ICS 35.040
L 80

中华人民共和国国家标准

GB/T 39335—2020

信息安全技术
个人信息安全影响评估指南

Information security technology—
Guidance for personal information security impact assessment

2020-11-19 发布　　2021-06-01 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:中国电子技术标准化研究院、四川大学、颐信科技有限公司、深圳市腾讯计算机系统有限公司、华为技术有限公司、全知科技(杭州)有限责任公司、北京腾云天下科技有限公司、国家金融IC卡安全检测中心、强韵数据科技有限公司、中国信息通信研究院、北京信息安全测评中心、联想(北京)有限公司、清华大学、阿里巴巴(北京)软件服务有限公司、中国软件评测中心、浙江蚂蚁小微金融服务集团股份有限公司、陕西省网络与信息安全测评中心。

本标准主要起草人:洪延青、何延哲、胡影、高强裔、陈湉、赵冉冉、刘贤刚、皮山杉、黄劲、葛梦莹、范为、宁华、葛鑫、周顿科、高磊、李汝鑫、秦颂、兰晓、陈舒、陈兴蜀、金涛、秦博阳、高志民、顾伟、白利芳、白晓媛、张谦、王伟光、贾雪飞、冯坚坚、朱信铭、王艳红、李怡。

信息安全技术
个人信息安全影响评估指南

1 范围

本标准给出了个人信息安全影响评估的基本原理、实施流程。

本标准适用于各类组织自行开展个人信息安全影响评估工作，同时可为主管监管部门、第三方测评机构等组织开展个人信息安全监督、检查、评估等工作提供参考。

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 20984 信息安全技术 信息安全风险评估规范

GB/T 25069—2010 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

3 术语和定义

GB/T 25069—2010、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。

[GB/T 35273—2020，定义 3.1]

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。

[GB/T 35273—2020，定义 3.2]

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。

[GB/T 35273—2020，定义 3.3]

3.4

个人信息安全影响评估 personal information security impact assessment

针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。