ICS 35.020
L80

T/ SIA

中 国 软 件 行 业 协 会 团 体 标 准

T/ SIA 001—2017

企业个人信息安全管理规范

Personal information security management specification for enterprises

2017 - 03-28 发布　　2017 - 04-28 实施

中 国 软 件 行 业 协 会　发 布

目 次

前　言

本标准按照GB/T 1.1-2009 给出的规则起草。

本标准由中国软件行业协会提出并归口。

本标准起草单位：大连软件行业协会、北京软件和信息服务业协会、上海市软件行业协会、广东软件行业协会、深圳软件行业协会、河北软件与信息服务业协会、中国软件评测中心、北京百度网讯科技有限公司、东华软件股份有限公司、博彦科技股份有限公司、南方信息保护产业基地有限公司、文思海辉技术有限公司、中国民航信息集团公司。

本标准主要起草人： 付晓宇、朱璇、尹宏、郎庆斌、娄邨、龙飞、陈尚义、严德铭、吕晖、朱信铭、白春玲、薛强、余江、余智文、陈彬。

本标准为首次制定。

企业个人信息安全管理规范

1 范围

本标准用于指导软件和信息技术服务企业安全、合理地利用个人信息，规范企业个人信息处理活动，提升企业个人信息安全管理水平。

本标准适用于软件和信息技术服务企业，事业单位、社会团体等组织和机构也可参考。

本标准可作为第三方测评机构、认证机构的评估、认证依据。

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/T 19001/ISO 9001 质量管理体系 要求

GB/Z 28828 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 20985 信息技术 安全技术 信息安全事件管理指南

3 术语和定义

3.1

个人 person

基于自然规律出生，具有生物学意义和法理人格，并被赋予民事主体资格的自然人个体。

3.2

个人信息 personal information

与特定个人相关、能够单独或参照其他相关信息识别该特定个人的各种信息。

3.3

个人信息主体 personal information subject

可通过个人信息识别的特定的个人。

3.4

个人敏感信息 personal sensitive information

一旦泄露或被滥用，会对标识的个人信息主体造成不良影响的个人信息。通常情况下，个人敏感信息包括身份信息（如：身份证号、护照号等）、通讯信息（如：通讯录、电子邮件、通话及聊天内容等）、财产信息（如：信用卡号、银行账号、理财信息等）、健康信息（如：基因、病历、家族病史等）、生物特征（如：指纹、DNA等）、犯罪记录等。

3.5

个人信息处理 personal information processing

对个人信息实施的操作，包括但不限于个人信息的收集、保存、使用、二次开发、公开、披露、共享、销毁等行为或活动。

3.6

个人信息管理 personal information management

计划、组织、控制、协调个人信息处理及相关资源、环境、管理体系等的相关活动或行为。

3.7

个人信息管理者 administrator of personal information

获得个人信息主体同意和授权，基于合法、正当、必要的目的，决定个人信息处理方式，实际控制个人信息的软件和信息技术服务企业。在本标准中简称为企业。

4 基本要求

4.1 原则

a）目的明确原则。处理个人信息具有合法、正当、必要的目的，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，及时删除个人信息；

c）公开告知原则。对个人信息主体应尽到告知、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目的、个人信息收集和使用范围、个人信息保护措施等信息；

d）个人同意原则。处理个人信息前应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）保护保障原则。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，防止未经授权的检索、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。

