏览、交易、客服咨询、使用服务等行为。

d） 从第三方间接获取个人信息。

e） 从非完全公开渠道获取个人信息。

注 3：非完全公开通常是指个人披露信息，但信息无法被任意人员通过互联网直接访问的状态，如设置了账户登录、关注、安装客户端、开通代理等条件。

f） 从与个人相关的他人账号收集个人信息。

g） 使用大数据、人工智能等技术分析、关联或生成个人信息。

5.2 提供、公开个人信息

个人信息处理者提供、公开个人信息包括但不限于以下情形：

a） 向其他个人信息处理者提供个人信息；

b） 向境外提供个人信息；

c） 在一定范围内或向不特定范围公开个人信息；

d） 因合并、分立、解散、被宣告破产等原因转移个人信息。

5.3 处理活动等发生变更

处理活动等发生变更包括但不限于以下情形。

a） 个人信息的处理目的、处理方式发生变更。

注 1：处理目的、方式的变更通常指个人信息处理者超出与收集个人信息时所告知的目的、方式具有直接或合理关联的范围处理个人信息。

注 2：将不同产品或服务所收集的个人信息进行汇聚融合通常属于处理方式的变更。

b） 处理的个人信息种类发生变更。

注 3：处理的个人信息种类的变更通常包括：现有业务功能处理个人信息种类增加、新增业务功能处理额外个人信息种类、向其他个人信息处理者提供个人信息种类增加。

c） 因合并、分立、解散、被宣告破产等原因转移个人信息，接收方变更原先的处理目的、处理方式的。

d） 向其他个人信息处理者提供其处理的个人信息，接收方变更原先的处理目的、处理方式的。

注 4：接收方包括境外接收方。

e） 公开的范围发生变更，如从一定范围内公开变为向不特定范围公开。

f） 个人信息的保存期限延长。

g） 个人信息处理者的名称或者姓名和联系方式发生变更。

注 5：包括涉及向其他个人信息处理者提供个人信息或向境外提供个人信息时，接收方的名称或者姓名和联系方式发生变更的情形。

h） 个人行使其权利的方式和程序发生变更。

5.4 其他情形

其他情形包括但不限于以下情形。

a） 两个及以上的个人信息处理者共同决定个人信息的处理目的和处理方式的。

b） 在产品或服务中接入需处理个人信息的其他个人信息处理者的产品或服务的。

c） 处理的个人信息涉及该个人以外的其他人的。

d） 处理已公开的个人信息，对个人权益有重大影响的。

e) 停止运营某类业务功能，或停止运营产品或服务时。

f) 个人行使权利，可能对其权益产生影响的。

注：通常包括个人拒绝同意、撤回同意、更正补充、删除、注销账号等情形。

g) 发生或者可能发生个人信息泄露、篡改、丢失等安全事件时。

h) 以下情形中处理个人信息的，采取适当方式向个人进行告知：

1) 为订立、履行个人作为一方当事人的合同所必需，或者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；

2) 为履行法定职责或者法定义务所必需；

3) 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；

4) 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；

5) 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；

6) 法律法规规定的其他情形。

6 同意的适用情形

6.1 需取得同意的情形

涉及5.1、5.2、5.3a)～e)、5.4a)～d)中的情形，个人信息处理者处理个人信息前，除有6.2中的情形外，需在告知的基础上取得个人同意。

6.2 免于取得同意的情形

6.2.1 订立、履行合同所必需

为订立、履行个人作为一方当事人的合同所必需，或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的，可免于取得个人同意。可被视为相关情形的个人信息处理活动，包括但不限于以下情形。

a) 为订立、履行个人作为一方当事人的合同，向个人提供产品或服务中的基本业务功能时，仅处理必要的个人信息。例如，按照电子商务合同约定配送货物而处理个人的收货地址、联系方式。

注1：个人信息处理者需明确出于何种目的、在何种场景下和范围内处理个人信息属于订立、履行合同的情形，并将相关事项以单独成文、成段等显著方式在个人使用基本业务功能前予以明确告知。

注2：不能将个人信息保护政策等公开个人信息处理规则的文件视为与个人订立的合同。

注3：必要是指该个人信息为实现产品或服务的基本业务功能所必需，且该实现方式对个人权益影响最小（如最少类型、最少数量、最低精度、最低频率等）。

b) 用人单位因与个人订立劳动合同而收集姓名、联系方式、学历、工作履历等必要的个人信息。

c) 商业银行、支付机构为履行支付服务合同义务，向重要支付系统等国家金融基础设施提供交易信息等必要的个人信息。

d) 为履行合同约定的售后服务条款，处理购买记录、联系方式等必要的个人信息。

e) 为履行合同约定，维护所提供产品或服务的安全、稳定运行所必需，且产品或服务无法安全、稳定运行将可能导致个人权益产生重大影响的，如为发现、处置健康状态监测设备的故障，收集必要的运行诊断数据等。

注4：出于该目的处理的数据，不能关联个人身份，且在披露的处理规则中详细说明处理的必要性。

如处理个人信息的目的、方式、范围超出合同约定，则不属于该情形。

6.2.2 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的个人信息处理活动，包括但不限于以下情形：

a) 履行反洗钱、反恐怖融资、反赌、反诈等监管要求，处理个人真实身份信息及相关交易记录；

b) 履行法律法规规定的网络实名认证要求，处理有效身份证件、移动电话号码等可以验证个人真实身份的必要的个人信息；

c) 履行法律规定的网络运营管理和网络安全保护等义务，处理相关网络日志信息，如IP地址、访问时间等；

d) 差旅住宿、航空、铁路运输、出行服务等行业，按照相关法律法规规定处理个人的实名身份信息；

e) 重要支付系统、证券结算系统等国家金融基础设施为履行法定义务，提供支付结算、证券登记等服务，处理必要的个人信息；

f) 与《中华人民共和国国家安全法》《中华人民共和国国防法》等法律规定国家安全、国防安全面临现实、紧迫的危险有关的个人信息处理活动；

g) 根据法律法规规定，为配合执法或司法机关要求提供相关个人信息；

h) 根据法律明确规定的方式与程序，对具体案件开展的与犯罪侦查直接相关的调查活动中涉及的个人信息处理活动。例如，为侦查刑事案件，侦查机关根据法律规定，向其他个人信息处理者或他人收集犯罪嫌疑人、被告人的指纹、脱氧核糖核酸（DNA）等生物信息、通话记录、上网记录等个人信息。

6.2.3 为应对突发公共卫生事件或者紧急情况所必需

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的个人信息处理活动，包括但不限于以下情形：

a) 在突发重大传染病疫情、群体性不明原因疾病、重大食物中毒或重大职业中毒事件以及其他严重影响公众健康的事件时，为推进应急处理工作，有关国家部门、医疗机构、疾病预防控制机构、卫生监督机构、出入境检验检疫机构等应急参与机构向有关个人或个人信息处理者收集、处理相关个人的姓名、住址、联系方式、行踪轨迹等必要的个人信息；

b) 因患者陷入严重昏迷等情形无法取得本人同意，不及时救助将使得其生命健康遭受现实、紧迫的威胁，医疗机构为实施救助，处理该个人的身体健康状况、身份信息、既往病史等必要的个人信息；

c) 发生自然灾害、事故灾难导致个人的人身安全遭受现实、紧迫的威胁，为实施救助，处理该个人的身份信息、位置等必要的个人信息；

d) 其他为了使自然人生命健康、财产安全免受正在进行的不法侵害或正在发生的危险，为阻断不法侵害或排除危险处理个人信息的情形。

6.2.4 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

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，包括但不限于以下情形：

a) 新闻媒体为公共利益报道时事新闻、热点事件等，合理使用自然人的姓名等个人信息；

b) 新闻媒体为公共利益实施舆论监督行为，合理使用自然人的姓名等个人信息。

6.2.5 在合理的范围内处理已公开的个人信息

在合理的范围内处理个人自行公开或者其他已合法公开的个人信息，包括但不限于以下情形。

a) 个人自行公开或其他已合法公开的个人信息，包括但不限于以下内容。
   1) 个人自行公开且已知悉或应当知悉可被不特定用户访问的个人信息。
   2) 个人向有关单位提供的信息，在提供时明确知悉其提供的信息将会被向社会公众公开。例如，用人单位在网站、宣传册等公开员工提供的简要职业履历等信息。
   3) 新闻媒体公开报道的信息。
   4) 司法、行政机关依据法定职责向社会公众公布的信息。例如，犯罪嫌疑人、被告人、失信被执行人等主体的信息。
b) 合理范围内处理是指个人未明确拒绝处理、处理未显著违背个人公开目的且未对个人权益造成重大影响。

6.2.6 法律法规规定的其他情形

法律法规规定的其他可免于取得个人同意的情形。

7 告知和同意的基本原则

7.1 告知的基本原则

个人信息处理者在实施告知时需考虑以下基本原则：

a) 公开透明：公布处理个人信息的种类、目的、方式、安全措施等处理规则，不采取故意遮挡、隐藏等方式诱导个人略过告知内容；
b) 有效传达：尽可能通过交互式界面、邮件、电话或短信等方式向相关个人进行告知；
c) 适时充分：在收集、提供、公开等个人信息处理活动发生之前或同时，对个人进行充分告知；
d) 真实明确：告知个人信息的处理种类、目的、方式等规则与实际情况一致，且需结合实际业务功能，不使用笼统、宽泛的表述；
e) 清晰易懂：告知文本符合个人的语言习惯，使用通用且无歧义的语言、数字、图示等。

注：主要面向境内个人提供产品或服务的，需提供规范汉字版（汉字简化字）的告知文本。

7.2 同意的基本原则

个人信息处理者在取得个人同意时需考虑以下基本原则：

a) 告知一致：取得同意的范围不超出所告知的内容；
b) 自主选择：支持个人通过自行操作的方式作出同意，不使用默认勾选的方式取得同意；
c) 时机恰当：在个人信息收集行为发生前，且同步传达告知内容时，取得个人同意，以增进个人对业务功能与所收集的个人信息之间关联性的理解；
d) 避免捆绑：区分产品或服务的业务功能，不采用捆绑方式强迫个人一次性同意多种业务功能可能收集的个人信息或多个处理活动；个人拒绝同意时，不影响与该个人信息无关的业务功能的正常使用。

7.3 告知和同意宜考虑的要素

个人信息处理者在实施告知和同意时宜考虑以下要素，优化告知和同意的方案和机制：

a) 友好展示：使用友好、生动、形象的方式编辑告知内容，优化告知内容组织形式，以便于个人理解；

b) 适配媒体：告知内容、展示形式、取得同意的方式等可根据告知媒体的种类、界面特点进行适应性设计，如适宜的字型大小、字体颜色、额外的震动和语音提示等；

c) 考虑影响：设计告知和同意方案时，可考虑个人信息处理活动对个人权益的影响程度以及个人的体验、习惯、合理预期等因素；

d) 区分阶段：根据个人使用产品或服务的不同阶段及交互场景，选用个人信息保护政策、弹窗提示、文字说明等不同的告知和同意方案；

e) 兼顾差异：考虑复杂多样的网络条件、软硬件差异、个人的知识水平和理解能力、身体机能差异等，使用可广泛适用且兼顾特定群体的告知和同意方案。

8 告知

8.1 告知的方式

个人信息处理者实施告知时，需结合产品或服务的业务功能特点，选择适当的告知方式或多种告知方式的组合，具体包括如下内容。

a) 一般告知，主要用于个人信息处理者在处理个人信息前向个人全面阐述个人信息处理规则，且通常采用制定、展示个人信息保护政策（或被称为“隐私协议”“隐私政策”“隐私权政策”等）的形式进行告知，包括以下内容。

1) 以公开且便于个人查阅的方式展示个人信息保护政策；个人信息保护政策支持拷贝、下载等方式以便于个人保存其内容。

注 1：使用交互式界面长期展示个人信息保护政策时，不能藏匿太深，如打开产品或服务的主界面后，个人不多于 4 次点击、滑动等操作能查看到个人信息保护政策。

2) 个人信息处理者宜将个人信息保护政策的完整内容置于产品或服务的基本业务功能开启时与告知相关的交互式界面中，并通过弹窗提示、提醒勾选、突出链接等明显方式，主动提示个人阅读个人信息保护政策。

3) 无法实现交互式界面展示个人信息保护政策的，需考虑以其他方式且在收集个人信息前的必要环节，以发送通知、邮件（或信件）、提供文档（包括电子版或纸质版）、张贴告示、播放音视频等方式向个人主动提供或展示。

4) 当向个人逐一告知的成本过高或者有显著困难时，可通过公告的形式发布个人信息保护政策。

注 2：个人信息保护影响评估认为个人信息处理活动对个人权益可能有重大影响的，即便存在显著困难，仍需坚持逐一告知的方式。

b) 增强告知，主要用于帮助个人理解个人信息处理规则中的关键内容或与特定业务功能处理目的相关的个人信息处理规则，且通常采用个人不可绕过的方式（如设置专门界面或单独步骤）向个人告知相关信息，以协助个人作出是否同意的决定，包括以下内容。

1) 增强告知的内容需浓缩一般告知的关键规则，突出展示个人最关心的内容，语言简洁、精练，方便阅读。

2) 增强告知的方式需凸显与一般告知方式的差异，其告知内容更加容易被个人所理解和获取。例如，一般告知采用要求个人勾选、点击等方式以达到提醒阅读的目的，而增强告知采用弹窗等方式向个人直接展示或送达关键内容。

3） 涉及发生停止运营某类业务功能，或停止运营产品或服务、涉及合并、分立、解散、被宣告破产等特殊情形的，宜通过邮件、短信、站内信等增强告知方式向个人告知具体情况，且保证个人可随时查阅告知内容。

4） 涉及可能对个人权益产生重大影响的个人信息处理活动时，还可选择使用电话、语音提示等方式进一步进行增强告知，以确保告知内容能够送达。

c） 即时提示，主要用于在个人使用产品或服务过程中，进一步强化个人对收集个人信息的目的的理解、方便个人获取有价值的信息等，包括以下内容。

1） 即时提示通常用于个人信息处理活动发生当时，或仅需告知的情形。

2） 即时提示的内容需简洁明了，提示方式宜结合产品或服务特点灵活选择，如选择使用弹窗、浮窗或浮层、文字说明、状态栏提示、提示条或提示框、提示音、短消息等方式。

注 3：可对不同方式进行对比，尽可能选取对个人打扰最少的方式。

3） 即时提示的主要作用为向个人及时、有效传达告知内容，辅助个人对个人信息处理规则的理解。

4） 即时提示需以保护个人权益为出发点，提示的内容不能存在误导性、偏向性。

8.2 告知的内容

8.2.1 收集个人信息时

收集个人信息时的告知内容包括如下内容。

a） 涉及 5.1 中收集个人信息的一种或多种情形，通常在首次收集个人的个人信息时，使用一般告知的方式，通过制定发布个人信息保护政策等机制，向个人告知个人信息处理者的身份和联系方式等基本情况，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、安全措施等规则，个人的权利及行使方式和程序，处理个人询问、投诉的渠道和机制等内容。

注 1：个人信息保护政策的具体内容见 GB/T 35273—2020 中 5.5 及附录 D。

b） 除 a）以外，为满足不同业务功能特点、不同收集个人信息方式告知的具体需求，尽可能全面、清晰阐述个人信息处理规则，还可考虑使用一般告知方式展示如下内容：

1） 产品或服务中所有业务功能可能收集的个人信息种类，可根据 5.1 所列情形予以分类描述；

2） 区分产品或服务提供的不同业务功能，并明确基本业务功能，说明各业务功能所收集的个人信息种类，或逐一说明每类个人信息的处理目的、方式；

3） 涉及自动采集个人信息的，说明自动采集个人信息的方式、时机、频次；

注 2：例如，App 通过申请获取移动智能终端提供的系统权限自动采集个人信息。

注 3：智能设备、应用软件的业务功能涉及后台运行时、长期监听时（如语音识别助手）自动采集个人信息的，还需说明必要性、安全措施、关闭方式等处理规则。

4） 收集的个人信息涉及敏感个人信息的，说明处理敏感个人信息的必要性以及对个人权益的影响；

注 4：可通过明确标识或突出显示等方式标注处理敏感个人信息相关的告知内容，以提醒个人予以重点关注。

5） 涉及 Cookie 等同类技术收集个人信息，需简要说明相关机制，包括收集个人信息的目的、种类，拒绝或清除记录的方法等；

注 5：同类技术如：脚本、点击流路径（Clickstream）、网络信标等。

6） 与其他个人信息处理者构成共同个人信息处理者时，说明各自分别承担的责任和义务；

7） 涉及嵌入的第三方代码、插件（如 SDK 等）收集个人信息，说明第三方身份，及收集个人信息的种类、目的、方式等；

注6：第三方代码、插件的提供方需向个人信息处理者主动披露收集个人信息的具体种类及处理规则以免告知内容出现偏差。

8） 保存期限届满后、停止运营某类业务功能时、停止运营产品或服务时如何对个人信息进行删除或匿名化处理的规则；

9） 以个人的操作视角，分步骤描述个人权利的实现机制；

10） 使用个性化推送方式进行商业营销、信息推送的，需说明如何设置不针对其个人特征的选项，或者拒绝个性化推送的方式；

11） 涉及使用自动化决策方式处理个人信息的，如根据GB/T 39335—2020开展个人信息保护影响评估认为对个人权益可能产生重大影响，宜主动说明自动化决策的基本原理、对个人权益的重大影响和拒绝自动化决策的方式；

