ICS 35.040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 28828—2012

信息安全技术 公共及商用服务信息系统 个人信息保护指南

Information security technology—Guideline for personal information protection within information system for public and commercial services

2012-11-05 发布　　2013-02-01 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

本指导性技术文件按照 GB/T 1.1—2009 给出的规则起草。

本指导性技术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。

本指导性技术文件起草单位:中国软件评测中心、北京赛迪信息技术评测有限公司、中国信息安全测评中心、中国电子技术标准化研究院、大连软件行业协会、中国软件行业协会、中国互联网协会、中国通信企业协会通信网络安全专业委员会、北京金山安全软件有限公司、深圳市腾讯计算机系统有限公司、北京奇虎科技有限公司、北京新浪互联信息服务有限公司、北京百合在线科技有限公司、上海花千树信息科技有限公司、北京百度网讯科技有限公司。

本指导性技术文件主要起草人:高炽扬、李守鹏、朱璇、杨建军、罗锋盈、何伟起、郭涛、彭勇、严霄凤、刘陶、朱信铭、王芳、郭臣、唐刚、张宏伟、唐旺、刘淑鹤、张博、王颖、孙鹏、曹剑、尹宏、王开红。

本指导性技术文件为首次制定。

引　言

随着信息技术的广泛应用和互联网的不断普及，个人信息在社会、经济活动中的地位日益凸显，滥用个人信息的现象随之出现，给社会秩序和个人切身利益带来了危害。为促进个人信息的合理利用，指导和规范利用信息系统处理个人信息的活动，制定本指导性技术文件。

信息安全技术
公共及商用服务信息系统
个人信息保护指南

1 范围

本指导性技术文件规范了全部或部分通过信息系统进行个人信息处理的过程，为信息系统中个人信息处理不同阶段的个人信息保护提供指导。

本指导性技术文件适用于指导除政府机关等行使公共管理职责的机构以外的各类组织和机构，如电信、金融、医疗等领域的服务机构，开展信息系统中的个人信息保护工作。

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/Z 20986—2007 信息安全技术 信息安全事件分类分级指南

3 术语和定义

GB/Z 20986—2007 中界定的以及下列术语和定义适用于文件。

3.1

信息系统 information system

计算机信息系统，由计算机(含移动通信终端)及其相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

注：改写 GB/Z 20986—2007，定义 2.1。

3.2

个人信息 personal information

可为信息系统所处理、与特定自然人相关、能够单独或通过与其他信息结合识别该特定自然人的计算机数据。

注：个人信息可以分为个人敏感信息和个人一般信息。

3.3

个人信息主体 subject of personal information

个人信息指向的自然人。

3.4

个人信息管理者 administrator of personal information

决定个人信息处理的目的和方式，实际控制个人信息并利用信息系统处理个人信息的组织和机构。

3.5

个人信息获得者 receiver of personal information

从信息系统获取个人信息，并对获得的个人信息进行处理的个人、组织和机构。