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 -- Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems

("Guidelines")

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。

With the extensive application of Information Technology (IT) and the ever-growing popularity of the Internet, personal information plays an increasingly prominent role in the social and economic activities. At the same time, the phenomenon of misusing personal information also appears, and brings harm to the social order and personal interests.

This technical guidance document is hereby made in order to promote the rational use of personal information, guide and regulate the activities of using information systems (IS) to process personal information.

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 -- Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems

1 范围

1 Scope

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。

This technical guidance document regulates all or part of the process of processing personal information through information systems. It provides guidance on personal information protection at different stages of personal information processing in information systems.

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。

This guidance document applies to all kinds of organizations and institutions other than the government agencies and other institutions which exercise public management responsibilities, such as service institutions in the fields of telecommunication, finance, medical treatment and other areas, to carry out their work in protecting personal information in information systems.

2 规范性引用文件

2 Normative references

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/T 20269-2006 信息安全技术 信息系统安全管理要求

GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南

The following documents are essential for the application of this document. For any dated reference, only the dated version is applicable to this document. For any undated reference, the latest version (including all amendments) applies to this document.

GB / T 20269-2006 Information security technology Information system security management requirements

GB / Z 20986-2007 Information Security technology Guideline on classification and grading of information security incident

3 术语和定义

3 Terms and definitions

GB/T 20269-2006 和 GB/Z 20986-2007 中界定的以及下列术语和定义适用于本技术性指导文件。

The terms and definitions defined in GB / T 20269-2006 and GB / Z 20986-2007, and those defined as below, apply to this technical guidance documents.

3.1信息系统 information system

即计算机信息系统,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,能够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。

3.1 Information System

Namely, computer information systems, consisted of the computers (including mobile communication terminal) and the relevant ancillary equipment and facilities (including network), which can conduct information collection, processing, storage, transmission, retrieval and so forth in accordance with certain application objectives.

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。个人信息可以分为个人 敏感信息和个人一般信

息。

3.2. Personal Information

Mean the computer data, that may be processed by an information system, is relevant to a certain natural person, and that may be used solely or along with other information to identify such natural person. Personal information can be divided into sensitive personal information and general personal information.

3.3个人信息主体 subject of personal information

个人信息指向的自然人。

3.3. Subject of personal information

The natural person that the personal information points to.

3.4个人信息管理者 administrator of personal information

3.4 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。

Namely, the organizations and institutions, which determine the purpose and manner of personal information processing, actually control personal information and use information system to process personal information.

3.5 个人信息获得者 receiver of personal information

从信息系统获取个人信息的个人、组织和机构,依据个人信息主 体的意愿对获得的个人信息进行处理。

3.5. Receiver of personal of personal information

Namely, the individuals, organizations and institutions, which obtain personal information from information system, and handle/process obtained personal information in accordance with the desire/willingness of the subject of personal information.

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。

3.6. Third party testing and evaluation agency

Namely, professional evaluation agency, which is independent from the personal information administrator

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。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。例如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。

3.7. Personal sensitive information

Namely, the information that would have an adverse impact on the subject of personal information if disclosed or altered. The specific contents of sensitive personal information of various industries shall be determined in accordance with the main desires of the subject of personal information accepting the services and the unique characteristics of the individual industry. For example, the sensitive personal information may include identity card numbers, mobile phone numbers, race, political viewpoint, religion, or biometric information (/gene), fingerprint and so forth.

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。

3.8 Personal general information

Mean all personal information other than personal sensitive information

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。

3.9 Personal information handing

Behaviors of personal information handling include collection, processing, transfer and deletion.

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。

3.10 Tacit consent

In the case that there is no expressed objection from the subject of personal information, it will be deemed as consent by the subject of personal information.

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。

3.11 Expressed consent

Mean that the consent has been expressly authorized by the subject of personal information, and the relevant evidence has been preserved.

4 个人信息保护概述

4 Overview of Personal Information Protection

4.1 角色和职责

4.1 Roles and Responsibilities

4.1.1 综述

4.1.1 Summary

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、个人信息获得者和独立测评机构, 其职责见 4.1.2 至 4.1.5。

The roles involved in the implementation process of informational system personal information protection mainly include: subject of personal information, administration of personal information, receiver of personal information and independent evaluation agency. For their responsibilities, see 4.1.2 to 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漏、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。

4.1.2 Subject of personal information

Before providing personal information, it is necessary to take the initiative to understand the personal information administrator's purpose of collecting such information, its uses of such information and so forth, and provide personal information in accordance with personal desires; once the disclosure, loss or alters of personal information are detected, a complaint or enquiry should be made to the administrator of personal information. Alternatively, a complaint should be initiated to the administrative department that is responsible for personal information protection.