12） 个人复制或转移已被收集个人信息的方法；

13） 针对不满14周岁未成年人个人信息处理规则以及保障措施；

注7：产品或服务的业务功能主要面向未成年人提供服务的，需制定专门的未成年人个人信息保护政策并予以发布。

14） 个人可再次查看一般告知内容的方法和路径，如个人信息保护政策等的访问渠道；

15） 如产品或服务涉及6.2所述的免于取得同意的具体情形，可予以说明。

注8：如为履行法定职责或法定义务、应对突发公共卫生事件，法律法规等明确指出必须收集的个人信息种类，在不影响履行职责或义务的前提下，说明所依据的法律法规等的具体条款。

c） 涉及以下收集个人信息的情形时，在一般告知的基础上，宜进一步使用增强告知的方式增进个人对个人信息处理的关键规则的理解。

1） 在产品或服务的基本业务功能开启前（如个人初始安装、首次使用、注册账号等情形）。如仅以链接等方式展示个人信息保护政策等处理规则时，可通过增强告知方式主动向个人告知其中的关键规则，包括个人信息保护政策的章节结构（点击后可直接访问对应内容），基本业务功能所必需的个人信息种类，收集方式、目的等，以及处理个人询问、投诉的联系方式。

2） 在个人选择使用扩展业功能务或新增业务功能时，通过增强告知方式向个人告知其处理个人信息的关键规则，如当前业务功能所必需的个人信息种类，收集方式、目的等，以及与产品或服务的完整个人信息保护政策有所区别的内容。

3） 涉及开通收集个人生物识别信息的业务功能，或某业务功能处理个人生物识别信息前，需通过增强告知方式向个人告知处理个人生物识别信息的必要性、对个人权益的影响，处理目的、方式，以及保存期限等规则。

4） 涉及通过间接方式获取个人信息的，宜通过增强告知方式向个人告知个人信息来源、需获取的个人信息种类及其必要性等。

注9：通过合并、收购等间接方式获取个人信息时，如原个人信息处理者已经通过8.2.2b）4）中的方式向个人告知的，不再重复使用增强告知的方式。

5） 产品或服务涉及收集不满14周岁的未成年人个人信息的，可通过增强告知方式提示需要向未成年人的监护人告知收集个人信息的情形，以及收集未成年人个人信息的目的、必要性、监护人可代为行使的权利及实现机制等规则。

d） 涉及以下收集个人信息的情形时，可使用增强告知的方式强化个人对收集个人信息的目的、方式、必要性等的理解。

1） 要求个人主动提供生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息时，宜根据GB/T 39335—2020开展个人信息保护影响评估，分析对个人权益的

影响，并通过增强告知的方式向个人告知处理个人信息的目的、处理的必要性和对个人权益的影响。

2） 采用软件程序或硬件设备自动采集个人信息时，可通过增强告知的方式向个人告知采集个人信息的目的。其中，通过自动采集精准地理位置等方式获取个人行踪信息的，还需告知处理的必要性和对个人权益的影响。

注 10：为帮助个人获知自动采集个人信息的时机或频次，还能采用状态灯、提示音等方式进行即时提示。例如，App 使用智能终端操作系统提供的“位置”权限自动采集个人的精准位置信息时，在智能终端屏幕的状态栏进行提示；智能摄像头在采集个人影像等数据时，采用红灯闪烁等方式向个人发出提示。

e） 在收集个人信息的过程中，需个人予以配合的（如人脸识别时需要个人点头配合）的，宜通过即时提示方式提醒收集的具体时机、注意点等。

8.2.2 提供、公开个人信息时

提供、公开个人信息时的告知内容包括如下内容。

a） 涉及 5.2 中提供个人信息的一种或多种情形，通常在提供个人信息前（或首次收集个人的个人信息时），使用一般告知的方式，通过制定发布个人信息保护政策等机制，向个人告知可能涉及的提供个人信息的场景，接收方的身份（或姓名、联系方式），提供的具体目的、方式，涉及的个人信息种类等。接收方位于境外的，还需告知个人向境外接收方行使权利的具体方法以及个人信息出境所具备的条件（如通过国家网信部门组织的评估、取得专业机构开展的个人信息保护认证、与接收方按照国家网信部门制定的标准合同订立了合同等）。

注 1：有一个或多个业务功能涉及提供个人信息，且涉及的处理规则复杂的，在个人信息保护政策以外，制定专门的个人信息提供政策详细说明相关规则。

注 2：有独立的业务功能涉及向境外提供个人信息，在个人信息保护政策以外，制定专门的个人信息出境政策详细说明相关规则。

b） 涉及以下提供个人信息的情形时，在一般告知的基础上，还需进一步使用增强告知的方式增进个人对个人信息处理的关键规则的理解：

1） 当个人首次使用涉及向其他个人信息处理者提供个人信息的具体业务功能时，可通过增强告知的方式向个人告知接收方身份、提供的具体目的、涉及个人信息种类等规则；

2） 当个人主动选择使用某个涉及向境外提供个人信息的业务功能时，可通过增强告知方式向个人告知境外接收方的身份、出境目的、涉及个人信息的种类、具备的出境条件等；

3） 当个人信息处理者在一定范围内或向不特定范围公开个人信息前，可通过增强告知方式向个人告知公开的原因、涉及的个人信息种类、已采取的去标识化等安全措施、可能产生的影响；

4） 当个人信息处理者业务功能发生变化，或因合并、分立、解散、被宣告破产等原因需要转移个人信息时，可通过增强告知方式向个人告知接收方身份和联系方式、转移的原因、涉及个人信息种类、可能产生的影响、接收方需继续履行的义务。

c） 当个人使用的业务功能可能导致其个人信息被公开的，个人信息处理者可通过即时提示的方式提醒个人谨慎使用，以免造成个人信息泄露。

注 3：可能导致个人信息被公开的情形如群组内发言、发布信息、回复评论、参加抽奖评选活动、接受访谈或个人信息被用于宣传推广等。

8.2.3 处理活动等发生变更时

处理活动等发生变更时的告知内容包括：

a) 在首次收集个人信息的一般告知过程中，所制定的个人信息保护政策可说明当所处理的个人信息种类、处理目的、方式等发生变更时，会重新取得个人同意；

b) 因产品或服务处理个人信息活动发生变更后更新个人信息保护政策的，可在个人再次使用产品或服务时，使用增强告知或即时提示的方式告知个人信息保护政策中更新的内容；

注 1：不涉及重新取得个人同意的更新，如 5.3f)～h)，使用即时提示的方式提醒个人关注处理规则中变更后的内容。

c) 涉及 5.3a)～e)中个人信息处理活动发生变更的一种或多种情形，可使用增强告知的方式增进个人对个人信息处理的关键规则的理解，告知的内容包括变更的原因，以及 5.3a)～e)中个人信息处理活动涉及的规则中发生变更后的内容；

注 2：变更涉及接收方变更原先的处理目的、处理方式的，经个人信息处理者与接收方协商一致后，也能由接收方选择履行相应告知义务。

注 3：变更可能会对个人权益带来不利影响的，还能向个人告知个人信息保护影响评估的结果。

d) 如将已收集个人信息用于临时性的目的进行处理时，宜通过增强告知的方式向个人告知临时性的目的、目的达成后的处理方式。

8.2.4 其他情形

其他情形的告知内容如下。

a) 当个人信息处理者与其他个人信息处理者为共同个人信息处理者时，可参考 8.2.1b)6)进行一般告知。当个人使用涉及其他个人信息处理者的业务功能时，可使用即时提示的方式提醒其身份与注意事项。

b) 产品或服务中接入了需处理个人信息的其他个人信息处理者的产品或服务时，当个人首次使用其他个人信息处理者提供的交互式界面、窗口时，可通过即时提示的方式向个人告知提供服务的其他个人信息处理者身份，并提醒个人关注该等其他个人信息处理者提供的个人信息保护政策等处理规则。

c) 处理的个人信息涉及个人以外的其他人时，可使用即时提示的方式告知可能产生的影响，并提醒个人向所涉及的其他人告知相关情况以取得对方的同意。

d) 个人信息处理者停止运营某类业务功能，或停止运营产品或服务时，除参考 8.2.1b)8)进行一般告知，还可使用增强告知方式，向个人告知复制或转移个人信息的方法、删除或匿名化的限定期限。

e) 个人行使权利，如拒绝处理、撤回同意、更正补充、删除等，可使用即时提示的方式向个人告知可能产生的影响，以助于其作出判断。

注 1：影响主要是指对个人带来的利益或权益减损，包括拒绝后无法使用何种业务功能，账户安全方面的保障水平下降等。

f) 个人注销账号时，可使用增强告知的方式向个人告知验证身份所需个人信息种类、设置的注销条件和理由、注销后的影响等规则。

g) 发生或者可能发生个人信息泄露、篡改、丢失等安全事件时，可使用增强告知的方式及时向个人告知个人信息安全事件出现的原因，以及 GB/T 35273—2020 中 10.2b)的内容。

注 2：个人信息处理者采取措施能够有效避免安全事件造成损害的，个人信息处理者能不告知个人，履行个人信息保护职责的部门不认为能有效避免损害的除外。

h) 涉及 5.4 h)的情形，如需要个人必须主动提供个人信息的，可通过即时提示的方式向个人告知具体的依据，以及处理的目的、方式、范围等规则。

i) 当个人信息处理者通过个人行为分析得出其个人信息可能存在泄露、被诈骗等风险时，可使用

即时提示的方式向个人进行风险预警及提出安全建议。

注 3：如通过安全风控的机制发现个人频繁发布，或向存在风险的联系人传送包含敏感个人信息种类（如身份证号、银行卡号等）的行为，向个人发出提示。为避免引起个人产生安全风控的机制对其行为构成监控的担忧，对安全风控的机制通过单独文档或问询答复等方式进行详细说明。

j） 当个人在使用产品或服务的过程中遇到关于个人信息保护方面的疑惑、问题，可使用即时提示的方式向个人展示处理个人询问、投诉的渠道。

k） 通过分析投诉、举报信息、社会反映情况等方式得知个人对某些个人信息处理规则不明，可在个人使用产品或服务过程中，使用即时提示的方式进一步解释说明。

l） 其他与个人权益密切相关、需要向个人强调的信息可使用即时提示的方式进行告知。

8.3 告知的实施

8.3.1 概述

个人信息处理者基于 7.1、7.3、8.1、8.2，明确告知的方式、内容，并根据 8.3.2～8.3.4 选择适当的告知内容展示界面或告知渠道、合理的告知时机和频率后，形成告知的具体实施方法和步骤。实施要点包括：

a） 不同场景下向个人告知的实施方法见附录 A～附录 M 中的相关内容；

b） 个人信息处理者宜对告知内容是否有效送达进行记录，并对告知的效果进行评估，不断优化告知的方式；

c） 法律法规规定需保密或者不需要告知的情形的，可以不向个人告知；

d） 紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者需在紧急情况消除后及时告知。

8.3.2 告知的界面或渠道

个人信息处理者需以便于个人立即阅读、获取的方式，设计适当的告知界面或渠道，并根据载体、环境等的不同进行调整，优化告知界面或渠道的形式，具体包括以下内容。

a） 在个人可操作的计算机、智能终端（包括固定终端、移动终端等）等屏幕展示告知界面时，可采取弹出可关闭（或点击按钮、滑动后可跳过）的单独窗口、设置经多次点击、下拉菜单访问的交互式界面等方式。

注 1：在个人注册界面、登录界面、App 启动页、首页等显著位置展示个人信息处理规则。

注 2：为了进一步方便个人寻找相关的告知界面及告知内容，还能设置关键字搜索、客服自动回复等方式指向告知界面。

b） 在个人不可操作的公共场所大屏幕、显示屏等展示告知界面时，可采取设置倒计时结束后自动关闭的单独窗口、屏幕特定区域展示扫描后可获取告知内容的二维码等方式。

注 3：单独窗口的弹出时间通常设置在屏幕启动后，或设置固定时间周期弹出。

c） 产品或服务没有可供个人直接操作的界面或可观看的屏幕的，可在产品或服务的纸质版用户手册、说明书，或设备外包装、外壳、标签上展示告知内容或设置告知内容的访问链接（如二维码）。

注 4：如 IoT 设备配备较小的显示屏不足以展示告知内容的，在自带的显示屏上设置告知内容的二维码。

注 5：如提供产品或服务的设备能连接互联网，还能引导个人绑定该设备的 App 后，由 App 展示告知内容。

d） 产品或服务没有可供个人直接操作的界面或可观看的屏幕，且不便逐一向个人提供告知内容时，可通过发布公告、特定范围内张贴、展示告知内容或告知内容的访问链接（如二维码）的方式。必要时，还可通过广播通知、声光提示等方式提醒个人关注告知的内容。

e) 产品或服务主要依赖书面方式进行告知的，可将个人信息处理规则的核心告知内容布置于签字确认区域附近。

f) 产品或服务涉及未成年人、老年人、身体机能差异人群等个人时，可适当增加额外的展示界面和渠道。

g) 产品或服务涉及个人主动填写和提交个人信息时，可在填写或选择框中简述目的等内容。

h) 产品或服务因客观条件限制无法通过交互式界面、书面方式、张贴告示方式等进行告知的，如已通过合法渠道获取了个人的联系方式，还可采用短信、邮件、电话等方式主动联系，向个人主动提供告知内容。

8.3.3 告知内容的展示

告知内容展示需以个人视角的用户体验和权益保障为出发点，以清晰易懂、内容简洁、主次分明为目标设计展示方案，具体包括：

a) 通过交互式界面展示告知内容的，可采用多层次的告知方式，如直接展示核心告知内容、提示关键内容、提供完整告知内容的链接等方式；

注：在个人注册界面、登录界面、App 启动页、首页等显著位置通过交互式界面展示个人信息保护政策核心内容，并提供完整的个人信息保护政策链接，相关内容位于界面中央等显著位置。

b) 告知的内容中涉及敏感个人信息、对个人权益有显著影响的条款、个人信息处理规则发生重大变化的部分，需明确标识或突出显示（如字体加粗、增大字号、醒目颜色等）；

c) 告知的内容中存在易引起异议或争端的部分，可采用主动推送、优先展示等方式尽可能保证个人可获取，必要时可设置确认个人确认已获知的机制；

d) 不在告知的界面中通过弹出窗口遮挡、置于边缘等造成个人忽略告知内容；

e) 使用文字方式进行告知的，选用的字号、字体、颜色、行间距、清晰度等不造成个人阅读困难；

f) 使用图形、音视频方式进行告知的，设置的亮度、清晰度、音量等不造成个人观看困难；

g) 使用插图、漫画等方式进行告知的，可兼顾告知内容的准确性与展示内容的生动性。

8.3.4 告知的时机和频率

告知适当性，主要指个人信息处理者可通过设置合理的告知时机和频率，以提高告知的充分性和有效性，帮助个人更加准确地掌握个人信息处理规则。如告知的时间点和收集个人信息的时间点相差较大，将使个人无法获知告知内容与所收集个人信息之间的关系。

