ICS 35.080
L 77

中华人民共和国国家标准

GB/T 33770.2—2019

信息技术服务　外包
第2部分:数据保护要求

Information technology service—Outsourcing—
Part 2:Data protection requirements

2019-08-30 发布　　2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 33770《信息技术服务　外包》分为6个部分：

——第1部分：服务提供方通用要求；

——第2部分：数据保护要求；

——第3部分：交付中心要求；

——第4部分：非结构化数据管理与服务要求；

——第5部分：发包方项目管理要求；

——第6部分：服务需方通用要求。

本部分为GB/T 33770的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本部分起草单位：大连软件行业协会、大连华信计算机技术股份有限公司、东软集团股份有限公司、成都市大数据中心、北京护航科技股份有限公司、广州赛宝认证中心服务有限公司、中国电子技术标准化研究院、金税信息技术服务股份有限公司、上海北宙企业管理咨询有限公司、上海有孚网络股份有限公司、北京信城通数码科技有限公司、广州番禺职业技术学院、上海三零卫士信息安全有限公司、神州数码系统集成服务有限公司、上海宝信软件股份有限公司、昆明东电科技有限公司、东软睿道教育信息技术有限公司、江苏润和软件股份有限公司、文思海辉技术有限公司。

本部分主要起草人：郎庆斌、尹宏、刘宏、高昕、陈锡民、赵振文、但强、于浩、梁晓雁、丁宗安、熊健淞、职亮亮、刘颋、张树玲、刘亭杉、杜远、唐百惠、王伟、邬敏华、李阳、郑义、王斌斌、万啟东、徐瑶、谢尚飞、韩沫、邵峰、董雷、宋悦、王鑫。

引　言

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

0.1　基准

本部分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，本部分中，代指涉及个人信息、商业数据的相关信息。

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

0.3　商业数据

“商业数据”亦是一个广义的概念，内涵宽泛。本部分中，特指敏感的商业秘密或其他需要保护的数据。

0.4　综合数据库

本部分限定综合数据库是由结构化、非结构化个人信息、商业数据（包括自动处理和非自动处理）分别构成的逻辑数据库。

0.5　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，本部分采用“数据管理”涵盖“数据保护”。本部分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。

0.6　数据安全性

本部分涉及的数据安全性，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。

0.7　数据管理体系

指具有特定功能、由相互关联的若干要素构成的有机整体，通过整合、协调资源，聚焦管理要素，实

现预定目标。要素与要素、要素与体系、体系与环境等之间相互作用又相互影响。

本部分为个人信息管理、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，充分保障数据主体的权利，保障相关业务的稳定、有效运行。

0.8 标准架构和体例

本部分以管理为主线，以数据生命周期为导向，构建数据管理标准架构，并不同于质量管理体系的标准体例，以便于集聚、整合管理要素，完善、改进、可控数据管理体系，以策数据安全。

0.9 标准兼容性

本部分与国际、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。

0.10 业务连续性

本部分在提供安全指导的同时，需基于数据的合理流通，保证业务的连续性。

0.11 标准适用性

IT服务外包组织与各类组织的数据安全属性、特征基本一致，其安全机制、安全策略是类同的，因而，本部分具有普适性：

a) 本部分规范的数据管理规则，既是IT服务管理的基础，亦可为IT服务的发展建立数据管理基准；

b) 本部分规范的数据管理规则，具有共性的特征，可以依据组织的特征解释、剪裁；

c) IT服务外包组织与各类组织的特征区别是组织的业务和管理，其所涉数据（含合同管理），亦为本部分范畴；

d) 本部分不仅适用于IT服务外包组织，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:数据保护要求

1　范围

GB/T 33770的本部分规定了信息技术外包服务中数据保护所涉及的数据生命周期、数据主体权利、数据管理者、数据管理、管理机制、数据获取、数据处理、安全管理、过程管理、应急管理等方面的基本规则和要求。

本部分适用于选择和提供IT服务、评价和认定IT服务提供能力的组织等。其他组织可参照执行。

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 22080　信息技术　安全技术　信息安全管理体系　要求

GB/T 22081　信息技术　安全技术　信息安全管理实用规则

3　术语和定义

下列术语和定义适用于本文件。

3.1

介质　medium

承载数据的载体。

3.2

媒介　mediation

存储、传输数据的载体。

3.3

媒体　media

生产、传播数据的媒介。

3.4

数据　data

描述个人信息、商业数据的形态、属性等,并便于保存、处理、使用。

3.5

个人信息　personal information

依附于个人,并可描述个人基本形态的信息,包括通过听觉、视觉、触觉等感官直接识别个人的信息,如声音、数字、文字、图像、影像等;借助各种手段间接识别个人的信息,如与个人相关各种信息对照、参考、分析等。

