

ICS 35.040
CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/Z 28828-2012

**Information security technology -- Guideline for personal
information protection within information system for public and
commercial services
(English Translation)**

Issued on: November 5, 2012

Implemented on: February 1, 2013

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine of the People's Republic of China**

Table of Contents

Foreword...	3
Introduction...	4
1 Scope...	5
2 Normative References...	5
3 Terms and Definitions...	5
4 Overview of Personal Information Protection...	7
5 Personal Information Protection During Information Handling...	10
Bibliography...	14

Foreword

This Standard is drafted according to the rules given in GB/T 1.1-2009.

This Standard shall be under the jurisdiction of National Technical Committee on Information Technology Security of Standardization Administration of China (SAC/TC 260).

Drafting organizations of this Standard. China Software Testing Center, Beijing CCID Information Technology Testing Co., Ltd., China Information Technology Security Evaluation Center, China Electronics Standardization Institute, Dalian Software Industry Association, China Software Industry Association, China Internet Association, Specialized Committee for Communication Network Security of China Association of Communications Enterprises, Beijing Kingsoft Security Software Co., Ltd., Shenzhen Tencent Computer System Co., Ltd., Beijing Qihoo Science and Technology Co., Ltd., Beijing Sina Internet Information Service Co., Ltd., Beijing Baihe Online Technology Co., Ltd., Jiayuan.com. Co., Ltd. AND Beijing Baidu Netcom Co., Ltd.

Chief drafting staffs of this Standard. Gao Chiyang, Li Shoupeng, Zhu Xuan, Yang Jianjun, Luo Fengying, He Weiqi, Guo Tao, Peng Yong, Yan Xiaofeng, Liu Tao, Zhu Xinming, Wang Fang, Guo Chen, Tang Gang, Zhang Hongwei, Tang Wang, Liu Shuhe, Zhang Bo, Wang Ying, Sun Peng, Cao Jian, Yin Hong and Wang Kaihong.

This Standard is formulated for the first time.

Introduction

With extensive application of the information technology and continuous popularization of the internet, the role of personal information becomes more and more important in social and economic activities, however, the phenomenon that personal information is misused still appears, which damages the social order and personal vital interest. With a view to promote the reasonable utilization of personal information, guide and standardize the activity to treat personal information by way of the information system, this Standard is formulated.

Information Security Technology - Guideline for
Personal Information Protection within Information
System for Public and Commercial Services

1 Scope

This Standard specifies the process that personal information is wholly or partially handled by way of the information system, and provides guidance for the protection of personal information in different stages for personal information handling in the information system.

This Standard is applicable to the protection of personal information in the information system performed by various organizations and institutes, except government agencies and institutes that exercise public administration duty, such as service institutions in telecommunication, finance and medical treatment.

2 Normative References

The following documents are essential for the application of this document. For dated reference, only the edition cited applies. For undated references, the latest edition (including any amendments) applies.

GB/Z 20986-2007 Information Security Technology - Guidelines for The Category and Classification of Information Security Incidents

3 Terms and Definitions

For the purpose of this Standard, the terms and definitions in GB/Z 20986-2007 and the followings apply.

3.1

Information system

Computer information system that is composed of computer (including mobile communication terminal), its associated equipment, and supporting equipment and facility (including network); a man-machine system that collects, handles, stores, transmits and retrieves the information according to certain application goal and rules.

Note: It is revised from that defined in 2.1 of GB/Z 20986-2007.

3.2

Personal information

Computer data which may be handled by the information system; it is relative to specific natural person and capable of identifying such specific natural person separately or by combining with other information.

Note: Personal information may be divided into personal sensitive information and personal general information.

3.3

Subject of personal information

The natural person directed by personal information.

3.4

Administrator of personal information

Institution and organization that determines the purpose and method to handle personal information, controls personal information actually and handles personal information by way of information system.

3.5

Receiver of personal information

Person, institution and organization which obtain personal information from the

information system and handle the personal information obtained.

3.6

Third party testing and evaluation agency

The professional testing and evaluation agency independent of administrator of personal information.

3.7

Personal sensitive information

The personal information which may, in case of being disclosed or modified, cause adverse impact on labeled subject of personal information.

Note: Specific contents of personal sensitive information for each industry are determined according to the willing of subject of personal information who accepts relevant services and characteristics of respective businesses. Personal sensitive information may include ID card No., mobile phone No., race, politic viewpoint, religious belief, gene and fingerprint etc.

3.8

Personal general information

The personal information except personal sensitive information.

3.9

Personal information handling

Behavior that handles personal information, including collecting, processing, transferring and deleting.

3.10

Tacit consent

The case that subject of personal information is considered to consent where no explicit objection is proposed.

3.11

Expressed consent

The case that subject of personal information authorizes to agree and evidences are reserved.