ICS 35.040
L 80

中华人民共和国国家标准

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

2017-12-29 发布　　2018-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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

本标准由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:北京信息安全测评中心、中国电子技术标准化研究院、颐信科技有限公司、四川大学、北京大学、清华大学、中国信息安全研究院有限公司、公安部第一研究所、上海国际问题研究院、阿里巴巴(北京)软件服务有限公司、深圳腾讯计算机系统有限公司、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、钱秀槟、何延哲、左晓栋、陈兴蜀、高磊、刘贤刚、邵华、蔡晓丹、黄晓林、顾伟、黄劲、上官晓丽、赵章界、范红、杜跃进、杨思磊、张亚男、金涛、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、赵冉冉、沈锡镛。

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，规范个人信息控制者在收集、保存、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、保存、使用、共享、转让、公开披露等个人信息处理活动应遵循的原则和安全要求。

本标准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：关于个人信息的范围和类型可参见附录 A。

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、银行账号、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 周岁以下(含)儿童的个人信息等。

注 2：关于个人敏感信息的范围和类型可参见附录 B。

3.3

个人信息主体　personal data subject

个人信息所标识的自然人。

3.4

个人信息控制者　personal data controller

有权决定个人信息处理目的、方式等的组织或个人。

3.5

收集　collect

获得对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