3.6

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），及其他需要保护的商业相关数据。

3.7

数据主体　data subject

可通过数据识别的数据所有者。

3.8

个人信息主体　personal information subject

可通过个人信息识别的、拥有且享有该个人信息权益的特定个人。

3.9

商业数据主体　business data subject

商业数据的合法所有者。

注：商业数据主体可由1个或多个民事主体构成。

3.10

综合数据库　general database

为实现一定目的，按照某种规则组织、管理数据的逻辑集合体。

3.11

个人信息数据库　personal information database

各种存在形态的个人信息构成的逻辑集合体，包括通过自动处理检索特定的个人信息的集合体，如磁媒体、电子及网络媒体等；采用非自动处理方式检索、查阅特定的个人信息的集合体，如纸媒体、声音、照片等；其他法律规定的可检索特定个人信息的集合体。

3.12

商业数据库　business database

各种存在形态的商业数据构成的逻辑集合体，包括可通过自动处理检索特定商业数据的集合体，如磁媒体、电子媒体及网络媒体等；可采用非自动处理方式检索、查阅特定商业数据的集合体，如纸媒体、声音、图片、产品等；其他法律规定的可检索特定商业数据的集合体。

3.13

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。

3.14

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。

3.15

数据生命周期　data life cycle

数据主体同意直接收集（或直接生成）数据直至数据彻底销毁的生命历程，是数据管理者向数据主体提供服务管理的过程。

注：数据生命周期可以是多重的，如间接收集应是数据生命周期内存在的新的生命周期。

3.16

数据管理体系　data management system

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。

3.17

数据管理方针　data management policy

数据管理者应遵守的行为规则，是数据管理的基准。

3.18

数据质量　data quality

数据的完整性、准确性、可用性和实效性。

3.19

收集　collection

基于明确、合法目的获取数据的行为。

3.20

处理　processing

自动或非自动处置数据的过程。

注：如加工、编辑、存储、检索、交换、传输、输出及其他使用行为或活动。

3.21

自动处理　automatic processing

利用计算机及其相关的和配套的设备、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。

3.22

非自动处理　non-automatic processing

除自动处理外的其他数据处置行为或活动。

3.23

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。

注 1：表达形式包括数据主体以书面形式同意，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 2：下述情况视为数据主体同意：

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；

c) 构成商业数据主体的多个民事主体表达的意愿完全一致。

4　缩略语

下列缩略语适用于本文件。

IT：信息技术(Information Technology)

PDCA：计划-实施-检查-改进(Plan-Do-Check-Act)

5　数据生命周期

数据生命周期应包括 3 个环节：

a) 数据获取过程：

1) 个人信息主体同意，基于特定、明确、合法目的，直接或间接收集个人信息；

2) 商业数据主体具有完全自主知识产权、直接生成的商业数据；

3) 商业数据主体同意，基于特定、明确、合法目的，直接或间接收集商业数据。

b) 数据处理过程：基于收集目的的数据使用、利用过程，或基于明确目的的直接生成的商业数据的使用、利用过程，包括：
   1) 编辑、加工、检索、存储、传输等不同的使用流程；
   2) 提供、委托、交换等不同的利用过程；
   3) 交易、二次开发等不同的利用过程；
   4) 数据的后处理过程。
c) 过程管理：在数据生命周期内，采用 PDCA 模式管理针对数据及相关资源、环境、管理体系等的活动或行为。

6 数据主体权利

6.1 知情权

知情权主要应包括：
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。

6.2 支配权

支配权主要应包括：
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。

6.3 控制权

商业数据主体对具有完全自主知识产权、直接生成的商业数据具有控制权，主要应包括：
a) 基于组织的环境、条件、运营目标等，具有完全的自主权利；
b) 控制数据应用的目的、处理、使用、范围和方式、方法等；
c) 自主管理、约束、监控商业数据的相关活动或行为等。

6.4 共享权

商业数据主体由 2 个或多个民事主体构成时，对其具有完全自主知识产权、直接生成的商业数据，应具有共享权：
a) 2 个或多个民事主体直接参与商业数据直接生成的过程、活动、行为，各自享有所有权；
b) 基于商业数据相关各方签署的有效文件，确定相关各方的权利等。

