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。

3.6

第三方测评机构　third party testing and evaluation agency

独立于个人信息管理者的专业测评机构。

3.7

个人敏感信息　personal sensitive information

一旦遭到泄露或修改，会对标识的个人信息主体造成不良影响的个人信息。

注：各行业个人敏感信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定。个人敏感信息可以包括身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等。

3.8

个人一般信息　personal general information

除个人敏感信息以外的个人信息。

3.9

个人信息处理　personal information handling

处置个人信息的行为，包括收集、加工、转移、删除。

3.10

默许同意　tacit consent

在个人信息主体无明确反对的情况下，认为个人信息主体同意。

3.11

明示同意　expressed consent

个人信息主体明确授权同意，并保留证据。

4　个人信息保护概述

4.1　角色和职责

4.1.1　综述

信息系统个人信息保护实施过程中涉及的角色主要有个人信息主体、个人信息管理者、个人信息获得者和第三方测评机构，其职责见4.1.2～4.1.5。

4.1.2　个人信息主体

在提供个人信息前，要主动了解个人信息管理者收集的目的、用途等信息，按照个人意愿提供个人信息；发现个人信息出现泄露、丢失、篡改后，向个人信息管理者投诉或提出质询，或向个人信息保护管理部门发起申诉。

4.1.3　个人信息管理者

负责依照国家法律、法规和本指导性技术文件，规划、设计和建立信息系统个人信息处理流程；制定个人信息管理制度、落实个人信息管理责任；指定专门机构或人员负责机构内部的个人信息保护工作，接受个人信息主体的投诉与质询；制定个人信息保护的教育培训计划并组织落实；建立个人信息保护的内控机制，并定期对信息系统个人信息的安全状况、保护制度及措施的落实情况进行自查或委托独立测评机构进行测评。

管控信息系统个人信息处理过程中的风险，对个人信息处理过程中可能出现的泄露、丢失、损坏、篡改、不当使用等事件制定预案；发现个人信息遭到泄露、丢失、篡改后，及时采取应对措施，防止事件影响进一步扩大，并及时告知受影响的个人信息主体；发生重大事件的，及时向个人信息保护管理部门通报。

接受个人信息保护管理部门对个人信息保护状况的检查、监督和指导，积极参与和配合第三方测评机构对信息系统个人信息保护状况的测评。

4.1.4 个人信息获得者

依据个人信息主体的意愿处理个人信息。

当个人信息的获取是出于对方委托加工等目的，个人信息获得者要依照本指导性技术文件和委托合同，对个人信息进行加工，并在完成加工任务后，立即删除相关个人信息。

4.1.5 第三方测评机构

从维护公众利益角度出发，根据个人信息保护管理部门和行业协会的授权，或受个人信息管理者的委托，依据相关国家法律、法规和本指导性技术文件，对信息系统进行测试和评估，获取个人信息保护状况，作为个人信息管理者评价、监督和指导个人信息保护的依据。

4.2 基本原则

个人信息管理者在使用信息系统对个人信息进行处理时，宜遵循以下基本原则：

a) 目的明确原则——处理个人信息具有特定、明确、合理的目的，不扩大使用范围，不在个人信息主体不知情的情况下改变处理个人信息的目的。

b) 最少够用原则——只处理与处理目的有关的最少信息，达到处理目的后，在最短时间内删除个人信息。

c) 公开告知原则——对个人信息主体要尽到告知、说明和警示的义务。以明确、易懂和适宜的方式如实向个人信息主体告知处理个人信息的目的、个人信息的收集和使用范围、个人信息保护措施等信息。

d) 个人同意原则——处理个人信息前要征得个人信息主体的同意。

e) 质量保证原则——保证处理过程中的个人信息完整、准确、可用，并处于最新状态。

f) 安全保障原则——采取适当的、与个人信息遭受损害的可能性和严重性相适应的管理措施和技术手段，保护个人信息安全，防止未经个人信息管理者授权的检索、披露及丢失、泄露、损毁和篡改个人信息。

