ICS 35.080
L77
备案号：

SJ

中 华 人 民 共 和 国 电 子 行 业 标 准

SJ/T 11445.2—2012

信息技术服务 外包
第2部分：数据（信息）保护规范

IT Service—Outsourcing—

Part 2: Specifications for Data Protection

2012－12－28 发布　　2013－01－01 实施

中华人民共和国工业和信息化部　　发布

目　　次

前　言

本标准根据 GB/T1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由工业和信息化部软件服务业司提出。

本标准由中国电子技术标准化研究院归口。

本标准起草单位：大连软件行业协会、东软集团股份有限公司、北京万国长安容灾备份服务有限公司、中金数据系统有限公司、广州越维信息科技有限公司、北京赛迪时代信息产业股份有限公司

本标准主要起草人：郎庆斌 孙鹏 赵兴华 马强 李岗 尹宏 赵振文 赵熙 程磊 杨帆 王开红 郭玉梅 曹剑 周平 崔静。

引　言

本标准内涵和外延均较宽泛，存在易于混淆、多义性的概念、理解，现予以说明，以便于标准条文的解释和标准的应用。

0.1　基准

本标准考虑个人信息与商业数据具有类同的特质，在收集、处理、使用中，其安全要求、安全机制、安全策略等是同等的，可以采用同一的管理方式，适于IT服务外包组织共同遵守和应用，也可为其他行业提供借鉴。

0.2　数据

“数据”是一个广义的概念，本标准中，代指涉及个人信息、商业数据（仅指敏感的商业秘密或其他需要保护的数据）的相关信息。

由于知识产权涉及面广、构成复杂，且已有相关法规，但是，与知识产权相关信息的保护存在法律空白。同时，这部分信息与商业数据的特质类同。因而，本标准将知识产权相关信息归入商业数据。

0.3　内容数据库

内容是相对宽泛的概念。本标准仅限定内容数据库是由结构化、非结构化个人信息、商业数据（包括自动处理和非自动处理）所构成的逻辑数据库。

0.4　数据管理

数据保护是针对数据及相关资源、环境、管理体系等的管理活动或行为之一，因而，本标准采用“数据管理”涵盖“数据保护”。本标准数据管理涉及个人信息管理、商业数据管理。

数据管理包含数据收集、处理、使用的整个生命周期。

0.5　数据安全性

本标准涉及的数据安全性，是指个人信息、商业数据的保密性、完整性、准确性、可用性、真实性、可控性和不可抵赖性。

0.6　数据管理体系

本标准为个人信息管理、商业数据管理提供了基本的规则和要求，以构建数据管理体系，最大程度降低数据因偶然的或者恶意的原因，遭到破坏、篡改、泄露、窃取和不当使用等的可能性。

0.7　业务连续性

本标准在提供安全指导的同时，应基于数据的合理流通，保证业务的连续性。

0.8　标准兼容性

本标准与其他国际、国内信息安全标准及其他相关标准协调一致，并与这些标准相互配合或相互整合实施和运行。

0.9　标准实施

本标准的适用范围并不仅限于IT服务外包组织。本标准规范的数据管理规则，是IT服务管理的基础，具有普适性，同时，为IT服务的发展建立数据管理基准。因而，其他机关、企业、事业、社会团体等各类组织，可以参照执行。