4.1.3 个人信息管理者

4.1.3. Administrator of personal information

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。

It is responsible for planning, designing and establishing personal information handling processes of information systems in accordance with national laws, regulations and this technical guidance document; developing a personal information administration system/rules, implementing its responsibilities on personal information

administration; appointing specialized agencies or persons to be responsible for the in-house personal information protection, and receiving complaints and questioning from the subject of personal information; developing education and training plans/programs on personal information protection and organizing to implement them; establishing internal control mechanisms for personal information protection, and conducting self-investigation or committing an independent evaluation agency to conduct evaluation on the security status of personal information of its information systems, its protection systems and their implementation statuses on a regular basis.
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漏、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。

[It is also responsible for] administrating and controlling the risks in the process of the informational system personal information handling, and making contingency plans for possible incidents in the process personal information handling, such as disclosure/divulgence, loss, damage, tampering, improper use and so forth. Once finding that personal information is divulged, lost, damaged, tampered and improperly used, it shall take relevant measure in a timely fashion in order to prevent a further expansion of the impacts of such incidents, and inform of the subject of personal information in a timely fashion. When major incidents happen, it shall report to relevant administrative department of personal information protection in a timely manner.

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。

[It shall] accept the inspection, supervision and guidance of relevant personal information administration department on its personal information protection status. It shall also actively participate and collaborate with a third party testing and evaluation agency to assess the personal information protection status of information system.

4.1.4 个人信息获得者

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。

4.1.4 Personal Information receiver

When the acquisition of personal information is for the purposes of information processing commissioned by the other party, personal information receiver shall, in accordance with the technical guidance documentation and the commission contract, process personal information, and immediately delete personal information after the processing task is completed.

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。

4.1.5 Third party testing and evaluation agency

From the point of view of defending public interest, on the basis of the authorization from personal information administration department and industry associations, or under the entrustment of personal information administrator, in accordance with the relevant national laws, regulations and technical guidance documents, (it is responsible for) conducting the testing and evaluation to information systems, obtaining personal information protection status. In doing so, provide evidences/basis for a personal information administrator to evaluate, supervise and guide the protection of personal information.

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:

4.2 Basic principles

Personal information administrator, in the use of information systems to handling personal information, should follow the basic principles as followings:

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。

a) Clear purpose principle - handle personal information with certain, clear and reasonable purposes, do not expand the scope of uses and not change the purpose of handling personal information without the knowledge of the subject of personal information.

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。

b) Minimum & sufficiency principle - only handle the minimal information that is relevant to the purpose of (information) handling. Once such a handling purpose is achieved, personal information should be deleted/removed in the shortest possible time period.

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。

c) Public notification principle – performing/fulfilling the obligations to the subject of

personal information on notification, instruction and warning. In a clear, easily understandable and appropriate manner, truthfully inform the subject of personal information of the purpose of handling personal information, the scope of the collection and use of personal information, personal information protection measures, and other information.

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。

d) Personal consent principle – before handling personal information, shall obtain the consent from the subject of personal information.

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

e) Quality assurance principle - ensuring that the confidentiality, integrity and availability of personal information are all up to date.

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。

f) Security guaranty principle – adopting appropriate administrative measures and technical means, which are adapt to the likelihood and severity of damage of the suffered personal information, to protect the security of personal information, and to prevent the retrieval, disclosure, loss, damage and alter/tampering of personal information without the authorization from personal information administrator.

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。

g) Good faith fulfilling principle - in accordance with the commitment made at the time of collection, or based on the reasons stated in laws, handling personal information. No longer continue to handle personal information once the intended purpose has been achieved.

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。

h) Clear responsibility principle – clearly define the responsibilities in the process of personal information handling, take appropriate measures to implement the relevant responsibilities, and record the personal information handling process in order to facilitate retrospective (investigation).

5 个人信息保护

5. Personal Information Protection

5.1 概述

5.1 Overview

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:

The process of handling personal information in an information system may be divided into four major segments/steps - collection, processing, transfer and removal. The protection of personal information shall be throughout the four segments/steps.

a) 收集指对个人信息进行获取并记录。

a) Collection means obtaining and recording personal information.

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。

b) Processing means operational conducts on personal information, such as (data) entry, storage, modification, annotation, comparison, mining, shielding.

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。

c) Transfer means the conducts/behaviors of providing personal information to the receivers of personal information, such as public disclosure, disclosure to certain groups, and copying personal information to other information systems due to the processing task commissioned to others.

d)删除指使个人信息在信息系统中不再可用。

d) Removal/deletion means that the personal information is no longer available in the information system.

5.2 收集阶段

5.2 Collection phase

5.2.1 要具有特定、明确、合法的目的。

5.2.1 With certain/specific, clear and legitimate purposes

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:

5.2.2 Before the collection, the subject of personal information should be notified, in a way that the PI subject is easy to be aware of, of the following matters:

a) 处理个人信息的目的;

a) The purpose of handling personal information;

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;

b) The manners and means of personal information collection, and specific contents to be collected, and the time/duration of retention;

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;

c) the scope of use of the collected personal information, including the scope of disclosure or provision of personal information to other organizations and institutions;

d)个人信息的保护措施;

d) the measures for protecting personal information;

e)个人信息管理者的名称、地址、联系方式等相关信息;

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

f) 个人信息主体提供个人信息后可能存在的风险;

f) the risks the subject of personal information may encounter after providing personal information;

g)个人信息主体不提供个人信息可能出现的后果;

g) the consequences if the subject of personal information is not willing to provide personal information;

h)个人信息主体的投诉渠道;

h) the channel for a subject of personal information to file a complaint; and

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。

i) in circumstances where personal information need to be transmitted or entrusted to another organization, the subject of personal information must be expressly notified with following but not limited to following information: the purpose for transmission or entrustment; the specific contents and scope of use of the transmitted or entrusted personal information; and the name, address, and contact information of the receiver of the entrusted personal information.