首先，个人信息处理者可将首次告知、同步告知、再次告知等时机相结合，优化不同阶段告知的内容的体量，以提升个人的接受度。通常，首次告知采用的是一般告知的方式，同步告知、再次告知采用增强告知或即时提示的机制。其次，个人信息处理者可以适当的频率或时间间隔确认现有的告知或发起新告知，既需要避免告知的频率过低，导致告知的内容无法有效传达，又需要避免告知的频率过高对个人造成不必要的打扰。总之，个人信息处理者选择的告知时机和频率需平衡告知的充分性和用户体验。具体包括：

a) 个人在首次使用产品或服务前，可进行首次告知；

b) 产品或服务在收集个人信息时，对个人权益影响较大、收集的必要性需要单独强调、相关业务功能收集目的不易理解的，可进行同步告知；

注 1：如业务功能所收集个人信息的必要性较为直接易懂、个人通常无需被另行告知即能理解的，可将业务功能名称介绍视为对目的的同步告知。

c) 通过其他载体收集或间接获取个人信息时，可进行同步告知，因客观条件所限（如无联系渠道）需在获取个人信息后才能告知的，需在获取后向个人进行再次告知；

d) 个人信息处理者变更个人信息处理目的、方式、范围前，可进行再次告知；

注 2：个人信息处理者能根据个人是否可以查阅告知或同意内容的历史记录，以及之前的告知或同意至再次告知或同意所隔时间等要素简化告知的内容。如个人能随时查阅其历史同意内容，或距上次告知时间较短，个人信息处理者能选择仅告知变更内容，否则个人信息处理者将变更内容和历史已告知的原始内容一并告知。

e) 个人信息处理者在向其他个人信息处理者提供个人信息前，可进行同步告知；

注 3：如业务功能需不间断或反复多次向其他个人信息处理者提供个人信息，在首次提供时同步告知，并说明后续提供的时机或频次等规则，避免频繁打扰。

f) 当个人拒绝对收集、提供、变更目的等的请求后，可采用再次告知的方式向个人说明必要性和对个人权益的影响，不采用频繁打扰方式进行反复告知；

g) 产品或服务更新后个人信息保护政策发生变化的，可进行再次告知；

注 4：个人信息保护政策发生变化，但不涉及 5.3 相关内容的，不进行再次告知，以免对个人带来打扰。例如，个人信息保护政策中的安全措施描述进行更新，不向个人告知。

h) 在个人注销账户时，可进行同步告知；

i) 个人信息处理者在停止业务功能运营前，可进行同步告知；

j) 个人信息处理者发生对个人信息有严重影响的安全事件时，可紧急进行同步告知。

9 同意

9.1 同意机制的选择

9.1.1 明示同意

个人信息处理者取得同意时，原则上需使用明示同意的方式，确保个人在理解收集目的和相关处理规则的基础上，自主给出具体、清晰、明确的意愿表示，且避免采取被动接受、默认选择的方式，导致个人忽略对个人信息处理规则的关注。个人用于表示明示同意的方式包括但不限于：

a) 个人通过交互式界面作出主动勾选、主动点击“同意”“下一步”“继续”、滑动滑块、主动发送等动作表示意愿；

b) 个人通过主动填写、上传、输入个人信息表示意愿；

c) 个人通过开启可收集个人信息的 API、权限、传感器开关表示意愿；

d) 个人通过纸质或电子的书面声明、签字确认表示意愿；

注：该方式通常被用于表示书面同意。

e) 个人通过主动出示证件、刷卡、刷指纹、刷脸等动作表示意愿；

f) 个人通过回复邮件、短信息等主动联络的方式表示意愿；

g) 个人通过电子签名方式表示意愿；

h) 个人通过电话录音、视频录像等方式表示意愿。

个人信息处理者可结合产品或服务的特点、个人信息处理活动可能对个人造成影响的程度等因素，选择上述明示同意操作方式中的一种或几种，来保证明示同意的有效性。

9.1.2 其他同意

因客观条件限制、个人自身习惯、保护各方合法利益等原因，个人无法通过 9.1.1 中的方式表达明示同意时，个人信息处理者可基于对个人行为的分析，如个人未明确表示拒绝个人信息处理，或个人选择继续使用特定业务功能时，推定出个人表示同意，可推定为个人表示同意的情形示例见附录 N。使用该方式取得个人同意时，需同时满足以下条件。

a) 取得明示同意存在显著困难，例如：

1) 产品或服务的业务功能所需的网络等环境条件受限；

2) 产品或服务的展示界面或渠道以及个人的反馈方式受限；

3) 涉及身体机能差异人群，进行交互或收集反馈存在困难；

4) 未掌握与个人沟通的渠道，导致无法确认个人作出了明示同意；

注：如个人信息是通过其他个人信息处理者间接获取的，不能视为未掌握沟通渠道的情形。

5) 个人拒绝后将导致个人使用产品或服务的安全性（账户安全、财产安全等）严重下降；

6) 为训练反欺诈模型、违法信息与音视频的识别等维护个人合法权益或公共利益等目的，使用去标识化后的个人信息。

b) 经个人信息保护影响评估确认个人信息的处理不会对个人权益造成不利影响。

c) 基于第8章，采取了适当的方式向个人告知个人信息处理规则。

d) 被推定为个人同意的情形不影响个人行使撤回同意的权利。

在后续的个人信息处理活动中，如个人信息处理者具备执行明示同意的条件时，需向个人告知撤回同意的方式，或重新取得个人的明示同意；如个人通过投诉、举报渠道反馈其个人权益受到不利影响的，经确认后需立即中止相关的个人信息处理活动，经个人明示同意的处理活动除外。

9.2 同意的实施

个人信息处理者根据第8章明确告知的方式、内容、实施方法后，基于7.2、7.3、9.1，形成同意的具体实施方法和步骤。实施要点包括：

a) 梳理所有需履行告知义务的个人信息处理活动，明确哪些个人信息处理活动需要取得个人同意；

注1：经分析（包括引入第三方进行分析）后认为个人信息处理活动涉及6.2所列出的情形的，经个人信息保护负责人审核批准后能排除在外。

注2：部分告知场景如只侧重于向个人传达相关情况，不设置取得个人同意的步骤，如发生个人信息安全事件后向个人通知采取的措施等。

b) 针对所有待取得个人同意的个人信息处理活动，根据9.1.1提出的机制设计取得个人明示同意的方案；如存在其他同意情形的，需事先分析（包括引入第三方进行分析）相关情形满足了9.1.2中的条件，并在处理个人信息期间留存了个人信息保护影响评估的结果；

c) 在页面篇幅允许的情况下，个人信息处理者宜在展示告知内容的同一页面征求个人同意；

注3：如告知内容与取得同意过程未设置在同一页面，个人可能会对同意的内容产生困惑。

d) 在使用个人信息保护政策等一般告知的方式展示全部个人信息处理规则时，可通过弹窗提示、独立段落等显著方式向个人说明：同意个人信息保护政策并不表示该政策中列明的所有个人信息均会被一次性收集，而是在个人使用具体业务功能时才会收集必要的个人信息；

e) 个人信息处理者需明确在产品或服务的哪些阶段需设置清晰易理解的同意操作界面或步骤，便于个人理解该界面或步骤所执行的操作是用于表达对个人信息处理活动的同意；

注4：通过设置点击“下一步”“注册”“继续”“愿意参与活动”等步骤取得个人同意的，需明确该等操作与同意个人信息保护政策或授权处理个人信息之间的逻辑关系并向个人清晰说明。

f) 个人信息处理者不能使用含糊其辞、避重就轻、模棱两可、有悖正常逻辑的文字或功能设计影响个人对同意的判断，让个人的期许与实际的个人信息处理活动出现偏差；

注5：例如，个人认为只是同意试用业务功能期间处理个人信息，但事实上试用期结束后仍然继续处理个人信息。

注6：例如，把“不把某类个人信息应用于特定目的”选项设置为默认关闭状态，可能会被个人误以为已经禁止了某类个人信息应用于特定目的。

g） 个人信息处理者宜将对个人信息处理的同意与其他同意事项以合理方式区分开来，避免将其隐匿在其他同意事项中，导致个人忽略了个人信息处理规则；

注 7：例如，将个人接受一般性的服务条款与个人同意个人信息处理规则予以区分。

h） 个人信息处理者可区分不同处理目的或不同业务功能所需的个人信息种类，通过分步骤获取同意的方式逐步取得个人同意，以保障个人自主表达意愿的权利；

注 8：当产品或服务提供多项需收集个人信息的业务功能时，避免采取捆绑等方式强迫个人同意多项业务功能的收集请求。

i） 个人信息处理者需将满足业务功能或特定目的所必需收集的个人信息，与提升服务质量和用户体验、提高安全性、支撑产品或服务改进等目的所收集的个人信息予以区分，分别取得个人同意；

j） 如处理个人信息可能对个人权益造成重大影响的，可同时使用多种方式确保个人充分知情，如在交互式界面执行“下一步”“同意”等操作基础上，进一步采取电话回访、签字确认等方式取得同意；

k） 个人信息处理者设计同意实施方案时，宜根据有关国家标准，通过个人信息安全工程等方法，对处理个人信息的系统架构设计进行充分评估，以支持个人通过便捷方式撤回同意、限制使用、删除个人信息等操作；

l） 个人信息处理活动可能对个人权益产生长期影响的，或可能引发个人长期的隐私担忧的，可采用限制同意期限或范围（如单次同意）的方式，仅在一次操作周期、一段时间内或一定区域内同意对个人信息的处理，超出授权处理的期限或范围时可再次取得个人同意，否则需立即停止个人信息的处理活动；

注 9：例如，针对智能网联汽车对车辆位置、驾驶人或乘车人音视频的收集和向车外传输等行为，驾驶人作出的同意仅在驾驶人行驶期间有效，驾驶人离开车辆后同意自动失效。

注 10：例如，智能终端操作系统开发商、App 运营者向个人提供针对位置信息、麦克风、摄像头等权限使用的“单次允许”或“仅使用中允许”的选项。

m） 除上述内容外，不同场景下取得个人同意的实施方法见附录 A～附录 M 中的相关内容。

9.3 单独同意的实施

9.3.1 通用实施要点

针对法律法规规定的特定个人信息处理情形或者可能对个人权益带来重大影响的个人信息处理活动，个人信息处理者需充分履行告知义务，取得个人单独同意。单独同意是一种增强的“同意”方式，在 9.2 的基础上实施时，还需关注以下实施要点。

a） 个人信息处理者梳理法律法规明确要求采取单独同意的情形，以及评估后认为可能对个人权益带来重大影响的个人信息处理活动，形成需执行单独同意的清单，并根据法律法规和处理活动的变化以及收到的有关投诉、举报情况，不断更新清单内容。

注 1：法律法规明确要求采取单独同意的情形通常包括：向其他个人信息处理者提供个人信息，公开个人信息，将在公共场所通过图像采集、个人身份识别设备所收集的个人图像、身份识别信息用于维护公共安全之外的目的，处理敏感个人信息，向境外提供个人信息。

注 2：实施对个人信用、绩效评定、所接受服务的质量、交易价格等会对自然人人格尊严、人身或财产安全等产生重大直接影响的自动化决策，通常属于可能对个人权益带来重大影响的个人信息处理活动。

b） 在个人作出单独同意之前，需通过增强告知的方式，针对需要单独同意的情形专门向个人进行充分告知。

注 3：单独同意的情形中涉及的个人信息处理规则较为复杂时，专门为单独同意的情形制定处理规则，如业务功能

处理人脸信息前，由个人查看弹窗提示的人脸信息处理规则后，进行单独同意。

c) 个人信息处理者需选择明示同意的方式来取得个人单独同意。

d) 个人信息处理者可根据产品或服务的业务功能特点，以及个人的使用习惯、隐私偏好等，选择易于展示、便于操作的具体实施方案，可选择的方案包括：

1) 在个人使用特定业务功能主动触发涉及需单独同意的情形时，在向个人充分告知后，由个人作出明示同意；

2) 特定业务功能涉及需单独同意的情形时，可采用单独的交互式界面或纸质页面向个人告知相关信息，涉及多个需要单独同意的情形时，可向个人提供可分项选择同意（如勾选、点亮等）的机制，分项选择同意的选项各自独立互不影响。

注 4：如特定业务功能为产品或服务的基本业务功能，将需单独同意的情形相关告知内容以突出显示、弹窗等与其他内容有所区分的方式单独告知，在个人同意使用基本业务功能时一并同意。

注 5：在个人首次使用产品或服务时，将涉及单独同意的场景（或部分场景）在展示个人信息保护政策时向个人提供分项选择同意的机制。

注 6：在个人作出分项选择的同意前，不以默认勾选、提前点亮、缩小字号、淡化字色等方式干扰、影响个人对单独同意的判断。

e) 单独同意所针对的处理活动需针对具体且独立的目的或业务功能，不与具备其他处理目的、采取其他处理方式的个人信息处理活动相捆绑或混同在其他同意事项中，以避免一揽子取得个人同意。

注 7：点击或勾选同意产品或服务的个人信息保护政策，不构成针对具体个人信息处理活动的单独同意。

注 8：在对具体个人信息处理活动给出单独同意的同时，如还要求个人同意针对该处理活动所必需的服务协议等其他与个人信息处理规则无关的法律文件的，不视为一揽子取得同意。

注 9：针对同一个处理目的或同一业务功能同时处理多项个人信息字段，且逐项拆分字段后无法达成处理个人信息目的或无法实现该业务功能的，就多项字段一并告知并一次性取得个人单独同意的，不视为一揽子取得同意。

f) 如个人拒绝给出单独同意或撤回所作出的单独同意的，需确保不会影响单独同意范围之外的其他业务功能或处理目的，单独同意所针对的业务功能为产品或服务的基本业务功能的除外。

9.3.2 提供个人信息

具体的实施要点包括：

a) 除非法律法规另有规定，个人信息处理者向其他个人信息处理者提供其处理的个人信息的，需在提供前向个人告知接收方的身份、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意；

注 1：向多个其他个人信息处理者提供个人信息，如提供个人信息的目的、方式、种类等一致，提供过程同时或同一场景发生的，在告知内容中逐一列举接收方的身份和联系方式，由个人一并进行同意。

b) 在取得个人的单独同意后，个人信息处理者才能将其处理的个人信息提供给其他个人信息处理者；

注 2：如 App 中接入的其他个人信息处理者的代码、插件，在取得个人对其处理个人信息的单独同意前，个人信息处理者需阻止代码、插件自动运行采集个人信息。

c) 个人信息处理者基于个人单独同意向其他个人信息处理者提供了敏感个人信息的，宜在提供之后及时通过短信、邮件、应用内消息等方式再次向个人告知就所提供的个人信息种类、目的和接收方，以便个人随时查询知悉。

9.3.3 公开个人信息

具体的实施要点包括：

a) 除非法律法规另有规定，个人信息处理者公开其处理的个人信息前，需向个人告知所公开个人信息的种类，公开的目的、方式、范围，可能对个人产生的不利影响以及个人的权利，并取得个人的单独同意；

注：例如，对于公开个人在其社交应用账号下记录的信息，个人信息处理者需允许个人在发布信息之前能够自由选择信息的公开范围，且不能自动设定为向所有不特定用户公开的选项，个人自行调整隐私偏好的除外。

b) 个人信息处理者公开其处理的个人信息前，或个人主动选择公开个人信息的，个人信息处理者需向个人提示公开的范围，如向特定的群体予以披露或者向公众予以公开；

c) 公开个人信息对个人权益影响较大的，可进一步通过与个人主动取得联系并告知等方式，保证个人对相关处理规则和公开可能产生的影响完全知情；

d) 除法律法规另有规定外，个人如将已自行或已同意向社会公众公开的信息撤回，与公开渠道相关的个人信息处理者需通过断开链接、删除信息发布记录等措施删除已公开的个人信息。其他个人信息处理者获取此前已公开的个人信息的，个人有权要求其进行删除。

9.3.4 公共场所收集信息用于维护公共安全之外的目的

具体的实施要点包括：

a) 除非法律法规另有规定，个人信息处理者将为维护公共安全目的在公共场所通过图像采集、个人身份识别设备所收集的个人图像、身份识别信息用于维护公共安全之外的目的，需向个人告知处理与该目的相关的个人信息处理规则，并取得个人的单独同意；

注 1：例如，因 6.2.4 中所涉情形处理包含个人图像、身份识别信息的，免于取得个人的单独同意。

注 2：出于维护公共安全目的，在公开场所收集个人图像、身份识别信息时，如需将相关信息用于维护公共安全以外的目的（如会员身份确认），通过引导个人通过扫描二维码等方式了解相应个人信息处理规则后，由其主动点击“同意”方式进行授权。

b) 将公共场所收集的个人图像、身份识别信息用于维护公共安全之外的目的时，如涉及多人的，在处理前，需逐一向每个人告知目的，并取得所有个人的单独同意，经匿名化处理（如自动将图像中的人物用单色替代）的除外。