信息技术服务 外包 第2部分：数据保护规范

1 范围

本标准规定了数据管理相关术语和定义、数据管理原则、数据主体权利、数据管理者的责任和义务、数据管理体系的建立和实施、数据管理体系内审、过程改进等基本规则和要求。

本标准适用于IT服务外包组织，其他组织可参照执行。

2 术语、定义和缩略语

2.1 术语和定义

下列术语和定义适用于本文件。

2.1.1

数据 data

描述个人信息、商业数据形态、属性等，并便于保存、处理、使用。

2.1.1.1

个人信息 personal information

与特定个人相关、并可识别该个人的数据、图像、声音等信息，包括不能直接确认，但与其他信息对照、参考、分析仍可间接识别特定个人的信息。

2.1.1.2

商业数据 business data

与数据主体利益相关，实用且已采取保密措施，并不为公众知悉的技术信息、经营信息等（含未公开的知识产权相关信息），及其它需要保护的数据。

2.1.2

内容数据库 content database

为实现一定目的，按照某种规则组织、管理的数据的逻辑集合体。

2.1.2.1

个人信息数据库 personal information database

a）可以通过自动处理检索特定的个人信息的集合体，形式如磁介质、电子及网络媒介等；

b）可以采用非自动处理方式检索、查阅特定的个人信息的集合体，如纸介质、声音、照片等；

c）除前2项外，法律规定的可检索特定个人信息的集合体。

2.1.2.2

商业数据库 business database

a）可以通过自动处理检索特定商业数据的集合体，形式如磁介质、电子及网络媒介等；

b）可以采用非自动处理方式检索、查阅特定商业数据的集合体，如纸介质、声音、图片、产品等；

c）除前 2 项外，法律规定的可检索特定商业数据的集合体。

2.1.3

数据主体 data subject

可通过数据识别的个人信息、商业数据的所有者。

2.1.3.1

个人信息主体 personal information subject

可通过个人信息识别的特定的个人。

2.1.3.2

商业数据主体 business data subject

商业数据的合法所有者。

2.1.4

数据管理 data management

计划、组织、协调、控制数据及相关资源、环境、管理体系等的相关活动或行为。

2.1.5

数据管理者 data controller

获数据主体授权，基于明确、合法目的，管理、使用数据的 IT 服务外包组织。

2.1.6

数据管理体系 data management system

数据管理活动或行为的结果。基于数据管理目标，整合目标、方针、原则、方法、过程、审核、改进等管理要素，及实现要素的方法和过程，提高数据管理有效性的系统。

2.1.7

数据管理方针 data management policy

数据管理者应遵守的行为规则，明示于与数据管理相关的环境中，是数据管理的基准。数据管理方针确立了数据管理的目标、原则、方法、措施等。

2.1.8

数据收集 data collection

基于明确、合法目的获取数据的行为。

2.1.9

数据处理 data processing

自动或非自动处置数据的过程，如加工、编辑、存储、检索、交换、传输、输出等及其它使用行为或活动。

2.1.9.1

自动处理 automatic processing

利用计算机及其相关和配套设备、信息网络系统、信息资源系统等，按照一定的应用目的和规则，加工、编辑、存储、检索、交换、传输、输出等相关数据处置行为或活动。

2.1.9.2

非自动处理 non-automatic processing

除自动处理外的其它数据处置行为或活动。

2.1.10

数据主体同意 data subject's consent

数据管理活动或行为与数据主体意愿一致，数据主体明确表示同意。表达形式包括：

a）数据主体以书面形式同意；

b）数据主体以可鉴证的、有规范记录的、满足书面形式要求的非书面形式同意。

注：下述情况视为个人信息主体同意：

a）由监护人代表未成年的或无法做出正确判断的成年的数据主体表达的意愿；

b）数据管理者与数据主体签订合同中确认了相关数据处理的规定，数据主体同意履行合同。

2.2 缩略语

PDCA 计划-实施-检查-改进 （plan-do-check-active）

全面质量管理应遵循的科学方法。本标准用于数据管理相关活动的质量管理

3 数据管理原则

3.1 目的明确

数据收集、处理、使用应基于明确、合法的目的。

3.2 主体权利

数据主体对相关的个人信息、商业数据享有权利。

3.3 数据质量

在数据管理行为或活动中，应保证数据的准确、完整、可用、真实、可控和不可抵赖。

3.4 使用限制

应采用合理、合法的手段和方式，收集、处理、使用数据，并征得数据主体同意。

3.5 安全保障

应采取必要、合理的管理和技术措施，防止发生数据泄露、丢失、损毁、篡改等的安全事件。

3.6 责任

应保证各项原则的有效实施。

4 数据主体权利

4.1 知情权

a）知悉数据收集、处理、使用的相关信息；
b）确认数据收集、处理、使用的目的、方式、范围等相关信息；
c）确认数据管理者保存数据的相关信息；
d）查询数据收集、处理、使用情况及数据质量等相关信息。

4.2 支配权

a）收集、处理、使用数据，应经数据主体同意；
b）数据主体有权修改、删除、完善与之相关的数据信息，以保证数据信息的质量；
c）数据主体有权控制、自主决定收集、处理、使用数据的方式、目的、内容、范围等。

