ICS 35.040
L 80

中华人民共和国国家标准

GB/T 35273—2020
代替 GB/T 35273—2017

信息安全技术　个人信息安全规范

Information security technology—Personal information security specification

2020-03-06 发布　　2020-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 个人信息安全规范
GB/T 35273—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2020年2月第一版
*
书号:155066·1-64947

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 35273—2017《信息安全技术　个人信息安全规范》，与 GB/T 35273—2017 相比，除编辑性修改外主要技术变化如下：

——增加了“多项业务功能的自主选择”(见 5.3)；

——修改了“征得授权同意的例外”(见 5.6，2017 年版的 5.4)；

——增加了“用户画像的使用限制”(见 7.4)；

——增加了“个性化展示的使用”(见 7.5)；

——增加了“基于不同业务目所收集个人信息的汇聚融合”(见 7.6)；

——修改了“个人信息主体注销账户”(见 8.5，2017 年版的 7.8)；

——增加了“第三方接入管理”(见 9.7)；

——修改了“明确责任部门与人员”(见 11.1，2017 年版的 10.1)；

——增加了“个人信息安全工程”(见 11.2)；

——增加了“个人信息处理活动记录”(见 11.3)；

——修改了“实现个人信息主体自主意愿的方法”(见附录 C，2017 年版的附录 C)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：中国电子技术标准化研究院、北京信息安全测评中心、颐信科技有限公司、四川大学、清华大学、中国信息通信研究院、公安部第一研究所、中国网络安全审查技术与认证中心、深圳腾讯计算机系统有限公司、上海国际问题研究院、阿里巴巴(北京)软件服务有限公司、中电长城网际系统应用有限公司、阿里云计算有限公司、华为技术有限公司、强韵数据科技有限公司。

本标准主要起草人：洪延青、何延哲、杨建军、钱秀槟、陈兴蜀、刘贤刚、上官晓丽、高林、邵正强、金涛、胡影、赵冉冉、韩煜、陈湉、高磊、张晓梅、张志强、葛鑫、周晨炜、秦小伟、邵华、蔡晓丹、黄晓林、顾伟、黄劲、李媛、许静慧、赵章界、孔耀晖、范红、杜跃进、杨思磊、张亚男、叶晓俊、郑斌、闵京华、鲁传颖、周亚超、杨露、王海舟、王建民、秦颂、姚相振、葛小宇、王道奎、沈锡镛。

本标准所代替标准的历次版本发布情况为：

——GB/T 35273—2017。

引　言

近年，随着信息技术的快速发展和互联网应用的普及，越来越多的组织大量收集、使用个人信息，给人们生活带来便利的同时，也出现了对个人信息的非法收集、滥用、泄露等问题，个人信息安全面临严重威胁。

本标准针对个人信息面临的安全问题，根据《中华人民共和国网络安全法》等相关法律，规范个人信息控制者在收集、存储、使用、共享、转让、公开披露等信息处理环节中的相关行为，旨在遏制个人信息非法收集、滥用、泄漏等乱象，最大程度地保障个人的合法权益和社会公共利益。

对标准中的具体事项，法律法规另有规定的，需遵照其规定执行。

信息安全技术　个人信息安全规范

1　范围

本标准规定了开展收集、存储、使用、共享、转让、公开披露、删除等个人信息处理活动的原则和安全要求。

本标准适用于规范各类组织的个人信息处理活动，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

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 25069—2010 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各种信息。

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参见附录 A。

注 3：个人信息控制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

个人敏感信息　personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注 1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账户、通信记录和内容、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、14 岁以下(含)儿童的个人信息等。

注 2：关于个人敏感信息的判定方法和类型参见附录 B。

注 3：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的，属于个人敏感信息。

3.3

个人信息主体　personal information subject

个人信息所标识或者关联的自然人。

3.4

个人信息控制者　personal information controller

有能力决定个人信息处理目的、方式等的组织或个人。