6.5 质疑权

质疑权主要应包括：
a) 数据主体有权质疑与之相关的数据质量；
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。

7 数据管理者

7.1 规则

数据管理者的约束规则应包括：

a) 数据管理者获取、处理、使用、利用、管理数据应获得数据主体授权，并确定明确、合法的目的；

b) 数据管理者应基于数据生命周期，为数据主体提供数据相关的服务管理；

c) 数据管理者不应因利益、条件等的变化降低数据管理质量的可靠性。

7.2 角色

7.2.1 描述

数据管理者可根据不同的需要细分角色，如数据获取、数据消费等，但均应遵循7.1确立的规则，保障数据主体的权益。

7.2.2 行为模式

角色细分应根据不同的行为模式划分，包括：

a) 限定数据管理者为合法、有效的数据管理组织；

b) 数据管理者的细分角色，根据目的、动机、方法等的不同存在行为差异；

c) 数据管理者细分角色的行为差异，存在合法和非法的可能性；

d) 数据管理者的细分角色可在条件、利益满足时转化。

7.2.3 约束

数据管理者根据不同需要细分的不同角色，具有同样的管理职能、权利和义务，均应遵循本部分确立的数据管理者的约束规则、责任和义务。

7.3 服务管理

数据管理应是数据管理者向数据主体提供服务的过程。数据管理者应满足：

a) 具有各类资源的转换能力和相应的管理职能，以保证数据管理的有效性；

b) 建立有效的内部管理机制并形成管理体系，以保证数据管理的质量可靠性；

c) 提供透明的服务管理过程，以保证第6章确立的数据主体的权力。

7.4 责任和义务

7.4.1 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。

7.4.2 权利保障

数据管理者应保障数据主体的权利。

7.4.3 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。

7.4.4 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。

7.4.5 质量保证

数据管理者应在管理活动或行为中保证数据质量，并保持最新状态。

7.4.6 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。

8 数据管理

8.1 要求

数据管理者应依据 7.4.1 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。数据管理相关资源见附录 A。

8.2 原则

8.2.1 目的明确

数据收集、处理、使用应基于明确、合法的目的，并应经数据主体明确同意。

8.2.2 主体权利

数据主体对相关的个人信息、商业数据享有权利。

8.2.3 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。

8.2.4 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。

8.2.5 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。

8.2.6 责任

应保证各项原则的有效实施。

8.3 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，制定数据管理方针，以指导数据管理。方针应以简洁、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) 数据管理者的责任义务；
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。

8.4 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。

8.5 组织

8.5.1 要求

数据管理者应根据管理计划，实施数据生命周期全过程的符合相关法规、标准的管理，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。

8.5.2 数据管理主体及职责

8.5.2.1 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，并选择、任命有能力的数据管理者代表，组建、负责相应的数据管理机构，并在资金、资源等各个方面提供完全的支持。其职责应包括：
a) 确立数据安全、保证管理和业务稳定运行的目标和方向；
b) 创造全体员工参与、资源保障、有利于实施数据管理的内部环境；
c) 组建数据管理机构，选择有能力的管理者代表，并赋予相应权限，确保数据管理体系的实施和运行；
d) 为实施、运行数据管理体系所需资源提供切实可行的支持，资源包括人员、资金、信息、技术、环境等；
e) 对数据管理体系实施、运行过程中可能出现的各种不利因素提供决策支持；
f) 为数据管理体系实施、运行制定合理、适宜的激励机制；
g) 对数据管理体系的持续改进提供决策支持；
h) 组建数据管理体系内审机构，选择适宜的内审代表，并赋予相应的权限，监控、检查、评估数据管理体系的实施和运行；
i) 批准数据管理相关责任主体的职责分配、数据管理方针、数据管理规章、数据安全宣传教育计划等管理机制，并协调、组织实施数据管理体系等。

8.5.2.2 数据管理者代表

应是最高管理者指定的数据管理机构责任主体，其职责应包括：

a) 代表最高管理者提出并制定数据管理计划；
b) 代表最高管理者负责数据管理机构的组建和日常工作；
c) 制定数据管理方针；
d) 负责数据管理体系构建、实施和运行；
e) 确定组织、构建和实施数据管理体系的资源需要和资源分配；
f) 组织制定、实施数据管理的基本规章制度，推进数据管理工作的开展；
g) 部署数据安全宣传，指导数据安全的培训和教育；
h) 监督数据安全管理机制的构建和实施；
i) 监督、指导数据管理体系各项文档的管理；
j) 数据管理体系实施、运行过程中的组织、协调和管理；
k) 协调内审机构的工作；
l) 实施过程改进。