4.2 个人信息主体权利

4.2.1 知情权

个人信息主体的知情权包括：

a）个人信息主体有权知悉个人信息处理的目的、方式、范围等相关信息；

b）个人信息主体有权查看与之相关的个人信息；

c）个人信息主体有权知悉个人信息的保护措施；

d）个人信息主体有权知悉个人信息的管理质量；

e）个人信息主体有权知悉个人信息的转移情况。

4.2.2 支配权

个人信息主体的支配权包括：

a）个人信息主体有权对是否提供个人信息做出选择；

b）个人信息主体有权修改、删除、完善与之相关的个人信息，以保证个人信息的完整、准确和最新状态；

c）个人信息主体有权在技术可行的条件下获取其个人信息副本；

d）个人信息主体有权决定如何使用与之相关的个人信息。

4.2.3 质疑权

个人信息主体的质疑权包括：

a）个人信息主体有权质疑或反对与之相关的个人信息处理目的、方式、范围等；

b）个人信息主体有权质疑个人信息的保护措施；

c）个人信息主体有权质疑个人信息的管理质量；

d）如果个人信息处理目的、方式违背了个人信息主体意愿且无其他正当理由，个人信息主体有权要求企业停止相关的个人信息处理活动或要求销毁相关的个人信息。

4.3 企业责任

4.3.1 法律责任

企业应承担的法律责任包括：

a）不得违反法律、法规和双方约定处理个人信息；

b）发生重大安全事件时，应及时向法律、法规规定的个人信息安全监管机构报告。

4.3.2 管理责任

企业应承担的管理责任包括但不限于：

a） 应建立有效的个人信息安全管理体系，落实个人信息管理责任；

b)应保证个人信息处理目的与个人信息主体同意的目的一致，处理活动不应超目的、超范围；

c）应对个人信息处理过程采取必要、恰当的安全管理措施和技术手段，防止个人信息滥用、篡改、泄露、损毁、丢失等；

d）应在处理活动中保证个人信息的完整性、准确性、可用性、保密性，并保持个人信息的最新状态；

e）未经个人信息主体同意，不得向他人提供个人信息，除非经过匿名化处理无法识别特定个人且不能还原的信息；

f）发现个人信息泄露、损毁、丢失等事件，应立即采取应对措施，并及时告知受影响的个人信息主体，告知内容包括事件影响的预判和已采取的措施；

g）建立个人信息管理质量的内审机制，定期对个人信息的安全状况、管理措施和技术手段进行自查或委托独立测评机构进行测评；

h) 接受个人信息安全监管机构对企业个人信息保护状况的检查、监督和指导。

4.3.3 权利保障责任

为保障个人信息主体权利，应：

a）在征得个人信息主体同意后开展与个人信息相关的处理活动，保障个人信息主体的知情权、支配权、质疑权；

b）在收集个人信息前，应将收集的目的、方式、范围、不提供个人信息的后果、查询和修改个人信息的渠道，以及企业的相关信息等告知个人信息主体；

c）指定专门部门负责接受投诉与质询，公开该部门的联系方式，便于个人信息主体和其他相关方的投诉和质询；

d）保障个人信息主体注销账户的权利，注销操作应方便易用。个人信息主体注销账户后，企业不得再处理与之相关的个人信息，并根据个人信息主体要求删除与之相关的个人信息。法律、法规另有规定的除外。

5 领导作用

5.1 最高管理者及职责

最高管理者作为企业的最高行政领导，其主要责任为：

a）批准个人信息管理方针并监督执行；

b）选择、任命有能力的管理者代表；

c）签发个人信息管理机构负责人任命书；

d）在资金、人力等资源方面对个人信息管理提供支持；

e）制定合理、适宜的激励政策；

f）任命内审负责人，组建内审机构，并赋予相应的权利；

g）对个人信息管理质量的持续改进提供决策支持。

5.2 管理方针

应制定个人信息管理方针，以指导个人信息管理的各项工作。个人信息管理方针应遵循法律、法规的原则和要求，符合企业实际情况，以简洁、明确的语言阐述，公之于众。个人信息管理方针内容宜包括：

a）个人信息主体的权利；

b）企业的责任和义务；

c）个人信息管理的目的和原则；

d）个人信息管理的措施和方法；

e）个人信息管理的改进和完善。

5.3 组织机构

5.3.1 管理机构及职责

个人信息管理机构由最高管理者、管理者代表、个人信息管理办公室、各部门个人信息保护负责人、个人信息处理相关责任人等组成。应根据企业具体情况设立专门的个人信息管理部门，负责企业的个人信息管理工作。企业应发布机构设置及责任人任命，确定其职能职责。