注 3：例如，通过与相关个人取得联系后，使用书面签字确认等方式取得单独同意；多人共同签署同一个授权书也能视为取得了单独同意。

9.3.5 处理敏感个人信息

具体的实施要点包括如下内容。

a) 除非法律法规另有规定，处理敏感个人信息的，除向个人告知处理敏感个人信息的目的、方式、范围等个人信息处理规则，还需告知处理敏感个人信息的必要性以及对个人权益的影响，并取得个人单独同意。

b) 以要求个人主动填写或选择选项方式取得对宗教信仰、特定身份等敏感个人信息单独同意的，可设置独立界面或在界面的独立区域向个人进行告知，并支持个人通过点击、勾选等肯定性动作表示同意意愿。

注 1：向个人提供选项方式时，不采取提前预选的方式。

c) 如为实现某一特定目的需要同时处理多项敏感个人信息的，可一并告知并一次性取得个人单独同意。

注 2：例如，个人信息处理者为了开通网上投资理财服务而需要收集投资人姓名、手机号码、身份证号和银行卡号等的，在一个表单页面中就需要收集的多项字段一并告知并一次性取得个人单独同意，对于其中的“身份证号”和“银行卡号”标识为“敏感个人信息”。

d) 如为实现某一特定目的处理敏感个人信息时，涉及收集、使用、提供等多个步骤个人信息处理活动或涉及多人的，且多个处理活动或多个主体拆分后无法达成该特定目的的，可一并告知并一次性取得个人单独同意。

注 3：例如，个人信息处理者使用了其他个人信息处理者的人脸识别技术，为进行身份鉴别需收集个人的人脸识别信息并提供给其他个人信息处理者的，对收集和提供的情形一并告知，并一次性取得个人单独同意。

e) 产品或服务的业务功能可能涉及处理不满 14 周岁的未成年人个人信息的，可采取以下方式实施单独同意：

1) 如产品或服务的目标人群没有限制的，且无法从业务功能所必需收集的个人信息中分析出个人为未成年人的，可主动提示未成年人向其父母或其他监护人（统称“监护人”）转达相关告知内容，并取得监护人的单独同意；

2) 如产品或服务的目标人群为不满 14 周岁的未成年人的，可采取未成人不易绕过的方式引导未成年人向其监护人转达相关告知内容，并取得监护人的单独同意；

注 4：例如，要求提供未成年人监护人的联系方式，或设置需要由未成年人监护人作出单独同意的步骤，通常属于不易绕过的方式。

3) 如产品或服务的目标人群为已满 14 周岁的未成年人的，可不设置由其监护人同意的机制，但需以增强告知等方式明确拒绝不满 14 周岁未成年人使用，必要时可设置验证年龄的措施以避免收集不满 14 周岁未成年人的个人信息；

4) 通过所收集的个人信息可确认个人为不满 14 周岁未成年人的，需主动提示和引导该未成年人向其监护人转达相关告知内容并取得监护人的单独同意，否则可拒绝继续为该未成年人提供产品或服务；

注 5：例如，通过个人主动提供的年龄、出生日期、身份证号等信息判断其是否为不满 14 周岁未成年人。

5) 个人信息处理者需仅以合理手段验证未成年人年龄、监护人身份，如验证过程无法避免收集个人信息的，需将个人信息严格限定在上述目的范围内处理，并在完成处理后立即删除收集的个人信息。

f) 除上述情形中涉及的敏感个人信息外，有关法律法规要求的其他种类的个人信息，在处理前需要取得个人单独同意的，可参考上述条款实施。

9.3.6 向境外提供个人信息

具体的实施要点包括：

a) 个人信息处理者向境外提供个人信息的，需向个人告知境外接收方的身份、联系方式、处理目的、处理方式，个人信息的种类、保存时间、保存区域（至少具体到国家或地区）以及个人向境外接收方行使相关权利的方式等内容，并取得个人的单独同意；

注：个人在自行了解境外接收方所公布的个人信息处理规则后，主动以邮件、短信息、点击启动服务、在线提交信息或直接确认等方式向境外接收方发送涉及其个人信息内容的，视为作出了单独同意。

b) 如产品或服务中涉及个人信息出境的业务功能可与其他业务功能相分离的，个人信息处理者宜将涉及个人信息出境的业务功能与其他业务功能区分，以便个人针对个人信息出境作出单独同意；

c) 个人拒绝涉及个人信息出境的业务功能后，不能影响其他业务功能的正常使用；

d) 收集个人信息时已事前单独就个人信息出境取得个人同意，满足出境其他条件的前提下，后续在出境时可不再次取得个人单独同意；

e) 如法律法规另有规定向境外受托处理者提供个人信息也需要取得个人单独同意的，可参考 9.3.6a)～d)实施。

9.4 书面同意的实施

针对法律法规要求取得个人书面同意的情形或者个人信息处理者认为需要以书面形式取得个人同意的，个人信息处理者需以纸质或数字电文等有形地表现所载内容，并由个人通过主动签名、签章等形式取得个人同意。实施要点包括：

a) 个人信息处理者需梳理法律法规明确要求采取书面同意的情形以及评估后认为需要进行增强存证或存档、加强证据固定效果等的个人信息处理活动，形成需执行书面同意的清单，并根据法律法规和处理活动的变化以及收到的有关投诉、举报情况，不断更新清单内容；

注 1：法律法规要求取得个人书面同意的情形包括：在广告中使用他人名义或者形象，通过指定网络通道送达某些类型的诉讼文书，采集人类遗传资源，征信机构采集个人的收入、存款、有价证券、商业保险、不动产的信息和纳税数额信息，向征信机构查询个人信息，使用金融信用信息基础数据库查询个人信息，从事信贷业务功能的机构向金融信用信息基础数据库或者其他主体提供信贷信息等。

注 2：其他规范性文件中要求取得个人书面同意的情形包括：邮政企业、快递企业及其从业人员向他人提供用户的个人身份信息及其使用邮政服务、快递业务功能的信息，为宣传报道和奖励检举有功人员而公开检举人的相关个人信息，用人单位公开劳动者的个人信息，商业银行与合作机构共享客户个人信息等。

b) 受托人转委托其他个人信息处理者处理个人信息，宜取得个人信息处理者的书面同意；

c) 在个人作出书面同意之前，需通过增强告知且以书面形式呈现的机制，针对需要书面同意的内容明确向个人进行充分告知；

注 3：如需要取得书面同意的告知内容与其他事项一并告知的，需以字体、字号、字色等方式突出需要取得书面同意的告知内容，以便提示个人关注，并明确告知该等处理活动对个人权益可能产生的影响，必要时根据个人的要求对影响作出明确的书面说明。

d) 个人信息处理者需选择明示同意的机制取得个人的书面同意，且明示同意需以文字形式予以明确表达，不以采取个人点击确认、点击同意、上传提交、登录使用或配合拍照等表示同意的方式取得个人的书面同意；

e) 个人信息处理者可根据产品或服务的业务功能特点，以及个人的使用习惯、隐私偏好等，选择易于展示、便于操作的书面同意具体实施方案，例如，个人在纸质界面、电子硬件载体、网页交互式界面或对话框上进行手写签名、签章等；

f) 如根据法律法规等要求，个人信息处理者既需要取得个人书面同意也需要取得其单独同意的，需在书面同意的基础上，根据 9.3 设计单独同意的机制，如单独签名、签章等。

9.5 拒绝同意的实施

个人信息处理者对于个人拒绝同意，实施要点包括：

a) 明确个人拒绝或放弃同意的表现形式，如点击拒绝、中断操作、关闭界面、回退到上一步等，以保证在个人未完成同意操作前，不收集在个人同意过程中涉及的个人信息；

注 1：如在个人表达同意前，已经填写了部分个人信息，或系统缓存了部分个人信息，在个人明确拒绝或放弃同意，或一段时间内未执行同意操作的，需采取措施自动删除相关的个人信息。

b) 个人拒绝同意后，宜采用适当的方式向个人展示、说明拒绝后的后果，如相关个人信息为提供服务所必需或个人主动触发相关业务功能，可再次向个人告知目的、拒绝同意造成的影响等，以再次取得个人同意；

c) 个人拒绝同意后，如相关个人信息并非为提供服务所必需，不以频繁询问、请求（如 48 h 内超过 1 次询问）同意方式对个人造成打扰；

注 2：个人主动选择使用某业务功能而触发的同意询问，不属于打扰情形。

d) 个人拒绝同意某业务功能处理个人信息后，不宜退出产品或服务的所有界面，宜保持原有界

面，或切换至产品或服务的基本业务功能或其他相关业务功能的界面；

e） 个人拒绝同意产品或服务的基本业务功能处理个人信息后，可切换至不涉及个人信息处理的服务模式（如静态页面、非个性化的浏览页面等）。

9.6 同意的撤回

9.6.1 撤回同意的机制设计

个人信息处理者需结合产品或服务的业务功能特点、收集个人信息的种类和方式、取得个人同意的过程等因素，设计个人撤回其同意的机制，具体包括如下内容。

a） 个人信息处理者对撤回同意的机制设计需充分考虑个人操作的便捷性，明确个人的何种操作意味着撤回同意，采取与取得同意过程类似的方法设置撤回同意的机制。

注 1：通过交互式界面提供产品或服务的，直接设置能操作的功能界面；没有交互式界面的，可提供电话、邮箱等方式响应个人撤回同意的诉求。

b） 个人信息处理者可从个人的实际需求和产品或服务的特点出发，合理设置撤回同意机制的颗粒度。通常可采取的撤回同意机制包括：

1） 个人通过撤回某个处理个人信息的业务功能来行使撤回同意权利的，个人信息处理者不能拒绝提供其他业务功能，或降低其他业务功能的服务质量，除非撤回同意的个人信息是其他业务功能所必需；

注 2：通常情况下，撤回对单个业务功能或特定目的处理个人信息的同意更符合个人使用产品或服务的习惯，不能通过将不同业务功能或不同目的进行强行捆绑的方式来设置撤回同意的机制。

2） 个人通过直接撤回处理某类个人信息的同意来行使撤回同意权利的，如明确了所撤回的具体处理目的的，个人信息处理者需暂停与此目的相关的处理活动，且不能拒绝或降低与此目的无关业务功能的服务质量；如未明确所撤回的具体处理目的的，不能拒绝提供或降低与此类个人信息无关业务功能的服务质量；

注 3：对于某个业务功能或特定目的直接能撤回的个人信息种类，采取清单勾选、开关键等方式通过交互式界面向个人展现。

注 4：个人主动选择关闭收集某类个人信息的通道，或主动向个人信息处理者设置的个人信息保护有关的投诉、举报等渠道反馈拒绝对某类个人信息的处理请求，视为对该类个人信息所有相关处理目的的撤回同意。

3） 由个人给出单独同意的个人信息处理活动，需具备与单独同意相对应的单独撤回同意机制；

4） 如因客观条件限制、撤回后对个人使用产品或服务的安全性等造成严重影响等情形，宜向个人详细说明无法直接撤回同意的理由，同时提供注销账号、停止使用产品或服务后整体删除数据等可行的方式以达到撤回同意的效果。

c） 个人信息处理者可通过一般告知的方式，在个人信息保护政策中向个人说明撤回同意的具体场景和操作方法。对于可能对个人权益造成重大影响的撤回同意，可在具体场景中以即时提示的方式向个人予以强调。

注 5：撤回同意的操作方法篇幅较长的，形成单独的文档，将其链接嵌入个人信息保护政策，或者以便于个人查找、检索的方式予以展现。

d） 个人撤回同意后，宜设计删除或匿名化相关个人信息的机制，并向个人主动告知相关机制，以供个人作出是否保留个人信息的选择。

注 6：如被撤回同意的个人信息处理活动相关的个人信息未被用于其他已同意的处理目的，则向个人说明影响，并直接提供是否进行删除的选项。

注 7：如被撤回同意的个人信息处理活动相关的个人信息被用于其他已同意的处理目的，具备技术条件的（如不同

处理目的使用独立数据库、数据表等），向个人直接提供是否进行删除的选项；不具备技术条件的（如其他处理目的与被撤回同意的处理目的共用一个数据库、数据表等），采取技术或管理措施对处理目的进行限制，明确向个人告知无法删除的个人信息种类将不再用于被撤回同意的处理目的。

9.6.2 撤回同意的实施

撤回同意的实施要点包括：

a) 个人撤回同意的范围仅限基于同意进行的个人信息处理活动，不包括基于其他合法性基础（如6.2中的情形）进行的个人信息处理活动；

b) 个人信息处理者在收到个人的撤回同意请求后，可通过验证个人身份等方式，确认提出请求者为个人本人或授权委托人；

c) 个人撤回同意后，个人信息处理者后续不能再处理相应的个人信息，但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；

d) 个人撤回同意后，需在承诺时限内（不超过15日）完成对撤回同意请求的确认，以及完成删除或匿名化相关个人信息的操作，并向个人反馈撤回同意的结果；

注1：个人发起撤回同意的请求后，至撤回同意的请求完成前，个人信息处理者不能对相关个人信息进行处理，因个人在此期间自行使用业务功能导致的个人信息处理活动除外。

注2：使用交互式界面向个人提供撤回同意的机制的，在个人执行撤回同意后，立即在后台进行处理，如无法立即处理的需向个人说明处理的时间。

e) 个人撤回同意后，个人信息处理者不采用频繁打扰等方式，反复提醒个人再次同意对个人信息的处理；

f) 个人撤回同意的范围涉及已向其他个人信息处理者提供的个人信息的，个人信息处理者需向其他个人信息处理者传达个人行使权利的诉求，或向个人提供其他个人信息处理者的申请受理机制；

g) 个人需变更同意的范围的，可通过先撤回同意后再次取得同意的方式进行变更，或直接同意新的个人信息处理规则，新的同意生效后，需中止基于此前同意的处理活动；

h) 个人信息处理者可通过投诉、举报等渠道了解个人对撤回同意的反馈，评价其实施效果，并不断补充、完善和更新撤回同意的机制，以增进撤回机制的便捷性和覆盖面。

9.7 同意的证据留存

个人信息处理者可采取技术或管理措施，留存取得个人同意过程的证据，以实现保证处理个人信息的合法性、向有关司法、监管部门提供必要证明材料，以及用于其他有助于保护个人权益和个人信息处理者合法利益的目的。证据留存的实施要点包括如下内容。

a) 个人信息处理者可选择留存的证据包括但不限于以下内容。

1) 个人信息处理者对个人信息处理活动进行评估后，设计并实施告知和同意方案的记录。记录可包括：个人信息保护影响评估实施的方案及记录、根据个人信息敏感程度及可能存在的风险等选择告知和同意方式的判断记录、告知内容的撰写与批准记录、实施后的验证与方案一致性的记录等；记录的方式可包括：个人信息处理者内部的文档或邮件记录、专业咨询机构提供的第三方意见记录等。

2) 与个人关联的同意记录。记录可包括：个人标识信息（如注册账户、真实身份信息、设备标识等）、同意的方式、同意的时间、同意的期限、同意的意见、同意对应的告知内容（如具体的个人信息处理规则）等。记录的方式可包括：直接以文件形式留存的个人同意的操作界面、与同意相关的操作日志记录、与同意有逻辑关联的数据库（或数据库中的字段）、与同

意直接相关的书面文件记录、与同意直接相关的电子签章记录等。

3) 涉及不同时期发布的需取得个人同意的个人信息保护政策、向其他个人信息处理者提供个人信息、向境外提供个人信息的规则等向个人所告知的个人信息处理规则文本及版本。

4) 涉及向其他个人信息处理者提供个人信息、与其他个人信息处理者构成共同个人信息处理者、接入其他个人信息处理者的产品或服务等的，在告知和同意过程中涉及多个角色时，除需要留存上述1)～3)中的记录外，还需要考虑到与其他个人信息处理者相关的要素；记录可包括：其他个人信息处理者的具体身份、其他个人信息处理者的个人信息处理规则、与其他个人信息处理者对告知和同意责任分配的约定记录、与其他个人信息处理者签署的合同或协议、对其他个人信息处理者的尽职调查记录等。