4.3 质疑权

a）数据主体有权质疑与之相关的数据的准确性、完整性和时效性；
b）数据主体有权质疑或反对与之相关的数据管理目的、过程等；
c）如果数据管理目的、过程违背了数据主体意愿或其他正当理由，数据主体有权请求停止数据管理活动、行为或提出撤销该数据。停止或撤销应经数据主体确认。

5 数据管理者的责任和义务

5.1 管理责任

数据管理者对所拥有的数据负有管理责任，并征得数据主体同意后开展数据管理相关活动或行为。

5.2 权利保障

数据管理者应保障数据主体的权利。

5.3 目的明确

数据管理者应保证数据管理目的与数据主体意愿一致，管理过程或行为不应超目的、超范围。

5.4 告知

数据管理者应将数据管理目的、方式、不提供数据的后果、查询和更正相关数据的权利，以及数据管理者本身的相关信息等通知数据主体。

5.5 质量保证

数据管理者应在管理活动或行为中保证数据的完整性、准确性、可用性，并保持最新状态。

5.6 安全和保密

数据管理者应对所管理的数据予以保密，并对数据管理过程中的安全负责。

6 数据管理

6.1 目的

数据管理者应依据 5.1 的规定，协调、组织数据管理体系和各类相关资源，根据收集、处理目的，采取相应的控制策略和措施，处理、使用数据。

6.2 计划

数据管理者应根据管理、业务目标，制定数据管理计划。计划应包括：

a）数据收集目的、策略；

b）数据管理措施、策略；

c）数据管理和各类相关资源的组织、协调、沟通；

d）数据安全风险评估；

e）计划评估；

f）其他必要的管理策略。

6.3 组织

数据管理者应根据管理计划，组织数据管理活动或行为，主要应包括：

a）建立数据管理体系；

b）明确数据管理职责和行为准则；

c）实施、运行数据管理体系；

d）评估数据管理体系效能；

e）评估数据管理效果；

f）其他相关管理。

6.4 控制

数据管理者应根据管理计划，检查、修正数据管理相关活动、行为，并监督管理计划的实施。

7 数据管理体系

数据管理体系应包括以下要素：

a）目标和基本原则；

b）方针；

c）机构及职责；

d）管理机制；

e）管理过程；

f）安全管理；

g）内审；

h）过程改进。

8 数据管理方针

数据管理者应基于实际情况，依据国家相关法规、标准的原则和措施，以简洁、明确的语言阐述、公示，以指导数据管理工作。内容宜包括：

a）数据主体的权利；

b）数据管理者的义务；

c）数据管理的目的和原则；

d）数据管理的措施和方法；

e）数据管理的改进和完善。

9 数据管理相关机构及职责

9.1 最高管理者

数据管理者的最高领导，应重视并激励数据管理体系建设，授权适宜的人员组建相应的数据管理机构，并为数据管理体系的构建、实施和运行提供完全的支持。

9.2 管理机构

数据管理机构负责数据管理体系构建、实施和运行，应由最高管理者任命的数据管理者代表负责。机构的主要职责应包括：

a）数据管理计划制定、实施；

b）数据管理体系建立、实施、运行；

c）明确数据管理相关机构和人员职责、责任；

d）管理数据相关活动、行为；

e）检查、评估、改进、完善数据管理体系；

f）记录数据管理活动，并编制数据管理体系运行报告。

9.2.1 宣传教育

宜指定专人负责宣传教育，在数据管理机构的指导下开展工作。其主要职责应包括：

a）组织、实施数据管理体系的宣传、教育；

b）制定数据管理体系宣传、教育制度、计划；

c）制定数据管理的宣传策略和方法；

d）数据管理相关知识、管理和安全技术等的培训、教育；

e）改进、完善宣传、教育措施、方法。

9.2.2 安全管理

宜指定信息安全责任人负责数据安全管理，在数据管理机构指导下开展数据安全管理工作。其主要职责应包括：

a）数据、数据管理体系安全风险管理；

b）数据收集、处理、使用安全；

c）数据管理体系安全；

d）制定数据安全管理策略、措施；

e）实施数据安全管理措施；

f）改进、完善数据安全管理措施。

9.2.3 服务台

宜指定专人负责，在数据管理机构的领导下开展工作。其主要职责应包括：

a）提供数据管理、安全的相关咨询和服务；