5.3.2 个人信息管理办公室及职责

个人信息管理办公室负责企业的个人信息管理的领导工作，其负责人为管理者代表。办公室可根据企业的实际情况单独设立，也可与其他管理职责共同设立。管理者代表应具备个人信息保护相关知识，了解企业业务的整体状况，熟悉业务流程，具备管理个人信息管理体系的能力。个人信息管理办公室的主要职责为：

a）制定个人信息管理方针，编制个人信息管理计划；

b）落实各部门个人信息管理负责人；

c）组织制定个人信息基本管理规定；

d）制定企业隐私政策，指导开展宣传和培训工作，指导各部门或岗位制定必要的管理细则；

e）定期或不定期对个人信息安全管理状况进行检查，监管相关管理记录，向最高管理者提交个人信息保护状况报告。发现重大事项及时向管理者代表或最高管理者报告；

f）负责接收个人信息主体的意见和建议，填写意见与建议处理登记表，协调相关责任人落实意见与建议，并及时反馈；

g）在发生个人信息安全事件时，负责与个人信息主体或其他相关方进行沟通协调，协商解决办法和补救方案；

h）向最高管理者提交个人信息安全风险评估报告和持续改进建议。

5.3.3 部门个人信息管理职责

企业应确定各部门的个人信息管理负责人。负责人应具备个人信息保护和信息安全基本知识，熟悉本部门业务、个人信息处理流程、信息系统及相关设备设施、内部和外部环境等。部门个人信息管理负责人的主要职责包括：

a）在管理者代表指导下开展个人信息管理工作，严格执行企业的各项管理规定；

b）制定部门个人信息安全管理细则并监督实施；

c）实施部门个人信息安全风险管理；

d）改进、完善部门个人信息管理工作；

e）支持和配合个人信息管理办公室和内审机构的工作；

f）编写部门个人信息管理工作报告。

5.3.4 宣传和培训部门及职责

宣传和培训部门负责企业对外宣传和员工培训工作，可根据企业情况单独设立或与其他管理职责共同设立部门。部门负责人应具备个人信息保护基本知识，了解企业个人信息管理总体情况，具备企业管理和培训经验，具备制定和完成宣传、培训计划的能力。宣传和培训部门负责人在管理者代表领导下开展工作。其主要职责包括：

