



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	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 告知的适用情形	2
5.1 收集个人信息	2
5.2 提供、公开个人信息	3
5.3 处理活动等发生变更	3
5.4 其他情形	3
6 同意的适用情形	4
6.1 需取得同意的情形	4
6.2 免于取得同意的情形	4
7 告知和同意的基本原则	6
7.1 告知的基本原则	6
7.2 同意的基本原则	6
7.3 告知和同意宜考虑的要素	6
8 告知	7
8.1 告知的方式	7
8.2 告知的内容	8
8.3 告知的实施	12
9 同意	14
9.1 同意机制的选择	14
9.2 同意的实施	15
9.3 单独同意的实施	16
9.4 书面同意的实施	20
9.5 拒绝同意的实施	20
9.6 同意的撤回	21
9.7 同意的证据留存	22
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	24
附录 B (资料性) App 嵌入第三方 SDK 场景下的告知和同意	26
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	28
附录 D (资料性) 智慧生活场景下的告知和同意	31
附录 E (资料性) 公共场所场景下的告知和同意	33
附录 F (资料性) 个性化推送场景下的告知和同意	35

附录 G (资料性) 云计算服务场景下的告知和同意	37
附录 H (资料性) 车内场景下的告知和同意	39
附录 I (资料性) 互联网金融场景下的告知和同意	42
附录 J (资料性) 网上购物场景下的告知和同意	44
附录 K (资料性) 快递物流场景下的告知和同意	46
附录 L (资料性) 互联网房产经纪服务场景下的告知和同意	48
附录 M (资料性) 个人身份认证场景下的告知和同意	50
附录 N (资料性) 可推定为同意的情形示例	52
参考文献	53

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、陈湑、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、王枫、李映婧、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,也可作为监管、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。