b）提供数据收集、处理、使用建议和意见；

c）接受有关数据管理、安全的意见、建议，并落实和反馈；

d）沟通、交流；

e）数据管理相关事项、问题处理等的发布；

f）其他应处理的问题。

9.3 内审机构

最高管理者应组建数据管理体系内审机构，选聘适宜的内审代表（或在数据管理者内部委任，或聘请社会人士），负责数据管理体系内审。其职责应包括：

a）制定数据管理体系内审计划，并按计划实施；

b）独立、公平、公正地监控、检查、审计数据管理体系状况；

c）跟踪、监控数据管理体系构建、实施和运行过程；

d）适时评估、审计数据管理体系运行过程；

e）编制内审报告，推进数据管理体系持续改进、完善。

10 管理机制

10.1 管理制度

10.1.1 概述

应制定实施数据管理应遵循的相关规章和制度，包括基本的管理规章和适用于各从属机构、部门特点的管理细则，并使每个工作人员完全理解并遵照执行。

10.1.2 基本规章

基本规章是数据管理者及其工作人员应遵循的行为准则，应在实施过程中不断改进和完善。基本规章宜包括以下各项：

a）数据管理相关机构职能及职责；

b）数据管理（包括数据收集、处理、使用等）；

c）数据管理安全风险和安全管理措施；

d）内容数据库管理；

e）数据管理相关文档管理；

f）数据管理体系宣传、培训教育；

g）数据管理体系内审；

h）过程改进；

i）服务台管理；

j）应急管理；

k）违反相关规章的处理；

l）其他必要的管理制度。

10.1.3 管理细则

各从属机构、部门应根据实际需要制定与基本规章协调一致，并符合从属机构、部门实际、切实可行的相关管理细则。

10.1.4 其他管理规定

在业务（包括有特殊要求的业务）活动中，涉及相关数据，应制定相应的管理规定。

10.2 宣传

10.2.1 基本宣传

数据管理机构应在其内部向全体工作人员及其他相关人员说明数据管理的重要性和相关管理策略，以得到工作人员及其他相关人员对数据管理工作的配合和重视。

10.2.2 业务宣传

数据管理者处理涉及相关数据的业务时，应主动说明数据管理的目的、措施、方法和规定，并做出保密承诺。

10.2.3 社会宣传

个人信息管理者应在相关媒介（宣传资料、网络媒介[如网站等]及其他相关的面向社会的电子类、纸质等材料）中增加个人信息管理的相关内容。

10.3 培训教育

10.3.1 计划

数据管理机构应根据人员、机构、业务、需求等实际情况，制定数据管理相关的培训和教育制度、计划，适时开展相应的培训教育。

10.3.2 对象

培训教育的对象应包括数据管理者的各级管理、业务部门及其所有员工。员工应包括：

a）在职人员；

b）临时员工；

c）其他相关人员。

10.3.3 内容

培训教育的主要内容，应包括：

a）数据管理的基本知识；

b）数据管理的重要性和必要性；

c）数据安全相关法规、标准和管理制度；

d）数据主体的权利和维护；

e）数据管理体系的构成、实施等；

f）管理、业务活动中数据管理的方式、措施等；

g）违反数据管理相关标准可能引起的损害和后果；

h）其他必要的教育。

10.4 公示

数据公开、公示，应征得数据主体同意。通知数据主体的内容应包括：

a）数据管理者的相关信息；

b）公开、公示的目的、方式、范围和内容；

c）数据主体的权利；

d）公示和非公示的结果。

10.5 内容数据库管理

10.5.1 保存

应明确确认个人信息、商业数据是以简明、易懂的语言记载、存储在内容数据库中，并可以清楚无误地提取、拷贝这些信息。

10.5.2 时限

应根据相关法规、标准，设定合理的数据存储、保存时限，并与目的充分相关。

10.5.3 备案

应建立内容数据库使用、查阅备案登记制度，并有专人负责。记录应包括责任人、存储（保存）目的、时限、更新时间、获取方法、获取途径、位置、使用目的、使用方法、安全承诺、废弃原因和方法等。

10.6 数据管理文档

10.6.1 记录

应在数据管理过程中记录与数据相关的行为、活动的目的、时间、范围、对象、方式方法、效果、反馈等信息。这些活动或行为包括体系建立、培训教育、宣传、安全管理、过程改进、内审等。