a）制定年度宣传、培训计划并负责实施；

b）组织实施个人信息保护相关知识和规章制度的宣传、培训；

c）改进、完善宣传和培训的内容和方式。

5.3.5 内审机构及职责

内审机构负责定期对企业个人信息管理的状况进行内审。企业应单独设立内审机构。内审机构负责人由最高管理者任命，要求熟悉企业个人信息管理的整体状况，直接向最

高管理者负责。内审工作人员可以在企业内部选聘，或聘请社会人士担任。其主要职责包括：

a）制定年度内审计划、内审实施计划；

b）独立、公平、公正地开展对个人信息管理状况进行监督、检查、调查；

c）实施内审计划；

d）评估个人信息管理规章制度的执行状况；

e）编制内审报告，提出个人信息管理的改进、完善建议；

f）督促个人信息管理内审不符合项整改。

6 策划

6.1 管理计划

在个人信息管理方针的指导下，根据企业的业务及管理状况，制定个人信息安全管理和实施计划。计划应包括：

a）个人信息处理目的、方式和范围；

b）个人信息管理规章制度和安全措施；

c）个人信息管理和各类相关资源的组织、协调、转换和沟通；

d）个人信息安全风险评估及管理；

e）个人信息管理活动的定期评估和日常监控；

f）个人信息管理过程的改进；

g）其他必要的管理措施。

6.2 风险管理

6.2.1 风险识别

发现、记录、描述危害个人信息和个人信息主体权益的风险因素。风险识别的内容包括：

a） 分析企业的个人信息处理流程，识别个人信息管理相关联的所有资源和风险因素；

b）业务风险的识别包括：业务流程的安全模式、业务团队的管理模式、业务管理及设施管理等；

c）管理风险的识别包括：个人信息的管理方式、部门的管理方式、网络管理、人员职责等；

d）环境风险的识别包括：运营场所、工作环境、出入管理、文档管理、个人终端及周边环境管理等；

e）行为风险的识别包括：管理人员、业务人员、设备管理人员、个人信息保护负责人等人员的行为规范；

f）意识风险的识别包括：网络技术欺骗、网络聊天、垃圾处理、人员聊天等；

g）可能对个人信息安全造成影响的其他因素。

6.2.2 风险评估

分析、判断风险发生的可能性和可能的影响。风险评估的方法包括：

a）采取必要的技术手段发现个人信息处理活动、管理环节等存在的脆弱性；

b）对个人信息管理依赖某一资源的程度进行分析、判断，依赖程度越高，该资源的风险就越大；

c）个人信息管理依赖某一资源的程度越高，资源价值越大，风险越大；

d）对业务、管理、技术、环境、行为因素引发的风险进行定性分析，并确定其发生的可能性的等级；

e）根据风险事件发生的可能性和对个人信息主体、企业和社会造成的影响和损失，确定风险等级。

6.2.3 风险控制

根据风险评估的结果，选择、实施合适的风险应对措施，将风险控制在可接受的范围内。风险控制的内容包括：

a）根据风险评估结果，建立风险管理台账，内容包括：风险来源、风险描述、风险等级、防范措施、残余风险等；

b）采用风险规避、风险弱化、风险转移和风险接受的风险防范措施，将风险控制在可接受范围内；

c）采取风险控制措施后，对仍然存在的残余风险应跟踪、监控，随时采取相应的应对措施；

d）应随时监控个人信息安全风险的变化，评估并调整风险防范措施；

e）当个人信息收集的内容和方式、使用方式发生变化及发生个人信息安全事件或其他异常情况时，应重新进行个人信息安全风 险评估；

f）当个人信息的内容、数量达到一旦遭到破坏、丧失功能或数据泄露时，将使国家安全、国计民生、公共利益遭受严重危害的程度时，应按照国家关键信息基础设施进行保护。

7 支持

7.1 人员管理

应加强企业全体员工特别是大量接触个人信息人员的管理，包括：

a）对于工作中大量接触个人信息的重要岗位人员，如数据库管理员等，应进行岗前背景审查；

b）应明确与个人信息处理直接相关人员的权限、责任，签订保密协议，通过培训提高其保障个人信息主体权利的意识；

c）应采取有效的激励措施，增强员工保护个人信息的自觉性和责任感；

d）应严格执行违反个人信息保护规章制度的处罚规定，并在处罚后及时编写处罚记录和处理报告。

7.2 宣传和培训

7.2.1 宣传

宣传管理部门负责对内、对外的宣传工作，包括：

a）应向企业全体员工及其他相关人员宣传个人信息保护的重要性和个人信息管理方针、管理制度，要求其遵照执行；

b）应向社会公开宣传企业的隐私政策。对外开展涉及个人信息的相关业务时，应主动宣传企业隐私政策、保护措施和保密承诺；

c）应在宣传资料、网络媒介及其他面向社会的各类文件中包含个人信息保护的相关内容。

7.2.2 培训

培训管理部门应根据部门、人员、业务、用户需求等实际情况开展培训工作，包括：

a）制定个人信息管理相关的培训计划和培训实施计划；

b）培训对象应包括全体员工、临时人员和其他相关人员；

c）培训内容应包括：

1）个人信息保护相关法律、法规、标准；

2）个人信息保护的重要性和必要性；

3）个人信息主体权利；

4）个人信息管理方针、管理制度等；

5）与其工作相关的个人信息保护管理措施和技术手段；

6）违反个人信息管理制度可能引起的损害和导致的后果；

7）其他必要的内容。

d）参加培训的人员应签到，培训后填写培训记录，评价培训效果并编写培训报告。

7.3 管理规定

7.3.1 基本管理规定

基本管理规定是企业进行个人信息管理的行为准则，要求企业全体员工深刻理解并遵照执行。基本管理规定应包括个人信息管理的各个方面和环节，并在实施过程中不断改进和完善。基本管理规定应包括：