8.5.2.3 管理机构

8.5.2.3.1 主要职责

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。其职责应包括：

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) 数据相关的活动、行为的管理，包括相关宣传教育、安全管理、服务咨询等；
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。

8.5.2.3.2 责任主体

数据管理责任主体，宜包括数据管理者从属的各机构、部门的负责人，并履行相应的管理职责。涉及的数据管理机构宜包括：

a) 宣传教育：宜指定责任主体，在数据管理者代表领导下开展工作。其主要职责应包括：
   1) 组织、实施数据管理体系宣传、教育；
   2) 制定数据管理体系宣传、教育制度、计划；
   3) 制定数据管理体系宣传策略和方法；
   4) 数据的相关知识、管理和安全技术等的宣传、教育；
   5) 改进、完善宣传、教育措施、方法。
b) 安全管理：宜指定信息安全责任主体负责，在数据管理者代表指导下开展数据安全管理工作。其职责应包括：
   1) 数据安全风险管理；
   2) 制定数据安全管理策略、措施；
   3) 实施数据安全管理措施；
   4) 改进、完善数据安全管理。

c） 服务台：宜指定责任主体，在数据管理者代表领导下提供数据的相关服务。其职责应包括：

1） 提供数据管理、安全的相关咨询和服务；

2） 提供数据处理、使用建议和意见；

3） 接受有关数据管理、安全的意见，并落实和反馈；

4） 沟通、交流；

5） 数据管理、安全相关事项、问题处理等的发布；

6） 其他应处理的问题等。

8.5.2.4 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。

8.6 数据管理体系

8.6.1 要求

数据管理者代表应建立基于服务管理的数据管理体系，满足数据管理的需要。数据管理体系主要应包括以下要素：

a） 数据管理目标和基本原则；

b） 数据管理方针；

c） 数据管理机构及职责；

d） 数据管理机制；

e） 数据获取过程；

f） 数据处理过程；

g） 数据安全管理；

h） 过程管理等。

8.6.2 流程

组织构建数据管理体系的流程，主要应包括：

a） 建立数据管理相关机构，明确机构职责和机构责任主体的责任。

b） 明确数据管理目标，确立数据管理的基本原则。

c） 制定数据管理方针，阐明数据管理的指导原则。

d） 根据管理和业务特征、资源、技术、环境、员工及其他相关因素确定数据管理体系范围。

e） 制定数据管理计划，明确数据管理活动或行为的准则。

f） 实施风险管理，识别风险源和安全隐患，确定数据管理体系的控制目标和控制方式。

g） 建立数据管理机制：

1） 根据管理和业务特征、信息安全相关法规、规范，制定数据管理应遵循的基本规章、数据管理体系运行规范和所有员工应遵循的制度；

2） 数据管理策略、管理模式，包括数据存储、保存、处理、使用、利用等；

3） 制定数据安全宣传策略，在内、外部宣传数据安全的重要性和所采取的管理策略；
4） 制定数据安全培训教育计划，对全体员工实施数据安全相关知识的教育，并跟踪培训教育的效果；
5） 其他数据相关管理事务等。

h） 在数据管理过程中，采用相应的管理、技术手段，保证与目的的一致性、符合性，保证数据的安全和数据主体的权益。
i） 数据安全管理。
j） 基于数据生命周期的过程管理：
1） 建立数据管理体系内审机制。检查、评估数据管理体系实施和运行过程，持续改进和完善体系；
2） 跟踪、监控数据管理体系实施、运行，随时改进、完善。
k） 应急管理，建立应急预案，对可能发生的数据安全事件或数据安全事故，及时采取相应的应对措施等。

8.7 资源管理

8.7.1 相关资源

应识别与管理、业务涉及数据部分关联的各种资源，见附录A。

8.7.2 资源分类

资源应分类管理，分类原则应包括：
a） 结合风险管理，确定在数据管理体系实施、运行中资源的敏感、关键程度；
b） 在涉及数据的管理、业务中所关联资源的重要性；
c） 涉及资源的数据的价值；
d） 资源的安全等级等。