10.6.2 备案

应建立与数据管理相关的规章、文件、记录、合同等文档的备案管理制度，并不断改进和完善。

10.7 人员管理

10.7.1 相关人员

应明确数据管理相关人员的权限、责任，加强监督和管理，防范未经授权的数据接触、职责不清等风险。

10.7.2 工作人员

应加强所有数据管理者相关工作人员的宣传和教育，明确岗位职责，提高保护数据主体权益的意识，避免发生数据安全事件。

10.7.3 保密

数据管理者应与全体工作人员和其他相关人员签署保密协议，明确个人信息、商业数据的保密原则、范围、等级、管理措施等。

11 管理过程

11.1 收集

11.1.1 目的

所有数据收集行为，应具有特定、明确、合法的目的，并应征得数据主体同意，限定在收集目的范围内。

11.1.2 限制

应基于特定、明确、合法的目的，采用科学、规范、合法、适度、适当的收集方法和手段，以保障数据主体的权益：

a）应将收集目的、范围、方法和手段、处理方式等清晰无误地告知数据主体，并征得数据主体同意；

b）应将收集目的、范围、内容、方法和手段、处理方式等以适当形式公开，如以公告形式发布。如有疑义、反对，应停止收集；

c）数据主体应采用适当的措施，防止不正当收集数据。

11.1.3 类别

11.1.3.1 直接收集

直接从数据主体收集相关数据时，应通知数据主体，并征得数据主体同意。应向数据主体提供的信息包括：

a）数据管理者的相关信息；

b）数据收集、处理、使用的目的、方法；

c）接受并管理该数据的第三方的相关信息；

d）数据主体拒绝提供相关数据可能会产生的后果；

e）数据主体的查询、修正、反对等相关权利；

f）数据安全和保密承诺；

g）后处理方式。

11.1.3.2 间接收集

非直接地、采用其他方式收集数据时，也应保证数据主体知悉并同意。间接收集应保证数据主体利益不受侵害。应保证数据主体知悉的信息参照 11.1.3.1。

11.2 处理

数据管理者处理、使用数据应基于明确、合法的目的，并遵循以下约束：

a）应征得数据主体同意；或为履行与数据主体达成的合法协议的需要；

b）应在数据收集目的范围内处理、使用数据。如需要超目的范围处理、使用数据，应征得该数据主体同意。通知信息参照 11.1.3.1。

c）处理、使用数据时，应履行第 5 章的要求，保证数据质量和数据安全。

11.3 提供

11.3.1 合法性

数据管理者所拥有的数据，应是依特定、明确、合法的目的，经数据主体同意，采取适当、合法、有效的方法和手段获得的，并不与收集目的相悖。

11.3.2 权益保障

数据管理者合法拥有的数据，在向第三方提供时，应履行第 5 章的要求，保障数据主体的合法权益。

11.3.3 授权许可

数据管理者向第三方提供数据，应获得数据主体授权，并在允许的目的范围内，采用合法、适当、适度的方法使用。应向数据主体说明的信息参照 11.1.3.1。

11.3.4 质量保证

第三方接受数据管理者提供的数据，应履行 5.5 的规定。

11.3.5 安全承诺

数据管理者向第三方提供数据时，应获得第三方以书面形式（或以可见证的、有规范记录的、满足书面形式要求的非书面形式）保证的数据完整性、准确性、安全性的明确承诺，避免不正确使用或泄露。

11.4 委托

11.4.1 范围限定

委托第三方收集数据、向第三方委托数据处理业务或接受数据处理委托业务时，应在数据主体明确同意的，或委托方以合同或其他方式要求的使用目的范围内处理，不可超范围、超目的随意处理，并将受托方相关信息提供给数据主体。提供的信息可参照 11.1.3.1。

11.4.2 委托信用

涉及数据委托业务时，应选择已建立数据管理体系的数据管理者，以建立相应的委托信用机制，保证不会发生数据泄露或滥用。在委托合同中应包括：

a）委托方和受托方的权利和责任；
b）委托目的和范围；
c）保护数据的安全措施和安全承诺；
d）再委托时的相关信息；
e）数据管理体系的相关说明；
f）与数据相关事故的责任认定和报告；
g）合同到期后数据的处理方式。