a）个人信息管理机构及职责规定；

b）个人信息安全风险管理规定；

c）个人信息处理活动相关管理规定；

d）设备、设施、场所等安全管理规定；

e）个人信息数据库管理规定；

f）文档管理规定；

g）宣传、培训管理规定；

h）内审管理规定；

i）持续改进管理规定；

j）事件应急管理规定；

k）违反管理制度的处罚规定；

l）其他必要的管理制度。

7.3.2 管理细则

企业各部门应制定与基本管理规定一致、符合各部门业务特点、切实可行的管理细则。特殊的岗位应制定相应的管理细则。

7.3.3 其他管理规定

对个人信息管理有特殊要求的业务应制定相应的管理规定。

7.4 文件控制

7.4.1 个人信息台账

应建立个人信息台账，分类记录个人信息管理情况，台账内容包括个人信息类别、收集时间、收集方法、提供者、使用目的、保存形式、保管场所、保存期限、销毁方式等内容。

7.4.2 文件管理

做好与个人信息管理相关的纸介质和电子介质文件管理，包括：

a）建立文件管理制度，并不断改进和完善；

b）做好个人信息处理过程中各项活动的记录，作为内审和过程改进的依据；

c）妥善保存个人信息管理相关的规章、文件、记录、合同等，建立文档清单和发放、借阅、归还等登记制度。

8 处理过程

8.1 收集

8.1.1 收集限制

在个人信息收集过程中的限制包括：

a）个人信息收集必须具有合法、正当的目的；

b）应遵循适度、适当原则，仅收集为达到个人信息处理目的所必需的个人信息；

c）当个人信息主体对收集有疑义或反对，应停止收集；

d）收集类型和范围须经企业个人信息管理办公室审定批准；

e）收集个人敏感信息时，应严格遵守法律、法规的要求，必要时需获得个人信息安全监管机构的许可；

f）不得采取隐蔽手段或未经个人信息主体同意间接收集个人信息；

g）利用网络终端软件持续收集个人信息时，应提供相关设置功能，允许个人信息主体配置、调整、关闭收集功能；

h）个人信息收集过程中应采取自动校验机制，对数据类型、数值范围等进行校验；

i）不直接向未成年人、限制民事行为能力或无行为能力人收集个人敏感信息，确需收集应征得其法定监护人的明示同意。

8.1.2 目的合法性

个人信息处理的目的合法性考虑因素包括但不限于：

a）遵循国家的法律、法规规定；

b）个人信息主体同意；

c）保护个人信息主体的重大利益，如涉及个人生命安全等；

d）维护公共利益。

8.1.3 事前告知

在收集个人信息前，应公开个人信息收集目的、收集的类别和范围，以明确、易懂和恰当的方式告知个人信息主体，告知内容应包括：

a）企业基本情况，包括注册名称、注册地址、办公地点、联系方式、管理者代表的联系方式等；

b）收集个人信息的目的、类别和范围，个人信息保存方式、保存期限和超出保存期限的处置方式等；

c）个人信息主体提供个人信息后可能存在的安全风险，如果不提供个人信息可能造成的影响；

d）个人信息保护措施及保证个人信息安全的承诺；

e）个人信息主体查询、修改、质疑等相关权利的实现方式及投诉渠道，外部争议解决机构及联络方式；

f）个人信息主体对处理其个人信息表达同意或撤回同意的机制。

8.1.4 同意表达

除法律、法规另有规定外，个人信息主体表达同意的方式包括但不限于：

a）个人信息主体以可鉴证和追溯的方式明示同意，包括数据电文或书面形式，如主动点击“同意”选项、签字等；

b）当个人信息主体明确知道处理其一般信息时，无明确反对表达被认为是默许同意；

c）个人信息主体提出异议时视为撤回同意。撤回同意不影响撤回同意前基于同意的数据处理。

8.1.5 收集方式

收集个人信息的方式包括：

a）征得个人信息主体同意后，直接向个人信息主体收集个人信息；

b）通过各种电子媒介（如博客、微博、微信、论坛、云盘、网盘、邮件、即时通讯、网站、网络视频等）、纸媒体和其他途径间接获取个人信息时，应保障个人信息主体知情权、支配权等权利不受侵害。