5) 涉及向境外提供个人信息的情形，除需要留存上述1)～4)中的记录外，还可留存的记录包括：境外接收方所处国家或地区、联系方式、与境外接收方签订的合同(如有)、与个人信息跨境提供相关的认证记录(如有)等。

b) 个人信息处理者可根据相关法律法规要求和自身举证的需要决定证据留存的时限，留存时间宜不少于3年，法律法规另有规定的除外。

c) 个人信息处理者留存同意的证据需遵循最小必要原则，避免以留存同意证据为由，扩大个人信息的收集范围。

d) 个人信息处理者需对留存证据的使用范围严格限制，不通过留存证据分析个人的习惯、意图、想法，并采取严格的访问控制措施防止留存证据被用于法律法规要求和自身举证以外的任何目的。

e) 个人信息处理者需采取充分的技术措施和其他必要措施，确保留存证据的数据安全，防止其被泄露、篡改、毁损、丢失。

f) 个人信息处理者因自身举证等目的向有关部门披露留存的证据时，以及因澄清异议或争议等目的向个人披露留存的证据时，仅披露最少必要的信息且披露的信息仅用于证明个人信息处理活动是否取得了个人同意，披露过程还需采取适当的技术或管理措施防止留存证据被无关组织或人员获知。

附 录 A
（资料性）
App 基本业务功能与扩展业务功能的告知和同意

A.1 概述

为满足用户的使用需求，App 可能提供多种类型服务，其中实现用户最主要使用目的的一种服务类型，通常被认为是为 App 的服务类型（即基础服务类型）。App 常见的服务类型见 GB/T 41391—2022 附录 A。

每种服务类型可能提供多项业务功能，按照 App 主要服务目的可分为基本业务功能和扩展业务功能。基本业务功能是 App 的基础服务类型中实现用户根本使用需求的业务功能，基本业务功能之外的其他业务功能属于扩展业务功能。用户首次使用 App 时，基本业务功能和扩展业务功能需采用不同的告知和同意实施方法，以充分保障用户的知情权和选择权。

A.2 告知的内容

除 8.2、GB/T 41391—2022 第 6 章中的相关内容外，可参考的告知内容包括：

a) App 的服务类型，以及 App 的基础服务类型外提供的其他服务类型情况（如有）；

b) App 的基本业务功能和扩展业务功能划分情况；

c) 为保障 App 基本业务功能正常运行所必需的个人信息种类及对应的处理目的；

注 1：基于法律法规要求收集的个人信息种类、目的等内容一并告知。

d) 用户开启或使用基本业务功能的方式；

注 2：通常，App 运营者采用多种方式来满足用户使用基本业务功能的需要，常见的有“游客或访客模式”“仅浏览模式”“非个性化推送服务模式”等。

e) App 扩展业务功能可能处理的个人信息种类、目的等规则。

A.3 基本业务功能告知和同意的实施

除第 8 章、第 9 章和 GB/T 41391—2022 第 6 章相关内容外，以下实施注意点可供参考。

a) App 运营者可在用户首次进入 App 时或基本业务功能开启前，通过交互式界面（如弹窗、文字说明、提示条、提示音等形式）向用户告知 App 所对应的服务类型，以及基本业务功能的开启或使用方式等，并通过简短的个人信息保护政策（指引、声明等）等告知用户基本业务功能所必需的个人信息种类、处理目的等处理规则。

b) App 运营者可提供基本业务功能模式设置项，并在用户首次使用 App 时，以显著方式展示开启或使用基本业务功能的路径，如在交互式界面提供“同意并仅使用基本业务功能”的选项。

c) App 运营者需在用户通过肯定性动作作出同意后提供基本业务功能。如用户不同意被收集基本业务功能所必需的个人信息的，App 运营者可拒绝向用户提供服务。

d) 上述内容的实现方法参考 A.5。

A.4 扩展业务功能告知和同意的实施

除第 8 章、第 9 章和 GB/T 41391—2022 第 6 章相关内容外，以下实施注意点可供参考：

a) App 运营者可在用户使用扩展业务功能前，通过交互式界面（如弹窗、文字说明、提示条等形式）向用户告知扩展业务功能的个人信息处理规则；

b) App运营者提供多个其他服务类型的，可参考A.3 a)的告知和同意方式，并由用户自主选择是否开启或使用相应的服务类型；

注：区分其他服务类型时，需从保障用户自主选择的权利角度出发，服务类型不可拆分的，需向用户说明不可拆分的原因，且确保如用户放弃开启或使用其他服务类型，不影响App基本业务功能的正常使用。

c) 用户不同意收集扩展业务功能所必需的个人信息的，不影响基本业务功能使用或降低基本业务功能的服务质量；

d) 上述内容的实现方法参考A.5。

A.5 告知和同意的方案设计示例

App运营者可参考以下示例，设计告知和同意的方案。

示例1：在用户首次进入App时，通过个人信息保护政策（指引、声明等）等告知用户提供基本业务功能模式所需的必要个人信息及相关处理规则，并为用户提供“同意”和“不同意”的选项；在用户进入到具体扩展业务功能界面前，为用户提供单独的告知内容，并为用户提供“同意”和“不同意”的选项。

示例2：在用户首次进入App时，通过个人信息保护政策（指引、声明等）等告知用户提供基本业务功能模式所需的必要个人信息及相关处理规则；同时在该界面同步列举本App涉及的扩展业务功能，以及所需的必要个人信息等内容，允许用户自行勾选。最下方为用户提供“同意”和“不同意”的选项。如用户勾选了任一扩展业务功能并点击“同意”，则视为用户主动同意开启基本业务功能与该扩展业务功能。

示例3：在用户首次进入App时，通过个人信息保护政策（指引、声明等）等对本产品所涉及的整体功能情况进行告知；如用户作出“不同意”的选择，进一步询问用户意图是否为“同意但仅使用基本业务功能”；在用户选择“仅使用基本业务功能”后，继续为用户提供基本业务功能。

示例4：在用户首次进入App时，通过弹窗等显著方式向用户说明基本业务功能所需的必要个人信息等规则，并提供直接点击即进入基本业务功能的通道。当用户主动触发扩展业务功能时，通过个人信息保护政策（指引、声明等）等方式告知被触发的扩展业务功能相关的处理规则，并为用户提供“同意”和“不同意”的选项。

附 录 B
（资料性）
App 嵌入第三方 SDK 场景下的告知和同意

B.1 概述

SDK 通常为协助 App 开发的软件库工具，用以实现 App 的具体业务功能。常见的 SDK 种类主要包括：广告类、推送类、统计类、地图类、第三方登录类、社交类、支付类、风控类、身份认证类、框架类等。

本附录中所述的 SDK 指第三方 SDK，即由 App 运营者之外的第三方所提供的 SDK。

B.2 告知的内容

App 嵌入第三方 SDK 时，除 8.2 和 GB/T 41391—2022 中 6.6.2 的相关内容外，可参考的告知内容包括：

a） SDK 的名称及其提供者名称、联系方式；

b） SDK 的个人信息处理规则。

注 1：SDK 提供者需自行如实、完整披露个人信息处理规则，App 中关于个人信息处理的告知内容需与 SDK 披露的信息保持一致；如 SDK 未披露相关信息，则 App 运营者通过与 SDK 沟通，或使用技术检测方法获知相关信息后，将其体现在告知内容中。

注 2：App 嵌入一个或多个 SDK 的，采用表格、链接文本等形式在其个人信息保护政策中逐一列举。

注 3：SDK 的个人信息处理规则（如个人信息保护政策）能链接文本等方式体现，但需保证链接文本来源的准确性，如 SDK 官网提供的链接。

B.3 告知和同意的实施

SDK 提供者与 App 运营者之间的合作模式决定了 App 就 SDK 处理个人信息进行告知和同意的实施方式。SDK 提供者有义务披露其个人信息处理规则，并与 App 运营者协作完成对使用 App 的用户进行的告知和同意。App 嵌入的 SDK 处理个人信息的，除第 8 章、第 9 章和 GB/T 41391—2022 中 6.6.2 相关内容外，以下实施注意点可供参考：

a） 当 SDK 提供者作为 App 运营者的受托处理者、根据 App 运营者的要求处理个人信息时，SDK 提供者需至少向 App 运营者披露 SDK 的个人信息处理规则，由 App 运营者向使用 App 的用户告知 SDK 的个人信息处理规则并取得用户同意后，SDK 才可处理个人信息；

注 1：如 SDK 无法触达使用 App 的用户或用户在使用 App 过程中无法感知到 SDK 的，App 协助 SDK 提供者将 SDK 需告知的内容以链接等方式置于 App 相关交互式界面或个人信息保护政策中进行展示。

b） 当 SDK 作为个人信息处理者时，SDK 提供者需向 App 运营者、使用 App 的用户披露 SDK 的个人信息处理规则。在用户使用 SDK 相关的业务功能时，在 App 的界面中或从 App 跳转至相关的业务功能界面中，可以 SDK 提供者的名义向使用 App 的用户进行相关的告知并取得其同意。

注 2：如在网上购物 App 的支付环节，使用 App 的用户点击或选中支付 SDK 的图标后，App 会跳转/展示支付功能的交互式界面，支付 SDK 在该界面上独立向用户告知支付服务的个人信息处理规则并取得用户同意（此前已经取得同意的除外）后，才能为用户提供支付服务。

注 3：App 收集个人信息后向作为个人信息处理者的 SDK 提供个人信息的，同样参考上述方法进行告知和同意；

注 4：App 协助 SDK 以设置单独界面等方式实施告知和同意的，需向 SDK 提供者同步用户作出同意的信息或记录。

c) SDK 提供者需披露 SDK 处理个人信息的具体时机，App 运营者在适配 App 的业务功能后，可在 SDK 收集个人信息之前或同步展示相应的 SDK 处理个人信息告知内容；

d) 在 App 运营者或作为个人信息处理者的 SDK 提供者没有确认取得使用 App 的用户之同意之前，App 中嵌入的 SDK 需避免收集处理个人信息，除非法律法规另有规定；

e) SDK 提供者在其个人信息处理规则发生变更后，如 5.3 中情形，需及时向 App 运营者同步告知，并参考 8.2.3 采取重新告知和同意等措施。

注 5：SDK 提供者和 App 运营者之间合作模式的变化也属于变更。

B.4 免于取得同意的情形

涉及 6.2 中的情形处理个人信息的，SDK 提供者、App 运营者可在各自的个人信息保护政策等文本中向使用 App 的用户进行告知。如 App 运营者嵌入 SDK 的目的是达成 6.2 中的情形，可进行单独说明，以确保使用 App 的用户充分知情。

附 录 C
（资料性）
处理不满 14 周岁的未成年人个人信息的告知和同意

C.1 概述

处理不满 14 周岁的未成年人个人信息前，需将个人信息处理规则告知不满 14 周岁的未成年人的监护人，并取得其父母或者其他监护人同意。

C.2 告知的内容

除 8.2 中的相关内容外，可参考的告知内容包括：

a） 不满 14 周岁的未成年人个人信息的敏感性、处理活动可能会对用户权益产生的影响；

b） 针对不满 14 周岁的未成年人个人信息所采取的特别安全保障措施；

c） 监护人管理不满 14 周岁的未成年人个人信息、行使相关权利的方式和途径；

d） 响应监护人诉求的专门渠道（如电话、邮箱等）；

e） 提示监护人正确履行监护职责；

f） 如涉及幼儿园、学校等采用自动化设备收集不满 14 周岁的未成年人个人信息的，可说明采取此类措施的合法性、正当性与必要性，必要时可提供相关的个人信息保护影响评估报告的全文或摘要。经过与监护人进行了集体沟通的，可公开告知沟通的总体情况与结论。

C.3 鉴别不满 14 周岁的未成年人和监护人身份的方式

个人信息处理者可结合产品或服务的目标人群情况，采取合理措施鉴别用户是否为不满 14 周岁的未成年人。确认用户为不满 14 周岁的未成年人，则可采取合理措施鉴别其监护人的身份。可参考的鉴别身份方式如下。

a） 产品或服务的目标人群为不满 14 周岁的未成年人的，如面向不满 14 周岁的未成年人提供教育、音视频等产品或服务的，可直接要求用户提供监护人的联络方式，并采取强度较高的方式（如要求提供身份证信息），进行监护人身份鉴别。

注 1：常用的联络方式有监护人短信、电话、邮箱等。例如，通过让不满 14 周岁的未成年人输入监护人的手机号码，将验证监护人身份的内容发送至监护人的手机上，监护人通过回复特定字段以表示确认其是否为监护人。

示例：发送内容范本示例：尊敬的用户您好！我们是×××公司。现有×××（对不满 14 周岁的未成年人信息做部分脱敏展示）申请使用我们的服务。我们根据有关法律法规规定，在收集不满 14 周岁的未成年人的个人信息前，需取得其监护人同意。如您是×××的监护人且同意我们按照我们的《个人信息保护政策》处理您孩子的个人信息的，请回复“同意”。本条短信 3 min 内有效。

注 2：个人信息处理者采取多种并行的措施完成不满 14 周岁的未成年人及其监护人的身份鉴别，避免仅因一种验证模式失效（如无法接收验证码）导致产品或服务无法使用。

b） 如产品或服务的目标人群不是不满 14 周岁的未成年人的，如金融理财、房屋交易、求职招聘等产品或服务，可在个人信息保护政策、用户服务协议等文本中告知或在服务页面声明：如用户不满 14 周岁的，需在取得监护人同意后才可使用相关产品或服务，或直接拒绝不满 14 周岁的用户注册使用。必要时，可采取验证强度较低的方式对用户身份进行鉴别，发现存在不满 14 周岁未成年人的，可在取得其监护人同意前暂停提供相关产品或服务。

注 3：鉴别的方式充分考虑不同的产品或服务在受众群体上的差异，如对所有的产品或服务都采取固定的鉴别方

式，鉴别效果可能得不到保证，用户也可能会遭受过多打扰。例如，对于购买火车票、机票的 App 而言，如用户通过登录账户后订票过程中提供的实名信息均为成年人，则无需再去鉴别用户是否为未成年人。

c) 如使用服务或产品的用户注册信息等显示为成年人用户，但个人信息处理者通过该用户在使用产品或服务中的行为特征等有合理理由推断该用户疑似为不满 14 周岁的未成年人的，则在触发一些对用户个人信息权益影响较大的操作时（如绑定第三方账号、向其他处理者提供个人信息、开通支付功能），可采用合理手段进一步鉴别用户身份，如确认用户为不满 14 周的未成年人的，后续按照未成年人进行保护。

d) 产品或服务为未成年人和监护人提供了不同服务界面或应用程序的，可直接在监护人专用服务界面或应用程序中鉴别监护人身份。

注 4：例如，在不满 14 周岁的未成年人的服务界面提示为满足国家有关儿童个人信息保护的要求，需要儿童将有关产品或服务的个人信息处理规则等信息告知其监护人，此时该儿童的终端或应用界面上已生成用于分享给其监护人的链接或二维码。儿童能分享链接或二维码至其监护人，其监护人打开该链接或扫描该二维码之后下载或进入监护人专用的服务界面或应用程序，确认其是否为儿童的监护人；此外，在监护人专用的服务界面或应用程序上完成注册并确认身份后，监护人端与儿童端通过局域网、蓝牙、移动网络等方式进行连接并确认绑定成功的，也能视为完成身份鉴别。

e) 产品或服务宜提供监护人主动申报渠道，在以上措施未能有效鉴别用户身份的情况下，监护人可主动向产品或服务提出进行补充验证。例如，设置人工服务渠道供监护人提交与被监护人相关的信息进行人工核验等。

f) 根据以上方式鉴别用户身份为不满 14 周岁未成年人的，宜根据个人信息处理活动对未成年人的影响程度，决定是否主动联系监护人以再次确认身份。例如，产品或服务收集批量儿童个人信息，或一旦处理不慎可能导致严重侵害儿童身心健康的（例如，学校为统计学生相关情况而收集其身体健康状况、生活作息习惯、家庭成员信息等），宜主动与监护人取得联系。

C.4 告知和同意的实施

除第 8 章、第 9 章相关内容外，实施要点包括如下内容。

a) 产品或服务的目标人群为不满 14 周岁的未成年人的，可使用目标人群易于理解的方式且显著的方式提示目标人群需取得其监护人同意。实施要点包括：

1) 针对不满 14 周岁的未成年人发布专门的个人信息保护政策，并在交互式界面中向其监护人增强告知处理不满 14 周岁的未成年人个人信息的种类、目的、必要性、产生的影响等规则；