11.5 其他

11.5.1 二次开发

分析、整合、整理、挖掘、加工等数据的二次开发，应履行第 5 章的要求，征得数据主体同意，并限定在数据主体同意的范围内，避免随意泄露、传播和扩散。通知的内容应包括：

a）数据管理者的相关信息；
b）二次开发的目的、方式、方法和范围；
c）安全措施和安全承诺；

d）事故责任认定和处理方式；
e）开发完成后的处理方式。

11.5.2 交易

数据相关交易应履行第5章的要求，征得数据主体同意，并限制在数据主体同意的范围内处理使用，避免随意泄露、传播和扩散。通知的内容应包括：

a）数据管理者相关信息；
b）数据来源的合法性、有效性；
c）数据交易的必要性；
d）数据交易的目的、方式、方法和范围；
e）安全措施和安全承诺；
f）事故责任认定和处理方式；
g）交易完成后的处理方式。

11.6 使用

任何使用数据的行为，应履行第5章的要求，征得数据主体同意，并限定在数据主体同意的范围内，避免随意泄露、传播和扩散。通知信息参照11.1.3.1。

11.7 后处理

数据处理、使用后，应根据数据主体意见或合同约定方式，采取相应的安全措施，避免发生丢失、损毁、泄漏等安全事故。

11.7.1 质量

数据处理、使用后，如需继续保存、使用、返还，应保证数据的准确性、完整性和时效性。

11.7.2 销毁

数据处理、使用后，如不需继续保存、使用、返还，应彻底销毁与数据相关的文档、介质等及其记录的数据。

12 安全管理

12.1 风险管理

应在数据管理过程或行为中，识别、分析、评估潜在的风险因素，制定风险应对策略，采取风险管理措施，监控风险变化，并将残余风险控制在可接受范围内。

12.2 物理环境安全

应根据需要采取必要的措施，保证数据存储、保存环境的安全，包括防火、防盗及其他自然灾害、意外事故、人为因素等。

12.3 工作环境安全

应确保工作人员工作环境内所有相关数据的安全管理，防止未经授权的、无意的、恶意的使用、泄露、损毁、丢失。工作环境应包括：

a）出入管理；
b）工作桌面；
c）计算机桌面；
d）计算机接口；
e）计算机管理（文件、文件夹等）；
f）其他相关管理。

12.4 网络行为管理

应制定网络管理措施，采用相应的技术手段，引导、约束通过网络利用、传播相关数据的行为，构建规范、科学、合理、文明的网络秩序。

12.5 IT 环境安全

应在整体信息安全体系建设中，充分考虑数据及相关因素的特点，加强数据安全防护，预防安全隐患和安全威胁。如网络基础平台、系统平台、应用系统、安全系统、数据管理等的安全，及信息交换中的安全防范、病毒预防和恢复、非传统信息安全等。

12.6 存储安全

数据管理者应保证个人计算机系统、可移动存储媒介（电子、磁、纸等介质及其他介质）的安全，以确保数据存储的准确性、完整性、可靠性和安全使用。

12.7 内容数据库安全

数据管理者应保证内容数据库存储、保存的数据的准确性、完整性、保密性和可用性，并适时更新，以保证数据的最新状态。

12.7.1 管理安全

数据管理者应履行第 5 章的要求，建立内容数据库管理机制。管理安全应包括：
a）内容数据库管理和使用制度；
b）内容数据库管理者的职责；
c）维护和记录；
d）事故处理。