8.2 存储

8.2.1 存储要求

个人信息应存储于专门的数据库内，并采取措施确保个人信息的完整性、准确性、可用性、保密性，避免个人信息的滥用、毁损或丢失。

8.2.2 脱敏处理

对个人敏感信息的存储应采用假名化、碎片化、加密、加噪等技术脱敏后存储。

8.2.3 存储期限

个人信息保存期限的确定依据包括；

a）存储期限应为完成个人信息处理目的所需的最短时间，法律、法规另有规定的除外；

b）处理个人信息的信息系统应设置存储期限的监控机制，对超过存储期限的个人信息应及时进入后处理程序。

8.2.4 数据库管理

数据库作为个人信息的重要载体，对其管理的要求包括：

a）建立个人信息数据库管理和使用制度，对登录、检索、导入、导出、删除等操作进行备案登记，设专人负责检查；

b）制定个人信息数据库管理策略，包括访问控制、权限设置、密钥管理等，防止非授权的登录、检索、导入、导出、删除等操作；

c）对于个人敏感信息的操作应设置日志，并规定日志保存时间；

d）建立个人信息数据库备份和恢复机制，保证备份的完整性、可用性和可靠性，并对备份和恢复情况进行记录。

8.3 使用

8.3.1 使用限制

个人信息的使用限制包括：

a）不得改变已告知个人信息主体的处理目的，或超出告知范围使用个人信息；

b）不得擅自修改数据，以保持个人信息的完整性和真实性；

c）应采取控制措施，确保员工只能使用与其职责相关的最少个人信息，严格限制并审计非个人信息主体对敏感信息的关联查询、复制等操作；

d）未经个人信息主体明示同意，不向其他个人、组织披露与之相关的个人信息；

e） 对个人信息进行统计分析、数据挖掘等二次开发所生成的符合个人信息特征的衍生信息，应按个人信息保护；

f）因业务需要，确需变更个人信息处理目的、扩大使用范围的，应重新执行告知程序，再次征得个人信息主体明示同意；

g）变更个人信息处理目的、扩大使用范围前，应进行安全风险评估，必要时调整保护措施；

h）信息系统应记录个人信息使用日志并可以追溯；

i）在终端屏幕上展示个人敏感信息时，宜酌情屏蔽部分字段。

8.3.2 二次开发

对个人信息进行统计、分析、整合、挖掘、标记、数字画像等二次开发，应符合在收集时已告知个人信息主体的目的，对二次开发所生成信息的使用应限定在个人信息主体同意的范围内。二次开发前需告知个人信息主体的内容应包括：

a）企业的相关信息；

b）二次开发的目的、方式和范围；

c）经二次开发所生成信息的使用方式；

d）个人信息保护措施和保证个人信息安全的承诺；

e）因二次开发而引发事件的责任认定和处理方式；

f）二次开发完成后个人信息的处置方式。

8.3.3 请求响应

对于个人信息主体提出的请求，应在验证个人信息主体身份后及时响应，对合理的请求不应收取任何费用，对超出合理次数的请求，可酌情收取一定费用。对请求响应的要求包括但不限于：

a）应设置个人信息查询机制，允许个人信息主体查询与之相关的个人信息内容，查看处理目的、保存期限、转让和披露的情况、采用何种自动决策机制等；

b）当个人信息主体提出修改相关的个人信息时，在不违背法律、法规和公共利益等的前提下，应尽快完成数据修改；

c）当个人信息主体提出获取与之相关的个人信息副本或要求将副本发给第三方时，应在技术可行的情况下给予支持；

d）当个人信息主体提出信息系统的自动决策机制影响自身权益时，应为个人信息主体提供辩解、投诉、退出等机制；

e）当个人信息主体提出删除相关的个人信息时，在不违背法律、法规和公共利益的前提下，属于下述情况时应给予删除：

1）已达到个人信息处理目的；

2）个人信息主体撤回同意；

3）个人信息收集行为属于未经个人信息主体同意的。

f）当需要删除的个人信息已披露给第三方时，应通知并采取必要措施监督第三方及时删除；

g）以下情况下可不响应个人信息主体的修改和删除请求，包括但不限于：

1）违背法律、法规规定；

2）危害重大公共利益；

3）与犯罪侦查、起诉和审判等有关；

4）危害个人信息主体或其他个人或组织的重大利益。

8.4 转移

8.4.1 公开和披露

公开和披露个人信息应遵循：

a）向公众公开和向特定群体披露个人信息应在已告知的目的、范围内；

b）对可公开访问的个人信息，未经个人信息主体明示同意，不得变更个人信息主体原来公开的范围，也不得对多个来源的个人信息进行汇总处理；

c）公开和披露前应进行个人信息安全风险评估，并采取措施有效降低风险；

d）需监控因披露个人信息而可能引发的风险，发生安全事件时应及时处理；

e）准确记录并保存个人信息的披露情况，包括披露时间、披露内容、披露对象等；

f）需要删除已披露的个人信息时，应通知已获取个人信息的相关方及时删除。

8.4.2 委托处理

委托第三方处理个人信息时，应将受托方相关信息告知个人信息主体，并获得个人信息主体明示同意。应选择符合本标准要求的企业，并与其签订委托处理合同。委托合同条款应包括：