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。

5.2.3 Prior to handling personal information, need to obtain the consent from the subject of the personal information, including tacit consent or express consent. When collecting “general” personal information, tacit consent of PI subject is assumed. If the subject of personal information expressly objected, then the collection must be stoped or personal information must be removed/deleted; when colleting “sensitive” personal information, then the subjects of personal information must clearly give their consent.

5.2.4 只收集能够达到已告知目的的最少信息。

5.2.4 Only collect the minimal information that is sufficient to achieve the notified purpose.

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。

5.2.5 Must adopt the notified/informed means and manner to directly collect PI information from the subject of personal information. Must not adopt any hidden means or indirect manners to collect personal information.

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。

5.2.6 provide relevant functions when continuously collecting personal information, and allow the subject of personal to configure, adjust, and turn off the functions of the collection of personal information.

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。

5.2.7 Must not directly collect sensitive personal information from minors under 16 years old and any persons with limited or no civil capability. If do need to collect their sensitive personal information, need to obtain the express consent of their legal guardians.

5.3 加工阶段

5.3 Processing phrase/stage

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。

5.3.1 Must not violate the informed/notified purposes of the use (of the PI) in the collection phase, or exceed informed/notified scope to process personal information.

5.3.2 采用已告知的方法和手段。

5.3.2 Adopting informed/notified methods and means

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。

5.3.3 ensure that, in the process of processing PI, personal information will not be obtained by any individuals, organizations and institutions that are not relevant to the purpose of PI processing.

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。

5.3.4 the handled personal information must not be disclosed to any other individuals, organizations and institutions without the express consent of the subject of personal information.

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。

5.3.5 ensure that, in the process of processing PI, the information system runs continuously and steadily, PI remains in a complete, available and up-to-date status.

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。

5.3.6 When the subject of personal information finds that its personal information is flawed and requires modifications, the administrator of personal information shall inspect and check in accordance with the requests of the PI subject, and, under the premise of ensuring the integrity of the personal information, modify or supplement the relevant information.

5.3.7 详细记录对个人信息的状态,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内容,除非告 知成本或者请求频率超出合理的范围。

5.3.7 keep a detailed record on personal information status. When subjects of personal information require for inspecting their personal information, personal information administrator must truthfully and freely inform them whether or not its has their personal information, PI processing status and other contents, unless it informs that the cost or the frequency of their requests have gone beyond reasonable range/scope.

5.4 转移阶段

5.4 Transfer phrase/stage

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。

5.4.1 The transfer of personal information shall not be contrary to the notified transfer purpose in the collection phrase/stage or go beyond the notified/informed scope/range of transfer.

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。

5.4.2 Prior to the transfer of personal information to other organization and institution, it must assess whether such an organization and institution is able to handle personal information in accordance with the requirements of this technical guidance document, and must explicitly define the responsibility of such an organization and institution in protecting personal information.

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。

5.4.3 must ensure that, in the transfer process, the personal information is not obtained/aware by any individuals, organizations and institutions other than the receiver of personal information.

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。

5.4.4 must ensure the integrity, availability and up-to-date of the personal information before and after the transfer.

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。

5.4.5 Absent express consent of the subject of the personal information, or explicit legal or regulatory permission, or absent the consent of the competent authorities, the administrator of personal information must not transfer the personal information to any overseas receiver of personal information, including any individuals located overseas or any organizations and institutions registered overseas.

5.5 删除阶段

5.5 Deletion/removal phrase/stage

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。

5.5.1. In case that the subject of personal information seeks to delete/remove PI for proper reasons, the PI must be deleted/removed in a timely manner.

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。

In case that the deletion/removal of such personal information may affect the investigation and evidence collection by law enforcement agencies, it shall take the appropriate storage and shielding measures (on the PI).

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。

5.5.2 once the purposes of the use of the personal information, which was informed in the collection phase, are achieved, such personal information must be deleted/removed immediately; if need to continue to handle (the PI), then it must

delete the contents that enable to identify specific individuals; if need to continuously handle sensitive personal information, then an express consent of the subject of the personal information must be obtained.

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。

5.5.3 Once the time of the PI retention notified in the collection phrase has passed, the relevant information must be deleted immediately; in case that the retention period has been clearly defined, the relevant provisions must be implemented.

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。

5.5.4 in case that the administrator of personal information bankrupts or goes to insolvency, if it cannot continue to complete the purpose of handling personal information it committed, it must delete such personal information. In case that the deletion/removal of such personal information may affect the investigation and evidence collection by law enforcement agencies, it shall take the appropriate storage and shielding measures (on the PI).