12.7.2 使用安全

应根据数据自动和非自动处理的特点，制定相应的内容数据库管理策略，包括访问/调用控制、权限设置、密钥管理等，防止数据的不当使用、毁损、泄露、删除等。

商业数据应建立商业数据库安全等级管理制度。

12.7.3 备份和恢复

应制定内容数据库备份和恢复机制，并保证备份、恢复的完整性、可靠性和准确性。

13 数据管理体系内审

13.1 管理

数据管理体系内审机构应依据相关法规、标准实施数据管理体系内审：

a）应审核数据管理相关活动和行为、数据管理体系、数据管理体系实施和运行过程；

b）内审应由与审核对象无直接关系人实施；

c）内审应提出过程改进和完善建议。

13.2 计划

应根据相关法律、规范和实际需求制定数据管理体系内审计划，主要应包括：

a）内审目标和原则；

b）内审策略和控制措施；

c）组织、协调相关资源；

d）内审周期、时间；

e）职责、责任；

f）内审实施；

g）其他必要的措施。

13.3 实施

应根据数据管理体系内审计划，定期独立、公平、公正地实施内审，并形成内审报告。

14 过程改进

14.1 服务台管理

服务台应接受数据主体、各类组织和人员提出的数据管理活动、数据管理体系的相关意见、建议、咨询、投诉等，并采取相应的处理措施，及时反馈。

14.2 跟踪和监控

数据管理体系内审机构应实时跟踪、监控数据管理体系的实施、运行，及时发现潜在的安全风险、缺陷和存在的问题，提出整改建议。

14.3 持续改进

数据管理机构应依据相关法规、内审报告、需求变化、服务台反馈、跟踪监控结果等，定期评估、分析数据管理体系运行状况，并持续改进和完善：

a）分析、判断数据管理体系实施、运行中的缺陷和漏洞；

b）制定预防和改进措施；

c）实时预防、改进；

d）跟踪改进结果。

14.4 过程模式

应采取 PDCA 模式（或其他以 PDCA 为基的相关模式），持续改进、完善数据管理过程、数据管理体系运行、数据管理体系内审过程。

15 应急管理

应制定应急预案，评估、分析获取、存储、处理和使用数据过程中可能出现的数据泄漏、丢失、损坏、篡改、不当使用等事件，采取相应的预防措施和处理。预案应包括：

a）事件的评估、分析；

b）事件的处理流程；

c）事件的应急机制；

d）事件的处理方案；

e）事件记录和报告制度；

f）事件的责任认定。

16 例外

16.1 收集例外

16.1.1 个人信息收集例外

不应收集、处理、使用敏感的个人信息。经个人信息主体同意，或法律特别规定的例外，但应采取特别的保护措施，履行第5章的要求。敏感的个人信息包括：

a）有关宗教、信仰、种族、血缘的事项；

b）有关身体障碍、精神障碍、犯罪史及相关可能造成社会歧视的事项；

c）有关健康、医疗及性生活的相关事项等；

d）法律特别规定的。

16.1.2 商业数据收集例外

不应收集下述商业数据。法律特别规定的例外，但应采取特别的保护措施，履行第5章的要求。这些商业数据包括：

a）商业数据主体认定的不可收集的商业数据；

b）竞业禁止协议适用的商业数据；

c）法律特别规定的。

16.2 法律例外

基于以下目的的例外，可以不必事先征得数据主体同意，但应依据相关法规，或经由专门机构确定：

a）法律特别规定的；

b）维护国家安全、公共安全、国家利益、制止刑事犯罪；

c）保护数据主体或公众的权利、生命、健康、财产等重大利益等。

17 管理评价

应对数据管理过程和数据管理体系实施过程进行认证，确定与相应法规、标准的符合性、一致性和目的有效性。

参 考 文 献

[1]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[2]OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

[3]ISO/IEC 27001:2005 Information technology-Security techniques-Information security management systems-Requirements

[4]ISO/IEC 27002:2005 Information technology-Security techniques-Code of practice for information security management

[5]Data Protection Act 1998

[6]個人情報の保護に関する法律（平成一五年五月三十日法律第五十七号）

[7]JIS Q 15001:2006 個人情報保護マネジメントシステム—要求事項

[8]BS 10012:2009 Data protection – Specification for a personal information management system

[9]GB/T22080-2008 信息技术 安全技术 信息安全管理体系 要求

[10]GB/T22081-2008 信息技术 安全技术 信息安全管理实用规则

[11]GB/T20984-2007 信息安全技术 信息安全风险评估规范

[12] GB/ Z 24364-2009 信息安全技术 信息安全风险管理指南

[13] 《中华人民共和国保守国家秘密法》

[14]商务部《关于保护网上商业数据的指导意见》（征求意见稿）

[15]个人信息保护法（专家建议稿）

[16]DB21/T 1628-2008 个人信息保护规范

[17]郎庆斌等 《个人信息保护概论》 人民出版社2008

[18]孙毅等《个人信息安全》 东北财经大学出版社2010