a）委托目的和范围；

b）委托方和受托方的权利和责任；

c）个人信息保护措施和保证个人信息安全的承诺；

d）再委托时的相关限定；

e）个人信息相关事件的责任认定和处理方式；

f）合同到期后个人信息的处置方式；

g）受托方符合本标准要求或达到委托处理目的所必需的个人信息保护能力的证明。

8.4.3 跨境转移

企业管理的个人信息跨境转移时，应遵循：

a）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、个人信息安全监管机构同意，企业不得将个人信息转移到境外，包括位于境外的个人或境外注册的组织和机构；

b）当个人信息确需转移到境外时，应与境外接收者签订书面合同，确保境外接收者具备不低于我国法律、法规或标准等所规定的个人信息保护水平；

c）不得违规向境外机构提供个人信息或为其获取个人信息提供便利条件；

d） 因个人信息转移到境外造成个人信息主体权益损害时，应为个人信息主体提供有效和便于操作的救济途径。

8.5 后处理

8.5.1 销毁

个人信息在达到处理目的和承诺的保存期限后，应遵循：

a）彻底销毁与个人信息相关的纸介质和电子介质上的相关记录，并填写个人信息销毁记录；

b）如需继续保存、使用或返还，可根据个人信息主体意愿或合同约定方式处理；

c）个人敏感信息在达到处理目的后，应立即删除。如需继续保存，应获得个人信息主体的明示同意，并尽量消除其中能够识别个人信息主体的内容；

d）企业被兼并或破产时，若无法继续保证承诺的个人信息处理目的，应通知个人信息主体，并删除个人信息。

8.5.2 特殊处理

按照法律、法规规定，需要对个人信息进行特殊处理的情况包括：

a）法律、法规对数据保存期限有明确规定的，按相关规定执行；

b）删除个人信息可能影响执法机构调查取证时，应采取适当的隔离和屏蔽措施。

8.6 意见处理

个人信息管理办公室负责处理与个人信息管理相关的各类意见和建议，主要工作包括但不限于：

a）受理个人信息主体、企业内部和外部相关方提出的有关个人信息管理的意见和建议，重要的意见和建议应及时上报；

b）按照企业相关制度规定的流程处理所受理的意见和建议，做好相关处理记录；

c）督促相关部门尽快落实所负责的意见和建议并及时反馈；

d）编写意见和建议处理及反馈情况报告。

8.7 应急管理

8.7.1 应急预案

应针对可能发生的安全事件制定事件响应及应急预案。通过培训、演练等使全体员工在发生个人信息滥用、泄露、篡改、损毁、丢失等事件时，能够及时采取必要的处理措施。应急预案应包括：

a）事件处理流程；

b）事件记录和报告制度；

c）事件应急机制；

d）事件处理方案；

e）事件责任认定方式；

f）向主管部门和个人信息安全监管机构报告的要求。

8.7.2 事件处置

在发生或者可能发生个人信息滥用、泄露、篡改、毁损、丢失等安全事件时，应按照应急预案的要求及时处置，包括：

a）采取补救措施，将损失减少到最小程度；

b）按照规定及时告知个人信息主体并向有关主管部门、个人信息安全监管机构报告；

c）进行风险评估，必要时修订管理制度、完善技术手段；

d）事件处理完毕后，应编写个人信息安全事件处理记录并归档保存。

9 安全管理

9.1 物理环境管理

应采取必要的措施，保证个人信息处理设备、设施及场所的安全，包括防火、防盗、防水、防意外断电及其他自然灾害、意外事件、人为因素等危害。设置重点保护区域，如机房、监控室、设备间、资料室等，采用电子门禁等方式对人员出入保护区域进行严格管理，建立登记备案制度。

