GB

NATIONAL STANDARD GUIDING TECHNICAL DOCUMENT

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80

GB/Z 28828-2012

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

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

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;

Standardization Administration of the People's Republic of China.

Table of Contents

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 Tecent 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.

4 Overview of Personal Information Protection

4.1 Roles and responsibilities

4.1.1 Overview

Those involved in the protection of personal information in the information system mainly include subject of personal information, administrator of personal information, receiver of personal information and third party testing and evaluation agency; their responsibilities are as shown in 4.1.2~4.1.5.

4.1.2 Subject of personal information

Before providing personal information, subject of personal information shall proactively learn about the goal and purpose for collection by administrator of personal information, and provide personal information according to personal willingness. If finding any disclosure, losing and falsifying of personal information, complain to or put forward the inquiry to the administrator of personal information OR

5 Personal Information Protection During Information Handling

5.1 Overview

Handling process of personal information in the information system may be divided into 4 key links - collecting, processing, transferring and deleting. Protection of personal information runs through these 4 links:

a) Collecting: it refers to acquiring and recording personal information.

b) Processing: it refers to operation on personal information, including typing in, storing, modifying, labeling, comparing, mining and shielding etc.

c) Transferring: it refers to the conduct to provide personal information to receiver of personal information, such as publicizing to the public, disclosing to specific groups, copying personal information to other information systems since personal information is entrusted to others to process.

d) Deleting: it refers to making personal information unavailable or not useable in the information system.

5.2 Stage of collecting

5.2.1 Personal information collecting shall be specific, clear and reasonable.

5.2.2 Prior to collecting, subject of personal information shall be informed and warned of the following matters in the method familiar to subject of personal information:

a) The purpose of personal information handling;

b) Collecting method and means, specific contents and remaining duration of personal information;

c) Application scope of personal information, including disclosing or the scope for providing personal information to other agencies and organizations;

d) Protective measures of personal information;

e) Name, address, contact information and other relevant information of administrator of personal information;

f) Possible risk in case subject of personal information have provided personal information;

g) Possible consequence in case subject of personal information doesn't provide personal information;

h) Complaint channel of subject of personal information;

i) If it is required to transfer or entrust personal information to other agencies and organizations, subject of personal information shall be informed of the following information (included but not limited to): purpose of transferring or entrusting, specific contents and application scope concerning personal information transferring or entrusting as well as name, address and contact information of receiver of personal information accepting entrust.

5.2.3 Consent by subject of personal information shall be acquired prior to personal information handling, including tacit consent or expressed consent. In case of personal general information collecting, it may be considered that subject of personal information has shown tacit consent; if subject of personal information shows clear opposition, personal information shall not be collected further or shall be deleted; expressed consent by subject of personal information shall be acquired in case of personal sensitive information collecting.

5.2.4 It is only allowed to collect the minimal information which is capable of realizing the known purpose.

5.2.5 Personal information shall be collected from subject of personal information by informed means and in informed ways, and concealed means or indirect way is not allowed.

5.2.6 Associated functions shall be provided in case personal information is collected continuously; subject of personal information is allowed to configure, adjust and close the function in collecting personal information.

5.2.7 It is not allowed to collect personal sensitive information from juniors younger than 16 years old and other person with limited civil capacity or person under disability; if it is necessary to collect the personal sensitive information of such person, expressed consent by their legal guardian shall be acquired.

5.3 Stage of processing

5.3.1 Process personal information without prejudice to the application purpose informed or by exceeding the informing scope.

5.3.2 Adopt methods and means having been informed.

5.3.3 Ensure personal information is not acquired by any individual, agency and organization irrelevant to handling purpose.

5.3.4 Do not disclose personal information handled by subject of personal

Bibliography

[1] Security Protection Regulations of Computer Information System of the People's Republic of China (the State Council Decree No. 147), 1994

[2] Temporary Provisions on International Network Management of Computer Information System of the People's Republic of China (the State Council Decree No.195), 1996

[3] Implemention Measure for Temporary Provisions on International Network Management of Computer Information System of the People's Republic of China, 1997

[4] Directive of EU on Personal Data Processing And Individual Privacy Protection in Electro-communication Field 2002/58/EC, 2002

[5] OECD Suggestion on Privacy and Personal Data Protection In Multinational Circulation

END

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------