ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 41817—2022

信息安全技术　个人信息安全工程指南

Information security technology—Guidelines for personal information security engineering

2022-10-12 发布　　2023-05-01 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、华为技术有限公司、北京百度网讯科技有限公司、深圳市腾讯计算机系统有限公司、阿里巴巴(北京)软件服务有限公司、联想(北京)有限公司、蚂蚁科技集团股份有限公司、上海市方达(北京)律师事务所、北京京东尚科信息技术有限公司、北京三快科技有限公司、中国银行股份有限公司、中电长城网际系统应用有限公司、微软(中国)有限公司、全知科技(杭州)有限责任公司、北京奇虎科技有限公司、北京字节跳动科技有限公司、贝壳找房(北京)科技有限公司、北京小桔科技有限公司、勤智数码科技股份有限公司、陕西省网络与信息安全测评中心、西安电子科技大学、北京邮电大学、上海工业控制安全创新科技有限公司、华东师范大学、浙江鹏信信息科技股份有限公司。

本文件主要起草人：刘贤刚、胡影、徐羽佳、范为、孙硕、郭铁涛、李汝鑫、贾雪飞、王昕、王佳敏、苏丹、白晓媛、武杨、赵冉冉、杨建媛、严少敏、刘笑岑、罗治兵、陈雪秀、白阳、周晨炜、刘行、王姣、王秉政、闵京华、王劲松、章娅玮、张冰烨、张屹、刘凯红、张朝、衣强、孙铁、李正、李俊、裴庆祺、魏玉峰、朱通、邓婷、孙彦、陈舒、张宇光、徐国爱、蒲戈光、刘虹、陈铭松、邹楠。

引　言

为规范网络产品和服务个人信息处理活动，最大程度保障用户个人信息权益，业界陆续提出个人信息安全措施与产品和服务同步规划、同步建设、同步使用的理念。例如，欧盟《通用数据保护条例》规定在产品设计阶段要考虑个人信息保护要求，同时产品默认设置也要最大程度保护用户个人信息。这不仅有助于主动防御个人信息安全风险，也便于预防侵害用户个人信息权益事件发生。

本文件根据个人信息保护法律法规和政策标准要求，结合国内外在隐私工程方面的实践经验，给出了具有处理个人信息功能的网络产品和服务在规划和建设阶段的个人信息安全工程实施指南，为帮助网络产品和服务提升个人信息保护能力提供工程化指引。

信息安全技术　个人信息安全工程指南

1　范围

本文件提出了个人信息安全工程的原则、目标、阶段和准备，提供了网络产品和服务在需求、设计、开发、测试、发布阶段落实个人信息安全要求的工程化指南。

本文件适用于涉及个人信息处理的网络产品和服务（含信息系统），为其同步规划、同步建设个人信息安全措施提供指导，也适用于组织在软件开发生存周期开展隐私工程时参考。

注：在不引起混淆的情况下，本文件中的“网络产品和服务”简称为“产品服务”。

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

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

3　术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

个人信息安全工程　personal information security engineering

将个人信息安全原则和要求融入到产品服务规划、建设的每个阶段，使个人信息安全要求在产品服务中有效落实的工程化过程。

注：也称“隐私工程”。

3.2

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，检验个人信息处理目的、处理方式是否合法、正当、必要，判断其对个人合法权益的影响及安全风险，以及评估所采取的个人信息保护措施有效性的过程。

注：也称“个人信息安全影响评估”。

3.3

个人信息处理活动　personal information processing

对个人信息的收集、存储、使用、加工、传输、提供、公开、删除等行为。

3.4

自动化决策　automated decision-making

通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。