9.2 工作区域管理

应对与个人信息相关的工作区域内的物品和设备进行管理，防止未经授权的、无意的、恶意的个人信息滥用、篡改、泄露、损毁、丢失等。包括：

a）采用电子门禁系统对工作区域人员出入进行管理，记录人员出入信息。设置监控系统，建立最晚离开日志；

b）保持工作桌面整洁；

c）设置计算机开机口令和屏幕保护口令；

d）建立计算机光驱、USB、网口等接口管理制度；

e）建立计算机文件、文件夹、共享文件等管理制度；

f）其他相关管理。

9.3 信息系统保护

应对处理个人信息的信息系统建立整体安全防范策略和保护措施。范围包括基础网络平台、硬件系统、软件系统、应用系统、数据库系统等，防范策略和措施包括系统访问控制、信息交换保护、病毒防范、系统入侵防范、系统恢复、应急处理等。网络管理员和设备管理员应采用工作日志方式记录信息系统运行状况。

9.4 上网行为管理

应采用合理的网络拓扑结构，按照分区分域的网络管理模式，设置严格的权限控制。制定上网行为管理制度，采用必要的管理措施和技术手段，监控非授权的网上使用、转移个人信息的行为。在公共网络上传输个人信息应采取保护措施，传输个人敏感信息应采用加密方式。

9.5 移动设备管理

应制定与个人信息相关的移动设备的保管、借用登记等管理制度，采取必要的管理措施和技术手段，建立移动设备使用追踪回溯机制，防止移动设备中的个人信息泄露、毁损、丢失等。不得在移动设备上以明文方式保存个人敏感信息。

10 监控

10.1 检查

个人信息管理办公室应对个人信息管理状况进行定期和非定期检查，编写检查报告，提交最高管理者。检查内容包括但不限于：

a）企业管理活动的有效性及与个人信息保护相关法律、法规、标准要求的符合性；

b）管理措施、技术手段和业务流程是否符合个人信息保护的需求；

c）检查个人信息处理的重点活动和行为，特别是个人信息数据库的操作，及时发现违规行为；

d）对个人信息主体和其他相关方的意见和建议的处理及反馈情况。

10.2 内审

10.2.1 内审职责

内审机构的主要职责包括：

a）审核企业管理活动的有效性及与个人信息保护相关法律、法规、标准要求的符合性；

b）审核管理措施、技术手段和业务流程是否符合个人信息保护的需求；

c）审核个人信息管理制度的执行情况；

d）提出过程改进和完善建议。

10.2.2 内审计划

应根据相关法律、规范和企业实际情况制定年度内审计划。内审计划应包括：

a）内审的目标和原则；

b）内审策略和控制措施；

c）内审周期、时间；
d）内审责任分工；
e）内审报告的要求；
f）其他必要的措施。

10.2.3 内审实施

应根据内审计划，组织、协调相关资源，选择与被审核对象无直接关系的人员作为内审员，独立、公平、公正地实施内审。应记录内审情况，形成内审报告。

11 改进

11.1 改进依据

应定期对个人信息管理状况进行评估，分析、判断个人信息管理制度及其落实情况，发现运行中的缺陷和漏洞，制定改进方案。制定改进方案的依据应包括：
a）国内外法律、法规、标准的变化情况；
b）日常检查、内审及其他体系运行的相关报告；
c）第三方测评和认证的结果；
d）企业业务范围的变化情况；
e）投诉及内外部的意见和建议；
f）社会环境、公众意识和技术进步等变化情况；
g）前一次改进实施的效果。

11.2 改进实施

应在个人信息管理办公室组织下，采用计划、执行、检查、改进模式（PDCA），对个人信息管理进行持续改进和完善，改进过程包括：
a）根据改进依据，制定改进方案；
b）按照持续改进管理规定的程序要求，公布并执行改进方案；
c）跟踪、检查改进方案的实施；
d）确认改进效果，提出新的改进建议。

12 例外

基于以下例外事项的个人信息处理，可以不必事先征得个人信息主体同意，但应严格依据法律、法规的规定，或经由主管部门、个人信息安全监管机构确定：
a）法律、法规特别规定的；
b）保护国家安全、公共利益、制止刑事犯罪；
c）保护个人信息主体或公众的权利、生命、健康、财产等重大利益等。

13 认证

企业有义务接受主管部门和个人信息安全监管机构的指导、监督和检查，并配合第三方测评机构、认证机构对企业的个人信息保护状况与相关法律、法规、标准的符合性、

一致性的测评、认证。企业获得的测评报告、认证证书可以作为企业个人信息保护能力的证明。

参 考 文 献

[1] DB21/T 1628.1-2016 信息安全 个人信息保护规范