g) 诚信履行原则——按照收集时的承诺，或基于法定事由处理个人信息，在达到既定目的后不再继续处理个人信息。

h) 责任明确原则——明确个人信息处理过程中的责任，采取相应的措施落实相关责任，并对个人信息处理过程进行记录以便于追溯。

5 信息处理过程中的个人信息保护

5.1 概述

信息系统中个人信息的处理过程可分为收集、加工、转移、删除4个主要环节。对个人信息的保护贯穿于4个环节中：

a) 收集指对个人信息进行获取并记录。

b) 加工指对个人信息进行的操作，如录入、存储、修改、标注、比对、挖掘、屏蔽等。

c) 转移指将个人信息提供给个人信息获得者的行为，如向公众公开、向特定群体披露、由于委托他人加工而将个人信息复制到其他信息系统等。

d) 删除指使个人信息在信息系统中不再可用。

5.2 收集阶段

5.2.1 收集个人信息要具有特定、明确、合理的目的。

5.2.2 收集前要采用个人信息主体易知悉的方式，向个人信息主体明确告知和警示如下事项：

a) 处理个人信息的目的；

b) 个人信息的收集方式和手段、收集的具体内容和留存时限；

c) 个人信息的使用范围，包括披露或向其他组织和机构提供其个人信息的范围；

d) 个人信息的保护措施；

e) 个人信息管理者的名称、地址、联系方式等相关信息；

f) 个人信息主体提供个人信息后可能存在的风险；

g) 个人信息主体不提供个人信息可能出现的后果；

h) 个人信息主体的投诉渠道；

i) 如需将个人信息转移或委托于其他组织和机构，要向个人信息主体明确告知包括但不限于以下信息：转移或委托的目的，转移或委托个人信息的具体内容和使用范围，接受委托的个人信息获得者的名称、地址、联系方式等。

5.2.3 处理个人信息前要征得个人信息主体的同意，包括默许同意或明示同意。收集个人一般信息时，可认为个人信息主体默许同意，如果个人信息主体明确反对，要停止收集或删除个人信息；收集个人敏感信息时，要得到个人信息主体的明示同意。

5.2.4 只收集能够达到已告知目的的最少信息。

5.2.5 要采用已告知的手段和方式直接向个人信息主体收集，不采取隐蔽手段或以间接方式收集个人信息。

5.2.6 持续收集个人信息时提供相关功能，允许个人信息主体配置、调整、关闭个人信息收集功能。

5.2.7 不直接向未满16周岁的未成年人等限制民事行为能力人或无行为能力人收集个人敏感信息，确需收集其个人敏感信息的，要征得其法定监护人的明示同意。

5.3 加工阶段

5.3.1 不违背收集阶段已告知的使用目的，或超出告知范围对个人信息进行加工。

5.3.2 采用已告知的方法和手段。

5.3.3 保证加工过程中个人信息不被任何与处理目的无关的个人、组织和机构获知。

5.3.4 未经个人信息主体明示同意，不向其他个人、组织和机构披露其处理的个人信息。

5.3.5 保证加工过程中信息系统持续稳定运行，个人信息处于完整、可用状态，且保持最新。

5.3.6 个人信息主体发现其个人信息存在缺陷并要求修改时，个人信息管理者要根据个人信息主体的要求进行查验核对，在保证个人信息完整性的前提下，修改或补充相关信息。

5.3.7 详细记录个人信息的状态，个人信息主体要求对其个人信息进行查询时，个人信息管理者要如实并免费告知是否拥有其个人信息、拥有其个人信息的内容、个人信息的加工状态等，除非告知成本或者请求频率超出合理的范围。

5.4 转移阶段

5.4.1 不违背收集阶段告知的转移目的，或超出告知的转移范围转移个人信息。

5.4.2 向其他组织和机构转移个人信息前，评估其是否能够按照本指导性技术文件的要求处理个人信息，并通过合同明确该组织和机构的个人信息保护责任。

5.4.3 保证转移过程中，个人信息不被个人信息获得者之外的任何个人、组织和机构所获知。

5.4.4 保证转移前后，个人信息的完整性和可用性，且保持最新。

5.4.5 未经个人信息主体的明示同意，或法律法规明确规定，或未经主管部门同意，个人信息管理者不得将个人信息转移给境外个人信息获得者，包括位于境外的个人或境外注册的组织和机构。

5.5 删除阶段

5.5.1 个人信息主体有正当理由要求删除其个人信息时，及时删除个人信息。删除个人信息可能会影响执法机构调查取证时，采取适当的存储和屏蔽措施。

5.5.2 收集阶段告知的个人信息使用目的达到后，立即删除个人信息；如需继续处理，要消除其中能够识别具体个人的内容；如需继续处理个人敏感信息，要获得个人信息主体的明示同意。

5.5.3 超出收集阶段告知的个人信息留存期限，要立即删除相关信息；对留存期限有明确规定的，按相关规定执行。

5.5.4 个人信息管理者破产或解散时，若无法继续完成承诺的个人信息处理目的，要删除个人信息。删除个人信息可能会影响执法机构调查取证时，采取适当的存储和屏蔽措施。

参 考 文 献

[1] 中华人民共和国计算机信息系统安全保护条例(国务院令第147号),1994
[2] 中华人民共和国计算机信息网络国际联网管理暂行规定(国务院令第195号),1996
[3] 中华人民共和国计算机信息网络国际联网管理暂行规定实施办法,1997
[4] 欧盟电子通讯领域个人数据处理及个人隐私保护指令2002/58/EC, 2002
[5] OECD关于保护隐私和个人数据跨国流通的建议,2007

中华人民共和国
国家标准化指导性技术文件
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
GB/Z 28828—2012

*

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(100013)
北京市西城区三里河北街16号(100045)

网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 0.75 字数 12千字
2013年2月第一版 2013年2月第一次印刷

*

书号:155066·1-45996 定价 16.00元

GB/Z 28828-2012

打印日期:2013年3月4日 F053