2) 使用发送短信、推送消息、发送邮件等方式，向监护人发送完整的儿童个人信息处理规则；

注 1：短信内容见附录 C 中 C.3a）中示例。

3) 在采用合理手段鉴别监护人身份后，取得监护人的单独同意。

b) 产品或服务的目标人群没有限制的，需针对可能存在的儿童个人信息处理活动设计告知和同意的机制，具体包括：

1) 制定儿童个人信息处理规则，并以个人信息保护政策的一部分或其他显著方式发布；

2) 产品或服务为儿童和监护人提供了不同服务界面的，可根据不同角色分别制定告知和同意的方案；

注 2：例如，通过弹窗等方式提示使用“青少年模式”，同时，在该模式的界面增加儿童个人信息处理规则的链接等方式向儿童或其监护人进行告知，并取得监护人单独同意。

3) 如经身份鉴别确认用户为不满 14 周岁未成年人的，可参考 a）取得监护人同意的。

c) 产品或服务的目标人群为成年人，但个人信息处理者主动发现存在不满 14 周岁的未成年人用

户，或监护人主动申报某个用户为受其监护的不满 14 周岁的未成年人的，可参考 a)取得监护人同意，或直接拒绝继续提供服务并在与监护人协商一致情况下删除该用户的个人信息。

d) 涉及幼儿园、中小学校、社会教育培训机构等开展教育活动，以及游乐场等公共场所场景下收集不满 14 周岁的未成年人个人信息的，可通过信件、告示、签署协议、即时通信工具等方式向不满 14 周岁的未成年人的监护人告知该未成年人的个人信息处理规则，并取得监护人同意。

注 3：幼儿园、学校决定采用自动化设备收集未成年人信息（例如，为保障校园安全而采取监控设备、采用电子课程应用软件布置教学作业、采用物联网设备辅助教学等），在决定采用自动化设备前，开展个人信息保护影响评估，以及与监护人进行集体协商，并根据协商结果作出最终决定。

C.5 免于取得同意的情形

学校根据法律法规要求和教学管理之必需而处理不满 14 周岁的未成年人个人信息的（例如：学籍信息、考勤信息、考试成绩等），可适用 6.2.2 的情形。

附 录 D
（资料性）
智慧生活场景下的告知和同意

D.1 概述

智慧生活场景通常是指利用IoT技术，通过智慧家居、智能可穿戴设备、智能音箱等方式，收集个人或家庭成员的信息，为其提供智能化服务的场景，具体可分为智慧家居场景、运动健康场景、智能音箱场景等。

D.2 智慧家居场景下告知和同意的实施

智慧家居通常指与用户家居生活相关各种设备，包括照明设备、家用电器、各类传感器、监控摄像头、网络设备等。通常，智慧家居可连接到云服务器，由云端提供管理和服务，并通过手机、音箱等控制设备对其进行控制。通过智慧家居处理个人信息，除第8章、第9章相关内容外，实施要点包括：

a) 如智慧家居为弱界面交互的产品，其告知内容可通过建立连接的其他设备的网络可访问界面(Web UI)展示，如无线路由器、用户驻地设备(CPE)；
b) 没有界面或者初次使用不需要打开相应界面的产品，可在用户手册、说明书或者设备标签上提供告知内容相关的访问链接(如二维码)；
c) 涉及收集家庭成员个人信息的，需向当前使用设备的用户明确告知收集的目的、方式、范围；
d) 智慧家居需要激活、初始化等操作才收集个人信息的，可通过其与用户交互的App中的界面进行告知；
e) 使用智慧生活平台对智慧家居进行管理的，可通过智慧生活平台对关联、管理智慧家居时向用户告知个人信息处理规则；
f) 智慧生活平台上的智慧家居提供方为独立的个人信息处理者的(例如，提供智慧家居的第三方厂商)，需自行或由平台协助其向用户告知个人信息处理规则；
g) 如智慧家居与相关App、智慧生活平台绑定时需要处理必要个人信息的，可在绑定时或绑定后立即通过相关App、智慧生活平台向用户告知。

D.3 运动健康场景下告知和同意的实施

运动健康场景通常指为用户提供运动指导和健康服务的产品或服务，运动健康场景相关设备包括智能手表、智能手环、耳机等穿戴设备和体脂秤、血压计、健身设备等健康管理设备。通过穿戴设备和健康管理设备处理个人信息，除第8章、第9章相关内容外，实施要点包括：

a) 运动健康相关设备多为没有屏幕或屏幕尺寸受限等难以实施告知和同意的设备，个人信息处理者可通过与运动健康服务相关的App实现告知和同意；
b) 用户通过提供运动健康服务的App绑定运动健康设备前，个人信息处理者需向用户告知运动数据、健康数据等个人信息会同步到提供运动健康服务的App，并在同步前取得用户同意；如存在不同设备间数据同步、共享的场景，需向用户告知同步的设备名称、在设备间分享的信息种类、停止共享的方式等；
c) 通过运动健康平台汇聚融合用户的基础个人信息(如身高、体重等)、运动信息、健康信息等个人信息的，需在汇聚融合前告知用户并取得同意。

D.4 智能音箱场景下告知和同意的实施

智能音箱通常是指可连接网络实现播报新闻、播放音乐、互动聊天以及可能包含控制其他智能家庭设备的功能，并可采用语音等交互方式操控的音箱设备。通过智能音箱处理个人信息，除第8、9章相关内容外，实施要点包括：

a) 如智能音箱配备显示屏（可触摸或可操控）且显示屏内容可自定义的，个人信息处理者可在显示屏上展示告知内容，并取得用户同意；

b) 如智能音箱不配备显示屏，或者为了更好的阅读体验，个人信息处理者可通过（在屏幕直接显示或在印刷包装上）提供访问链接（如二维码）等方式引导用户获取告知内容，或者采用语音播报方式提示重要内容，并取得用户同意；

c) 如智能音箱支持绑定App，个人信息处理者还可在用户使用前通过绑定App，并在App启动后或账号登录时展示告知内容，并取得用户同意；

d) 如智能音箱是其他智能家居设备的控制中枢，且该智能家居设备由第三方提供，或智能音箱集成了第三方开发的应用程序的，在向第三方提供或获取第三方收集的个人信息前（例如，需要通过智能音箱将用户操作指令传输给其他设备实现操作，其他设备执行操作后返回操作结果等给智能音箱，进而播报给用户），个人信息处理者可通过智能音箱向用户告知，并取得用户同意；

e) 智能音箱为实现唤醒服务，需要监听环境声音的，在开启该功能前，需向用户清晰告知需要实现监听所需的条件以及相关机制，如是否为本地化使用麦克风的方式，是否仅监听唤醒词，是否需要向后台回传的数据（如回传，说明回传的数据类型、时机或频次），并经用户单独同意后才开启；

f) 对于允许多用户（例如，家庭不同成员）使用的智能音箱，可采用由某个家庭成员代为授权的方式取得同意。但对于需要识别用户身份后才能使用的功能（例如，支付），通常需要区分不同家庭成员并分别取得其同意。

附 录 E
（资料性）
公共场所场景下的告知和同意

E.1 概述

公共场所通常是指向社会公众开放的、供公共使用和活动的、具有人群流动性高、聚集性强等特点的各类场所，包括市政道路、建筑物、公园、广场、绿地、滨水区域等开放式空间，也包括机场、火车站、汽车站、地铁站、学校（如教室、食堂）、图书馆、博物馆、商场、店铺、餐饮娱乐场所、居民区、公共交通工具等非开放式场所。其中，部分非开放式场所主要向特定人群开放，如学校、居民区等。

E.2 告知的内容

除 8.2 中的相关内容外，可参考的告知内容包括：采集设备的名称、功能、覆盖范围、个人信息种类、处理目的、保存期限、个人行使权利的方式和程序等。

注：可能被采集的个人信息种类通常包括：人脸图像、人脸特征、步态、身份特征、常用设备唯一标识信息（如手机 MAC 地址）、位置信息（包括与其他信息相关联分析得出的位置信息）。

E.3 告知和同意的实施

除第 8 章、第 9 章相关内容外，实施要点包括如下内容。

a) 在公共场所通过设备采集个人信息时，个人信息处理者需以显著方式向用户展示个人信息处理规则。显著方式通常是指在醒目位置张贴、播放简短易懂的告知内容，同时告知获取更多相关信息的途径。具体包括：

1) 在汽车站、火车站、地铁站、机场、商场、店铺入口显著处张贴告示或在大屏幕播放个人信息处理规则；

示例 1：地铁站的告知内容范本：本地铁站安装有人脸识别系统，用于进行人群分流安检，我们承诺会保护您的人脸等信息的安全，了解个人信息处理的详细规则向询问台咨询或扫描二维码。

示例 2：商场的告知内容范本：本商场安装有视频采集系统，以便进行客流分析，客流分析过程仅统计人数，不会保存任何人脸图像、特征信息，了解个人信息处理的详细规则向询问台咨询或扫描二维码。

2) 在摄像头安装处张贴告示向用户告知简要的个人信息处理规则；

示例 3：告知内容范本：为保障用户人身财产安全，此处摄像头将记录短期内的个人影像信息，我们承诺会保护数据安全，了解详情拨打电话或扫描二维码。

3) 在人脸识别购物柜台张贴或通过屏幕展示简要的个人信息处理规则，并在用户单独同意后采集个人信息。

示例 4：告知内容范本：此购物柜支持使用刷脸支付功能，您可以自行选择是否开通，我们承诺会保护您的人脸等信息的安全，扫码查看详细的人脸信息处理规则和开通协议。

b) 在特定人群进入的非开放式场所部署设备采集个人信息的，需符合法律法规的相关规定，除 a）中的方式外，还可通过与设备相关联的 PC（个人计算机）端、App，或由问询处、管理办公室等向用户提供包含个人信息处理规则的文本，供其需要时查阅。

c) 出于公共安全目的，在公共场所安装图像采集、个人身份识别设备采集个人图像、身份识别信息的，可参考 a）中的方式向用户告知。

d) 出于公共安全之外目的在公共场所采集个人图像、身份识别信息的，需取得用户的单独同意。

单独同意的实施方法和步骤可参考9.3.4；当用户拒绝时，公共场所管理者需提供合理替代性方案，例如，人工的服务通道，无需刷脸认证的门禁，不通过人脸识别的支付方式等。

e) 在学校、幼儿园、培训中心等公共场所采集儿童个人信息的，告知和同意的实施还可参考附录C。

E.4 免于取得同意的情形

主要情形包括：

a) 根据相应职责需求，或配合监管部门，在公共场所接入安防监控系统，可适用6.2.2的情形；

b) 收集公共场所下用户自行向公众公开的本人姓名、电话、照片等个人信息的，可适用6.2.5的情形；

c) 乘坐公共交通时，公交服务提供者记录刷卡人身份识别号、刷卡时间、乘车地点和下车地点等信息，可适用6.2.1的情形。

附 录 F
（资料性）
个性化推送场景下的告知和同意

F.1 概述

个性化推送一般是指个人信息处理者利用个人信息，基于个人行为习惯、兴趣爱好或者经济、健康、信用状况等向用户有针对性地推送商品、新闻、资讯、音视频、广告等信息。仅根据热度、地区或时间流等自然排序的信息分发模式通常不属于个性化推送。

F.2 告知的内容

除 8.2 中的相关内容外，可参考的告知内容包括：

a） 实现个性化推送需处理的个人信息种类、实现个性化推送的简单原理、算法说明，如形成画像的过程、评分的要素、推送的渠道等；

注 1：使用形象、生动的示例、图示、漫画等方式描述相关原理，以增进用户对规则的理解。

b） 个性化推送由第三方提供并由第三方直接处理个人信息的，可向用户告知第三方主体身份、第三方为提供个性化推送服务所必需的个人信息种类及处理方式等；

注 2：例如，信息流推送功能由第三方提供的，在用户首次进入相关功能时向其告知该服务的提供者，并可由第三方通过链接、单独的界面等形式展示个人信息处理规则。

c） 用户管理个性化推送功能的方式，包括如何重置、修改、调整个性化推送的标签、参数，如何标注或屏蔽不感兴趣的信息、广告等；

d） 用户关闭、退出个性化推送模式、页面，或拒绝、撤回个性化推送机制的方法；

注 3：例如，向用户告知的交互式界面中提供“一键关闭”个性化推送的选项，或类似的简便易操作的方式。

注 4：主动向用户告知哪些频道、板块、页面提供了非个性化的内容，便于用户作出选择。

e） 通过用户协议、个人信息保护政策、产品功能说明文案、弹窗界面等灵活方式说明开启或关闭个性化推送可能对用户权益造成的影响。

F.3 告知和同意的实施

除第 8 章、第 9 章相关内容外，实施要点包括：

a） 以个性化推送为核心业务功能模式的产品或服务（例如资讯浏览、音视频播放、社区论坛等），可在用户首次使用其产品或服务前，通过交互设计（弹窗、文字说明、提示条、提示框、提示音）等方式向用户告知个性化推送的机制和相关内容；

b） 产品或服务通过部分业务功能、栏目、版块、频道向用户提供个性化推送的，可在用户首次使用相关功能前，通过弹窗、提示条、浮层等显著提示的方式告知；

c） 程序化广告服务提供商可在专门界面或可访问的文档中以简单通俗的方式描述程序化广告服务的基本原理，产品或服务接入程序化广告的，可在服务界面、个人信息保护政策文本中将相关内容以链接等方式予以展示；

d） 用户主动提交的信息被用于个性化推送的，需告知该信息被分发的方式或基本原理；

注 1：例如，对用户在短视频平台发布的作品、评论、点赞进行分发的，告知用户其可能会被推荐给感兴趣的其他用户。

注 2：例如，对用户通过自己的账号发布的内容，告知用户可能会将该内容推送给关注该账号或可能对该内容感兴

趣的其他账号。

e) 个人信息处理者在提供个性化推送服务时，可将个性化推送服务与非个性化推送服务进行区分，如在信息流、文章、音视频相关位置进行标识，或者在栏目、版块、频道的页面相关位置标注相关信息系通过个性化推送方式推送。

注 3：在广告联盟服务场景下，由媒介方成员标识个性化推送广告，当媒介方不具备标识的控制权时，由需求方平台进行标识。

附 录 G
（资料性）
云计算服务场景下的告知和同意

G.1 概述

云计算服务是通过网络将可伸缩、弹性的共享物理和虚拟资源池以按需自助服务的方式供应和管理的服务模式。

当云计算服务向个人用户提供服务时，云服务商作为个人信息处理者需履行个人信息告知和同意的义务。当云服务商作为组织客户（通常指以一个机构、公司、团体、群体等形式存在的客户）选定的供应商，根据组织客户的需求向其指定的个人用户提供服务时，云服务商和组织客户双方需确认服务过程中处理个人信息的合法性基础，并约定各自在服务过程中保护个人信息的职责和义务。如处理个人信息的合法性基础是基于个人用户的同意，则可由组织客户和云服务商双方约定，由其中一方或双方协作完成对个人用户的告知和同意。如需要采用在线交互方式对用户进行告知和同意的，云服务商需提供必要的技术支持。

G.2 告知的内容

除 8.2 中的相关内容外，可参考的告知内容包括：

a） 用户的账号信息，包括登录账号、手机号、其他身份鉴别信息等；

b） 用户的实名认证信息，包括个人或企业的认证信息，如姓名/组织机构名称、身份证（号码）/营业执照（编号）、手机号/邮箱等信息；

c） 用户采购、使用云计算服务过程中产生的信息，包括充值信息、交易记录、订单信息等；

d） 用户个人信息的存储地点（通常具体到城市）；

注 1：当存储地点发生变化时，同步告知用户。

e） 涉及行业特点的云计算服务，如医疗、金融、教育、交通、电商、物流、房地产，宜考虑所属行业的特点及相关的个人信息种类、处理目的、方式等要素确定告知内容；

f） 涉及软件即服务（SaaS）模式的云计算服务时，需考虑 SaaS 涉及的业务功能及相关的个人信息种类、处理目的、方式等要素确定告知内容。

注 2：SaaS 往往是直接向个人用户提供应用层的软件服务，与个人的交互情形及处理个人信息的种类较多。

G.3 告知和同意的实施

除第 8 章、第 9 章相关内容外，实施要点包括如下内容。

a） 使用在线交互方式告知和同意时，实施要点包括：

1） 当用户通过网页浏览器使用云计算服务时，需在注册（登录）界面设置个人信息保护政策的链接，用户在首次注册或登录管理控制台时，云服务商需提示用户仔细阅读个人信息保护政策的条款，并通过用户主动点击的方式取得用户同意；