8.7.3 资源使用

应制定使与数据管理者所有相关人员接受并执行的与数据相关资源的使用规定，如：
a） 网络使用规定；
b） 电子邮件使用规定；
c） 移动设备使用规定；
d） 系统软件更新、病毒防范；
e） 综合数据库管理；
f） 文档管理；
g） 门禁管理等。

与数据管理者所有相关人员应对所使用的资源负责。

8.8 控制

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

8.9 协调

在数据管理活动或行为中，应注意数据主体与数据管理者、数据管理者各部门（从属机构）与数据管理体系、数据管理体系内、数据管理体系与相关资源之间等的协调、沟通。

9 管理机制

9.1 管理制度

9.1.1 综述

应制定实施数据管理应遵循的相关规章和制度，并使每个工作人员完全理解并遵照执行。

9.1.2 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) 数据安全风险和安全管理措施；
d) 综合数据库管理；
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。

9.1.3 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一致，并符合从属机构、部门实际、切实可行的相关管理细则。

9.1.4 其他管理规定

在业务（包括有特殊要求的业务）活动中，涉及相关数据管理，应制定相应的管理规定。

9.2 宣传

9.2.1 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。

9.2.2 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、方法和规定等，并做出保密承诺。

9.2.3 社会宣传

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

9.3 培训教育

9.3.1 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。

9.3.2 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。

9.3.3 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。

9.4 公示

数据公开、公示，应通知数据主体并征得数据主体同意。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等。

9.5 数据库管理

9.5.1 媒介

综合数据库是数据管理者在数据管理过程中的所有记录及相关媒介。主要应包括：

a) 磁介质：计算机硬盘、数据存储设备（如磁盘阵列等）、移动存储设备（如移动硬盘、U 盘、磁带等）、手持移动设备（如智能手机、PDA、PAD 等）等；
b) 光介质：光盘、光存储设备等；
c) 芯片介质：芯片卡（如银行卡、护照等）；
d) 纸介质：纸质文档；
e) 电子媒介：广播、电视、电影等；
f) 网络媒介：博客、微博、微信、论坛、邮件、即时通信、网站、网络视频等；
g) 多媒体媒介：录音、录像等。

9.5.2 管理限制

综合数据库管理应满足条件：

a) 各种媒介记载、存储数据，应简明、清晰、可识别，易于提取、复制；

b) 各种媒介记载、存储数据，应根据环境、条件、业务、管理等实际需要，确定适宜的管理时限；

c) 各种媒介记载、存储数据，应保证准确性、完整性、可用性，并在数据发生变化时，及时更新，保持最新状态；

d) 数据库媒介应保存在适宜媒介存放的环境、条件下，并保证综合数据库的保密性、安全性。

9.5.3 移动数据管理

9.5.3.1 移动综合数据库

数据管理者、个人保有的可移动设备、媒介等所存储、保存的数据构成移动的综合数据库，应包括：

a) 移动存储设备、手持移动设备形成的可移动的个人信息、商业数据存储；

b) 数据主体随身携带的芯片卡、纸质文档等形成的个人信息、商业数据储存等。

9.5.3.2 安全防范

数据主体应在各种公共空间、网络空间、通信等场合，提高安全意识，注意采取可能的安全防范措施，防止不正当收集个人信息、商业数据，避免数据泄漏。

9.5.4 保存

应确认个人信息、商业数据是以简明、易懂、易识别的文字、符号等记载、存储在个人信息数据库、商业数据库中，并可以清楚无误地提取、复制这些信息。

9.5.5 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。

9.5.6 形式

各类保存、存储媒介记载、存储的个人信息、商业数据，应形成逻辑统一的个人信息数据库、商业数据库，并构建规范、统一的相应的数据库事务：

a) 数据管理者内部的个人信息、商业数据，应在管理过程中分别建立统一的数据库事务；

b) 数据管理者业务相关的个人信息、商业数据，应在业务管理过程中分别建立统一的数据库事务；

c) 移动的数据也宜形成规范的综合数据库事务。

9.5.7 管理

综合数据库的管理，应由数据管理者代表指定专人负责，并明确管理职责。应制定相应的综合数据库管理相关规章制度。

9.5.8 备案

应建立综合数据库使用、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。

9.6 数据管理文档

9.6.1 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。

9.6.2 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。

9.7 人员管理

9.7.1 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。

9.7.2 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。

9.8 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。

10 数据获取

10.1 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。

10.2 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) 间接或被动收集时，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；
d) 收集商业数据时，应取得商业数据主体共享权利各方的一致同意，如有不同意见，应停止收集。