2） 当用户通过客户端使用云计算服务时，需在客户端应用程序首次运行时，通过弹窗等方式提示用户仔细阅读个人信息保护政策的条款，并取得用户同意；

3） 宜向个人用户提供可视化管理其个人信息的相关权限的方式，并以适当、透明的方式使得用户享有便利可行的管理权限。

b) 使用线下书面方式告知和同意时，当组织客户、云服务商中的一方或双方与个人用户之间有线下的沟通渠道（例如，与个人用户签订线下的服务合同），可将个人信息保护政策等告知内容文本提供或展示给个人，通过个人书面签字等方式取得个人用户同意。

附 录 H
（资料性）
车内场景下的告知和同意

H.1 概述

车内场景是指通过网络连接实现汽车及汽车座舱内人车交互及系统服务的各种应用场景，包括驾驶辅助系统、信息娱乐系统、交通信息管理系统、应急救援系统等系统服务所涉及的场景。车内场景的个人信息处理者通常包括汽车制造商、零部件和软件供应商、云计算服务提供商、经销商、维修机构及车载系统服务提供商等；用户包括车主、驾驶人、乘车人（含儿童）等。随着网络技术、大数据算法能力、人工智能等技术的发展，车内场景可能会出现更多的融合模式。

H.2 告知

H.2.1 告知的内容

除 8.2 中的相关内容外，可参考的告知内容如下。

a） 处理个人信息的种类，包括车辆行踪轨迹、驾驶习惯、音频、视频、图像和生物识别特征等。

注 1：车内场景下的个人信息可能包含用户的人脸、声纹、指纹、心律等敏感个人信息。收集个人信息及敏感个人信息的情形需明确区分标识或突出显示，避免将敏感个人信息的告知和其他内容的告知混淆。

b） 处理个人信息的目的、具体情境。例如，驾驶辅助功能需要告知用户收集人脸信息用于验证用户身份、确认驾驶人驾驶状态。

c） 处理个人信息的方式或工具。

注 2：收集方式包括使用摄像头、指纹传感器、麦克风、红外传感器等传感器采集汽车座舱内的个人信息，上述信息可能包含用户的人脸、指纹、声纹、心率等信息，或通过卫星定位、通信网络等其他方式获取的车辆位置和途经路径等位置轨迹数据。

注 3：传输方式包括通过移动通信网络、无线局域网、充电桩接口等方式，向位于车外的设备、系统传输。

注 4：存储方式包括个人信息存储地点、存储期限，或者确定存储地点、存储期限的规则。例如，驾驶人个人身份验证结果将被存储于车内和移动智能终端，且不储存人脸照片；或将个人信息上传至云端储存。汽车采集的车辆位置、轨迹相关数据在车内存储设备、远程信息服务平台（TSP）中保存时间不能超过 7 天。

d） 停止处理个人信息的方式和途径。

e） 用户执行更正、备份、导出、删除、恢复车内数据的操作和限制情形，以及为完成该操作而提供的身份验证等安全认证措施。

注 5：限制情形主要指基于保证行车安全、反欺诈或其他法律法规要求，不能提供相关执行操作的情形。例如，为了保障车辆购买人的合法权益，保护驾驶人安全，汽车行驶总里程数、保养和维修记录等实时记录的真实数据不能提供修改、删除的操作方式。

H.2.2 告知的方式

车内场景下选择个人信息处理有关的规则等内容的告知方式时，除 8.1 的相关内容外，宜充分考虑车内环境、汽车驾驶场景的特殊性，以及不同用户在车内场景下的数据处理需求和场景触发的差异，结合汽车具体性能、车载系统的安装位置等合理设置，依据道路交通安全法律法规、国家及行业标准的相关规定，选择适当的告知方式。在设计告知及与用户交互的方案时，不宜设置可能干扰行车安全的机

制。车内场景下可选择的适当告知方式包括：

a) 通过车辆使用说明书、销售协议等文本，全面介绍车载系统及应用服务，并告知 H.2.1 中的告知内容；

b) 通过用户手册、车载显示面板、语音、汽车使用相关 App 等易于访问的方式向用户展示个人信息处理规则；汽车制造商及车载系统服务提供商宜在控制系统中提供上述交互式界面或其他可行的机制；

c) 存在汽车与移动智能终端互联或账号设定为可交互的情形，可选择将告知内容通过已建立连接的移动智能终端进行展示；

d) 与用户身份、生物识别特征、行踪轨迹等相关的敏感个人信息，可通过语音、视频、弹窗、提示条、提示音等显著方式引起用户的注意，告知用户收集相关敏感个人信息的目的或所依据的法律法规；

e) 可通过邮件、短信等方式补充告知临时性的个人信息处理活动及处理规则。例如，行车过程中信号缺失时收集敏感个人信息，或因法律法规等规定导致的处理规则的变化；

f) 可通过动画、音/视频等形象化的方式向车主告知。

H.2.3 告知的时机

基于车内环境、驾驶场景、告知方式等因素，可选择车内场景下告知的时机，包括：

a) 提前告知：对于用户产生重要的或易于引起异议或争端的内容，宜提前在销售协议、用户手册等文件中进行功能介绍及个人信息处理相关说明（包括个人信息处理场景清单、敏感个人信息采集说明等），以便用户理解并作出判断；同时也可通过 App、小程序、网页、二维码等渠道提供相关说明，供用户在车外及车尚未启动的场景下阅读；

b) 触发时告知：根据用户的选择，通过语音、视频、图像等方式，在保证行车安全的前提下（如控制车速、限制路径等），在触发收集个人信息的功能时对告知内容进行展示；

c) 补充告知：如因履行合同或保护人身或财产安全所必需，在未能确认用户是否已经了解告知的内容时事先收集了个人信息，需在条件具备时及时向用户补充告知。

注：例如，在人脸验证驾驶人的场景下，临时驾驶人（代驾）进入座舱时被采集了人脸信息，此时向临时驾驶人说明身份验证未通过，并告知此时采集的临时驾驶人人脸信息将在确认车辆未发生被盗等情形后予以删除。

H.3 同意

H.3.1 同意的实施

除第 9 章相关内容外，车内场景下实施同意，需要考虑车辆购买人、车辆驾驶人、乘车人的不同特点，在依据法律法规且不超出技术能力和合理成本的情况下，结合服务场景和个人信息处理活动的特性。实施要点如下。

a) 车内场景的个人信息处理活动可能对车辆购买人权益造成重大影响时，可在采购协议中设置相关条款，车辆购买人通过签署采购协议完成同意。

注 1：车辆购买人同意不能视为驾驶人也同意。

b) 宜在每次汽车启动前，说明驾驶活动所处理的个人信息，并取得车辆驾驶人的同意。如通过人脸识别验证驾驶人身份为车主时，可适当简化告知过程；识别发现为临时驾驶人（如代驾、租车等情形）的，需知个人信息处理规则，取得临时驾驶人同意。

c) 针对不同类型的车辆特点、运营模式等，宜区分车内场景中的基本业务功能和扩展业务功能以

确定同意模式，基本业务功能通常为保障正常驾驶、安全驾驶、车辆运营所必需的业务功能。

注 2：例如，收集乘车人的身高、体重、年龄等信息用于提高车内座椅的舒适度属于扩展业务功能。

注 3：在驾驶过程中，不能以干扰行车安全的方式询问用户对扩展业务功能的同意。

d) 同一车辆座舱内无法区分用户的身份时（例如，无法准确判断乘车人是否为临时乘车人或驾驶人的家庭成员），可采用代为授权方式，以保障车内场景下基本业务功能的实现。

e) 车载系统相关的 App 区别于车内场景的告知和同意机制，具体可参照附录 A 的告知和同意实施方法。

f) 针对高频率、重复模式的场景，可支持用户设置同意次数、同意期限，或设置仅在使用期间同意等多样化的同意机制。

g) 通过网络、物理接口向车外传输包含个人信息的数据需取得用户的单独同意。将清晰度转换为满足有关强制性标准的要求或已进行匿名化处理的视频、图像数据除外。

H.3.2 同意的撤回

个人信息处理者需设置便捷的机制，在不影响行车安全且不对用户或第三人造成不利影响的情况下，保障用户变更同意范围、撤回其同意的权利。

H.4 免于取得同意的情形

为应对紧急情况下保护自然人的生命健康和财产安全所必需，例如，车辆在发生交通事故将位置信息、生命体征信息等传输给急救中心及交管部门，或车辆在被盗时将位置信息、人脸识别信息等上传云端并同步至移动智能终端，可适用 6.2.3 免于取得用户同意的情形。

附 录 I
（资料性）
互联网金融场景下的告知和同意

I.1 概述

互联网金融场景主要包括互联网借贷场景和网络支付场景。

互联网借贷场景，是指商业银行等贷款机构运用互联网和移动通信等技术，基于风险数据和风险模型进行交叉验证和风险管理，线上自动受理贷款申请及开展风险评估，并完成授信审批、合同签订、贷款支付、贷后管理等业务功能环节操作，为符合条件的借款人提供用于消费、日常生产经营周转等的个人贷款和流动资金贷款。贷款机构是指有资质授权的商业银行、消费金融公司、小贷公司等在网络上提供借贷服务的机构。

网络支付场景，是指收款人或付款人通过计算机、移动终端等电子设备，依托公共网络信息系统远程发起支付指令，且付款人电子设备不与收款人特定专属设备交互，由商业银行、非银行支付机构（以下合称“支付服务机构”）为收付款人提供货币资金转移服务。

以下“金融机构”包括上述贷款机构、支付服务机构等互联网金融业务功能经营机构。

I.2 收集使用个人信息的告知和同意

金融机构收集使用个人信息的告知和同意，除第 8 章、第 9 章相关内容外，实施要点包括如下内容。

a) 贷款机构收集法律法规要求和实现服务所需的个人信息时，需将所收集的个人信息种类、使用目的等告知用户：
   1) 当贷款机构出于向用户提供授信、借款、还款等产品或服务的目的而收集使用个人信息时，需在实名认证、绑定银行账户信息、查询个人征信信息等基本业务功能开启前，向用户告知基本业务功能所收集的必要个人信息种类，包括注册用户手机号码、借款人姓名、证件种类和号码、证件有效期限、银行卡号码等，并向用户说明拒绝提供将带来的影响；
   2) 除 8.3.4 中相关内容外，互联网借贷业务功能实施告知和同意的适当时机还可以是在借款客户选择“申请借款”“立即申请”“立即借款”等类似表述后、收集借款客户个人信息前，向借款客户告知基本业务功能所收集的必要个人信息种类，以及拒绝提供将带来的影响；
   3) 当贷款机构向用户提供产品或服务的业务功能，包括话费充值、网上购物、互联网理财等，可在扩展业务功能开启前，向用户逐一告知所提供扩展业务功能及所收集的必要个人信息，并允许用户对扩展业务功能逐项选择同意开启。

b) 支付服务机构收集法律法规、部门规章、规范性文件强制要求的和实现网络支付服务所需的个人信息时，需将所收集的个人信息种类、使用目的等告知用户：
   1) 当支付服务机构出于向用户提供网络支付的基本业务功能的目的而收集使用个人信息时，需在开立支付账户或银行账户、实名认证、绑定银行账户信息、支付交易验证时，以及设立、变更、挂失密码和数字证书等基本功能开启前，向用户告知基本业务功能所收集的必要个人信息种类，包括注册用户手机号码、注册用户姓名、证件种类和号码、证件有效期限、银行卡号码等，并向用户说明拒绝提供将带来的影响；
   2) 当支付服务机构向用户提供产品或服务的扩展业务功能时，包括话费充值、信用卡还款、

互联网理财等，在扩展业务功能开启前，向用户告知所提供扩展业务功能及所收集的必要个人信息，并允许用户对扩展业务功能逐项选择同意开启，不能因用户不同意收集扩展业务功能所需个人信息，而拒绝用户使用网络支付的基本业务功能。

I.3 提供和委托处理个人信息的告知和同意

金融机构向其他个人信息处理者提供个人信息和委托第三方处理个人信息的告知和同意，除第8章、第9章相关内容外，实施要点包括如下内容。

a) 金融机构向集团内部的其他控股公司提供个人信息的，需向用户事先告知，并取得其同意。例如，在互联网借贷场景中，消费金融机构可在将消费者的相关个人信息发送给集团控股的风控机构进行授信审核前告知消费者并取得消费者的同意。

b) 金融机构通过合同、协议等方式委托第三方对个人信息进行处理，如计算机系统外包服务、科技外包服务商、广告服务、云计算服务、债务追讨、司法诉讼、法律及财务专业咨询机构、嵌入第三方SDK/API等，可采取以下措施：

1) 长期的委托服务可在个人信息保护政策、服务合同等文件中清晰说明，以供用户随时查阅；

2) 临时的委托服务可在具体业务功能予以说明，必要时可标示、提示第三方的名称。

注1：委托第三方处理之前，需充分评估第三方保护个人信息的能力，通过委托处理协议约定职责和义务，对其进行监督，并约定第三方不能私自转委托。金融机构对委托行为承担首要责任，不因委托而转移、减免。

注2：法律法规等禁止委托处理的业务功能不能进行委托处理。

I.4 免于取得同意的情形

主要情形包括：

a) 金融机构自身或者配合其他机构履行反洗钱、反恐怖融资等监管要求，在合理范围内使用、提供必要信息的，可适用6.2.2的情形；

b) 金融机构根据法律法规等要求，向有权机关、有权机关授权的监督机构报送必要信息的，可适用6.2.2的情形；

c) 金融机构为配合司法机关、清算机构、监管部门办理司法案件，提供有关的必要信息的，可适用6.2.2的情形；

d) 金融机构根据监管部门具体要求，配合其开展反赌、反诈等处理目的而已收集信息的，可适用6.2.2的情形。

附 录 J
（资料性）
网上购物场景下的告知和同意

J.1 概述

网上购物场景，是指用户通过购物网站、App 等获取商品信息后，通过电子订单方式发出购物请求，提供详细地址与联系方式，通过货到付款、第三方支付等方式完成支付，商家以快递物流方式等方式将商品送至用户的交易过程。

J.2 告知的内容

除 8.2 中的相关内容外，可参考的告知内容如下。

a) 用户的手机号码及其目的。可通过输入框背景文字等方式提示用户，引导其主动输入手机号码，避免从第三方收集其手机号码。

b) 用户与购物平台之间通信内容及其目的。例如，可在用户拨通客服电话时提示用户："为了保证服务质量，您的本次通话可能会被录音"。

c) 用户地址或地理位置信息及其目的。例如，需通过使用移动智能终端系统权限获取地理位置的，需告知具体的场景或触发的时机，用户拒绝提供权限不影响其继续使用网上购物服务。

d) 购物平台与商家约定的保护用户个人信息的相关守则、安全措施、举报渠道等。

e) 如根据有关管理规定，购买部分商品需要收集用户身份证件信息时，需明确说明收集的依据或目的、必要性、使用范围、安全保障措施和拒绝提供该信息带来的影响等。

f) 收集支付账户信息（第三方支付账号、银行卡号等）时，需明确说明收集的目的、必要性、使用范围、安全保障措施和拒绝提供该信息带来的影响等。出于方便用户长期使用而保存相关信息前，需告知保存的期限、删除的方式等。

g) 收集用户生物识别信息（如人脸信息）时，需明确说明收集的依据或目的、必要性、使用范围、安全保障措施和拒绝提供该信息带来的影响等。同时，用户拒绝后不影响其继续使用网上购物服务。

J.3 告知和同意的实施

除第 8 章、第 9 章相关内容外，实施要点包括如下内容。

a) 固定位置展示个人信息保护政策：

1) 网站主页页尾处可设置专门的个人信息保护政策链接，确保用户可随时访问个人信息保护政策内容。网页中可采用侧边栏、目录树等便于用户阅读的形式。

2) App 的交互界面设置专门的个人信息保护政策链接，确保用户可随时访问个人信息保护政策内容。例如，在 App 中设置的"隐私"相关功能界面集中展示个人信息保护政策等。

b) 变更个人信息保护政策时，需确保变更前的上一版本在网站或 App 的适当位置可被公开访问。例如，在"隐私"相关功能界面可查询历史版本的个人信息保护政策。

c) 用户自行注册账号时，以弹窗等形式向用户展示个人信息保护政策核心内容，同时提供完整的个人信息保护政策全文链接，并通过用户主动勾选或点击的形式取得用户同意。

d) 在用户访问商家界面、与商家进行沟通时，提示用户注意隐私保护，不要向商家提供网上购物

无关的个人信息。

e) 如果用户选择第三方账号登录，在为用户提供信息发布、下单支付等功能前，要求用户绑定手机号码以满足账号实名制的要求时，并向用户告知相关的依据。

f) 用户开通支付功能或增加支付方式时，如添加个人银行卡用于网上购物支付时，可在网页端或App界面提示用户了解具体的个人信息处理规则，在取得个人单独同意后才展示个人信息填写栏。

g) 用户使用售后赔付服务时，如财产、人身损害赔付等，网络购物平台可通过个人信息保护政策、用户服务协议、电话或在线客服等方式向用户明确告知索赔过程处理相关个人信息的种类、目的，并取得索赔用户的同意。

J.4 免于取得同意的情形

购物网站、App等为了向用户交付商品或服务、提供售后服务退换货等服务时向快递服务组织提供物流配送所需的订单信息、姓名、电话号码、地址等必要个人信息，可适用6.2.1“履行合同所必需”的情形。

注：需与快递服务组织约定相关个人信息的保存期限、处理目的、范围等，还能通过向其提供技术处理后的个人信息，如虚拟号码等，降低个人信息泄露、滥用等风险。

附 录 K
（资料性）
快递物流场景下的告知和同意

K.1 概述

快递物流场景下，快递服务组织提供的主要业务功能包括：用户注册/登录、下单、支付、寄件/收派员取件，快件中转、清关、转运，用户查单，收派员派件，用户取件；为实现全流程业务功能，快递服务组织需收集寄件人、收件人、快递收派员的个人信息。

K.2 告知的内容

除 8.2 中的相关内容外，可参考的告知内容包括：

a) 快递物流寄件场景中，用户下单寄件所需的个人信息、收集实名信息的原因、用户提供个人信息不详或错误可能导致的后果、营业场所收寄件视频监控、遵守禁止寄递和限制寄递物品的有关规定、物品保价规则和物品保险服务项目等；

b) 快递物流清关场景中，出入境快件报关所需的信息；

c) 快递物流转运场景中，对收件地址位于无法送达的地区需交由其他快递服务组织承运的说明，可具体到服务组织名称。

K.3 告知和同意的实施

除第 8 章、第 9 章相关内容外，实施要点包括如下内容。

a) 快递物流寄件场景处理个人信息的告知和同意。

1) 当寄递用户通过网站、App（含小程序）等进行自主下单或自行到营业场所寄递物品时，对于寄递所需的必要信息，快递服务组织可通过弹窗、页面显著提示等方式向用户告知，并通过用户自主点击及勾选等方式取得用户同意。其中必要信息包括：寄件人姓名、身份证件类型和号码等身份信息、寄件人地址、联系电话、收件人姓名（名称）、地址、联系电话、寄递物品的名称、性质、数量等。

2) 如快递服务组织在营业场所安装视频监控，可采用张贴告示等方式向进入场所人员告知。

3) 寄递用户提供个人信息不详或错误可能导致的后果、禁止寄递和限制寄递物品的有关规定、相关物品保价规则和物品保险服务项目可通过寄递服务协议及快递收派员口头告知。

4) 寄递用户通过网站、App、小程序等进行下单的，快递服务组织上门收件前，可提前通过短信、消息推送等方式通知用户关于实名信息收集、寄递物品查验的要求。

示例 1：告知内容范本：您的预约已成功，请您保持电话畅通，我们将尽快安排收派员上门取件，为了确保快件的安全运送，请配合收派员开箱检查，并准备好身份证件以进行身份查验和身份信息登记，感谢您的支持与信任。

b) 快递物流清关场景处理个人信息时（如因国际或港澳台入境快递的报关需要收集个人信息时），快递服务组织可通过短信、消息推送、弹窗、页面显著提示等方式向用户告知后，通过用户自主上传、填写等方式收集相应个人信息。

示例 2：报关信息收集告知内容范本（中国内地进境快件场景）：尊敬的用户，您好！ 您有一票通过×××寄递的快件，运单号×××。为了确保您的货物顺利清关至中国内地，根据《中华人民共和国海关对进出境快件监管办法》，您需要提供收件人身份证影印件（正反面）。上传方式如下：1.点击身份证上传专属通道×××进行上传；2.微信上传：查找并

关注×××公众号，关注成功后选择【我的】→【通关服务】上传。如已上传忽略此短信。如有疑问拨打客服热线×××，谢谢！

c) 快递物流转运场景下需委托第三方处理个人信息时（如快递服务组织对于偏远地区等无法送达的地区，通过委托第三方开展寄递服务时），可通过个人信息保护政策、寄递服务协议、电话、短信、消息推送等方式明确告知寄递用户会委托第三方处理个人信息以实现寄递目的；同时，快递服务组织需充分评估第三方保护寄递用户个人信息的能力，与其签订保密协议和数据委托处理协议，约定完成寄递服务后第三方对获取的个人信息采取删除等处理措施。

附 录 L
（资料性）
互联网房产经纪服务场景下的告知和同意

L.1 概述

互联网房产经纪服务平台，是指帮助房产经纪机构和房产从业人员通过网络向用户提供房产经纪服务，帮助用户获得线上找房、看房、带看、认证、签约、交易、支付等信息技术服务和房产经纪服务的平台（以下简称“平台”）。

房产交易金额大、周期长、风控需求高，平台必须依赖于收集和使用用户的个人身份信息、购房资格信息、房屋信息、房屋产权信息、财产状况信息、交易信息和支付信息等，对房源可售性、真实性、交易双方身份的真实性、交易资格的合法性、交易行为的有效性等进行核验和审查，以确保整个线上交易流程顺利、安全地完成。同时，平台也必须依赖于收集和使用房产从业人员的个人身份信息和作业行为信息，对从业人员的服务能力和服务行为进行评价，促进服务质量及用户和服务人员匹配效率的提升。

L.2 告知的内容

除 8.2 中的相关内容外，可参考的告知内容包括：

a） 平台如何在协作机构之间共享房源信息和求租求购或其他房产需求信息，以促成机构间协同；

b） 有房屋租购需求的用户关闭或限制服务人员通过线上拨号的方式提供咨询服务的方法。

L.3 告知和同意的实施

除第 8 章、第 9 章相关内容外，实施要点包括如下内容。

a） 针对平台一般用户：在用户首次安装/注册互联网平台的应用程序时，需设置展示个人信息处理规则的交互式界面，由用户作出主动勾选、主动点击“同意”“下一步”“继续”、滑动滑块、主动发送等动作表示同意。

b） 针对房源业主：

1） 当业主（含业主的合法授权人，下同）自行通过平台填写并提交房产信息和联系电话，拟发布房源信息时，平台宜再次通过电话向业主告知发布房产信息的影响，取得业主口头同意后再将业主信息推送给拟为其服务的经纪人，并在达成委托协议后，才能对外展示房源信息；

注 1：涉及进行口头告知、同意的采用电话录音等方式留存相关证据。

2） 当业主委托平台的房产经纪机构代为发布房源和租售房产时，房产经纪机构和经纪人需在《委托协议》签署环节对收集业主的身份信息、房屋基本信息、房屋权属信息以及联系方式信息的目的通过口头、书面或展示电子协议等方式进行告知，业主通过在纸质或线上电子协议上签字或电子签名等方式表示同意；

3） 当业主通过平台的房产经纪机构达成房屋租售协议和居间协议时，房产经纪机构和经纪人宜在协议签署环节对收集房源业主的产权证明文件、婚姻证明文件、配偶及共有权人身份证明文件等达成交易的必要信息通过口头、书面或展示电子协议等方式进行告知，业主通过在纸质或线上电子协议上签字或电子签名等方式表示同意。

c） 针对租购客户：

1） 针对在平台直接发起预约请求的客户，需设置交互式界面，明确告知用户在线发起租购咨询服务或预约看房请求时其联系方式将被推送给经纪人，以用于向用户推送满足需求的房源信息或联系带看房源；

注 2：为用户提供便捷的渠道，如交互式界面的撤回按钮或 9.6 中提及的其他方式，以支持用户随时可撤回其提供联系方式用于寻求房源目的的同意。

2） 当租购客户通过平台的房产经纪机构达成房屋租售协议和居间协议时，房产经纪机构和经纪人可在协议签署环节对收集租购客户的身份信息、联系方式等达成交易的必要信息等通过口头、书面或展示电子协议方式进行告知，业主通过在纸质或线上电子协议上签字或电子签名等方式表示同意。

d） 针对房产从业人员：

1） 平台需通过与房产经纪机构签署或确认的平台协议和平台规则等，明确房产经纪机构需向其从业人员告知平台的辅助作业应用程序收集和使用其身份和作业信息的目的、方式等规则，以协助其作业及保护作业安全性；

2） 在房产从业人员首次安装/注册平台提供的辅助作业应用程序时，需通过弹窗等增强告知的方式，向房产从业人员告知应用程序的个人信息处理规则和使用应用程序时保护租购客户个人信息的守则。

L.4 免于取得同意的情形

主要情形包括如下内容。

a） 以下情形可适用 6.2.1 的情形：

1） 为实现平台对服务规范性、服务质量的监督和把控，收集房产从业人员的个人身份信息和作业行为信息；

2） 为完成房产交易的款项托管、监管及支付、房屋价值评估、购房贷款申请、税金缴纳、房屋主管机构的网签、过户登记及行政备案，平台接受房产经纪机构的委托后，需按照相关机构的要求与资金支付公司、第三方税务服务系统、银行、评估公司、公证机构、房屋交易主管机关系统进行客户信息的共享。

b） 以下情形可适用 6.2.2 的情形：

1） 根据法律法规、部门规章、行业规范性文件的强制性要求，房产经纪机构对外发布房源前查看委托人的房屋及房屋权属证书、委托人的身份证明等有关资料，并编制房屋状况说明书；

2） 房产经纪机构为履行反洗钱等法定义务而交叉验证客户姓名、手机号、证件号码等身份信息后再向客户提供经纪服务。

附 录 M
（资料性）
个人身份认证场景下的告知和同意

M.1 概述

个人身份认证也称为“个人身份验证”或“个人身份鉴别”，是指在实际应用场景中，通过实名、实人、实证等方式，确认个体身份的过程，从而确定该个体是否具备访问某种资源、使用某项功能、获取某项服务的权利。

从认证的实际场景来区分，个人身份认证可分为离线身份认证场景和在线身份认证场景。

离线身份认证，是指通过人工判断到场人员和身份证件信息的人证同一性，或使用终端设备（如与用户有近距离交互的计算机终端、自助机、手机移动端、通关设备等），以现场采集人脸的方式配合活体检测，再通过离线人脸特征比对，完成对用户的身份认证。离线身份认证广泛应用于政务办理、酒店前台、人脸门禁/闸机、企业考勤机、自助柜机、通关核验等。在离线身份认证场景中，个人信息处理者在信息采集、验证设备中处理个人信息时应在所属离线系统中完成，不通过网络传输至其他设备和系统。

在线身份认证，是指个人信息处理者通过终端设备采集用户的身份信息，并将个人身份信息、用户所控制的口令、密码设备等其他认证因子提交给身份认证机构，由身份认证机构对用户进行身份鉴别的过程。在线身份认证的告知可参考第8章的内容实施，根据法律法规要求，在线身份认证需取得用户同意的，可参考第9章内容实施。

M.2 告知的方式和内容

M.2.1 离线身份认证场景

个人信息处理者使用离线身份认证的方式时，可参考的告知方式和内容包括：

a） 在相关离线身份认证的终端设备上，告知当前离线身份认证的实现方式、个人身份认证的目的、相关法律依据、个人信息处理范围等，并参考第8章设计告知方案；

示例1：交通出行场景下，告知内容范本为：为保障乘客的出行安全，依据“××法律法规”，请您配合工作人员进行身份认证，您的个人信息仅在本地设备上进行处理。

示例2：安全场所场景下，告知内容范本为：＜场所名称，如机房＞是安全重地闲人免进，进出＜场所名称＞请先进行身份认证，您的个人信息仅在本地设备上进行收集处理，如未能完成身份认证，则不能进入＜场所名称＞。

b） 在现场显著位置，如问讯处、柜台、管理办公室等，向用户展示相关的个人信息处理规则，供用户需要时查阅；

c） 宜提供人工核验身份的应急处置机制，防止认证设备不可用时导致用户权益受到损害；

d） 涉及收集人脸信息等敏感个人信息时，需符合法律法规的相关规定，并明确告知收集敏感个人信息的目的（如仅用于识别个人身份）、处理方式（不保存或本地保存）、范围、不提供带来的影响等关键信息。

M.2.2 在线身份认证场景

个人信息处理者使用在线身份认证的方式时，可参考的告知方式和内容包括：

a） 在相关在线身份认证的终端设备上，告知当前在线身份认证的实现方式、个人身份认证的目

的、身份认证机构名称、向身份认证机构传输的敏感个人信息种类、相关法律依据、个人信息处理范围等，并参考第8章设计告知方案；

示例1：实名认证场景下，告知内容范本为：为落实“××法律法规”的要求，＜处理者＞需收集您的××信息，用于核实您的身份。

示例2：业务功能办理场景下，告知内容范本为：您正在办理＜业务功能名＞，＜处理者＞需收集您的××信息，用于核实您的身份。

b) 在用户拒绝一种个人身份认证机制时，个人信息处理者可选择向用户展示其他身份认证的方案，或回退到无需身份认证即可提供的业务功能；

c) 个人身份认证涉及收集人脸信息等敏感个人信息的，需符合法律法规的相关规定，并明确告知收集敏感个人信息的目的（如仅用于识别个人身份）、范围、传输方式（是否传输原始图像，或仅传输经去标识化、加密等处理后的人脸特征等）、存储方式（存储期限，完成识别后是否删除原始人脸图像信息等）、安全措施、删除已被收集人脸信息的方法等。

附 录 N
（资料性）
可推定为同意的情形示例

以下情形，通常可推定为个人对个人信息处理活动表示同意。

a） 在确认个人可以收到包含个人信息处理规则的提示后，如个人信息保护政策的文本、链接、弹窗、电子邮件、信函等，个人未主动作出明示同意的操作或未明确表示拒绝，但仍继续主动执行提供个人信息的操作，例如，个人向产品或服务的反馈渠道发送包含个人信息的留言，主动向邮箱发送包含个人信息的邮件等。

注：个人通过某种渠道了解到向某个邮箱发送邮件能领取到纪念品，即便无法确认其是否在已获知个人信息保护政策的情形下，个人发送了包含姓名、地址、联系方式等个人信息的邮件，也能视为上述情形；同时，个人信息处理者在收到邮件后，通过向其发送个人信息保护政策（或链接）等方式尽可能完成自身的告知义务。

b） 个人信息处理者明确告知个人特定行为将导致收集其个人信息后，个人未主动表示拒绝继续执行操作，或未改变其当前的活动状态。例如，个人已知图像采集区域的存在而继续选择进入该区域或在该区域停留，或个人已被告知通话将被录音而继续保持通话。

c） 产品或服务具有普遍性，能够推断个人已知正常使用产品或服务所需收集的必要个人信息，个人虽未主动作出明示同意的操作，但在直接使用产品或服务时发生了收集个人信息的行为。例如，个人直接插入手机用户识别卡（SIM 卡）连接移动网络，移动运营商直接收集 SIM 卡相关标识信息。

d） 产品或服务进行升级、更新后，个人信息处理规则发生了变化，但个人自行更换了联系方式，个人信息处理者无法与个人立即取得联系进行告知，且如果中止处理个人信息将可能导致个人权益受到损害。

参 考 文 献

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

[2] 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)

[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] 中华人民共和国国家安全法(2015年7月1日第十二届全国人民代表大会常务委员会第十五次会议通过)

[5] 中华人民共和国国防法(2020年12月26日第十三届全国人民代表大会常务委员会第二十四次会议修订通过)

[6] 常见类型移动互联网应用程序必要个人信息范围规定(2021年3月22日国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局发布)

[7] 电信和互联网用户个人信息保护规定(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)

[8] 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)

[9] GB/T 41391—2022 信息安全技术 移动互联网应用程序(App)收集个人信息基本要求

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

[11] ISO/IEC DIS 29184 Information technology—Online privacy notices and consent

[12] APEC Privacy Framework,APEC,2005

[13] CWA 16113:2012 Personal data protection good practices

[14] EU General Data Protection Regulation,2016

[15] The OECD Privacy Framework,OECD,2013