10.3 类别

10.3.1 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。

10.3.2 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见10.3.1。

10.3.3 被动收集

在数据主体不知情或不能控制的情况下收集、处理、使用、利用数据，应保证数据主体权益不受侵害：

a） 应遵循7.4、8.2确定的责任、义务和原则；
b） 应遵循10.2的限制；
c） 通过各种电子媒介（如博客、微博、微信、论坛、云盘、网盘、邮件、即时通信、网站、网络视频等）、纸媒体等获取公开的数据，亦应遵循7.4、8.2确定的责任、义务和原则，同时应遵循10.2的限制；
d） 依据10.2，应采取适宜的方式公告、公示。通过公告、公示保证数据主体知悉的信息，见10.3.1。

10.4 保存

以各种形式、方式收集（生成）的数据，应保存或存储在统一的个人信息数据库、商业数据库内，并应依据9.5建立相应的数据库管理机制。

11 数据处理

11.1 过程

在数据处理过程中，应遵循：

a） 根据第7章、第8章的相关规则，管控数据处理过程，以保证数据质量和数据主体权益；
b） 接受内审机构的检查、监控，随时改进、完善数据处理过程，以保证数据安全。

11.2 使用

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。通知信息见10.3.1。
c） 任何处理、使用数据的行为，应履行7.4、8.2规定的责任、义务和原则，征得数据主体同意，并限定在数据主体同意的范围内，避免随意泄漏、传播和扩散，以保证数据安全。通知信息见10.3.1。

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，应按照第6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，见10.3.1。

11.3.4 质量保证

第三方接受数据管理者提供的数据，应遵循7.4关于质量保证的原则。

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。提供的信息见10.3.1。

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 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7.4、8.2规定的责任、义务和原则，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。

11.6 交易

11.6.1 数据交易

数据交易应保证：
a) 应限定在法律许可的范围内；
b) 应通知数据主体并征得数据主体同意，且限定在数据主体同意的范围内处理使用，避免随意泄漏、传播和扩散；
c) 交易双方均应履行 7.4、8.2 规定的责任、义务和原则，保障数据主体权益。

11.6.2 数据主体

通知数据主体的内容应包括：
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。

11.7 后处理

11.7.1 总则

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。

11.7.2 质量

数据处理、使用后，如需继续保存、使用、返还，应保证数据质量。

11.7.3 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、媒体等及其记录的数据。

12 安全管理

12.1 要求

安全管理应遵循 GB/T 22080、GB/T 22081 的规则：
a) 融合信息安全管理体系，统一规划、设计信息安全；
b) 融合中考虑个人信息、商业数据的安全特征和需要；
c) 依据统一的设计，构建信息安全体系。

12.2 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。

12.3 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。

12.4 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) 办公桌面；
c) 计算机屏幕；
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。

12.5 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。

12.6 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、数据传输等的安全，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。

12.7 存储安全

数据管理者应保证计算机系统、可移动存储媒介(电子、磁、纸等介质及其他媒介)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。

12.8 数据库安全

12.8.1 总则

数据管理者应保证综合数据库存储、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。

12.8.2 管理安全

数据管理者应按照 9.5 的要求，建立综合数据库管理机制，包括：

a) 综合数据库管理和使用制度；
b) 综合数据库管理者的职责；
c) 维护和记录；

d) 事故处理等。

12.8.3 使用安全

应根据数据自动和非自动处理的特点，制定相应的综合数据库管理策略，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。

12.8.4 备份和恢复

应制定综合数据库备份和恢复机制，并保证备份、恢复的数据质量。

12.9 移动终端安全

12.9.1 管理安全

应制定与数据相关的移动设备、媒体的管理制度，采用管理和技术措施，并建立设备使用追踪回溯机制，防止数据毁损、泄漏、删除、遗失等。

12.9.2 终端安全

数据主体对所保有的移动设备，应提高安全意识，根据不同的物理环境和使用环境，采取相应的安全防范措施，避免数据泄漏。

12.10 数据主体安全

在多种情况下，数据主体应提高安全意识，采取相应和适当的措施，防止不当收集、使用、利用数据，以保护数据主体权益。这些情况可包括：

a) 各种网络环境下与数据相关的各种行为、活动；
b) 各种工作环境下与数据相关的各种行为、活动；
c) 各种生活环境下与数据相关的各种行为、活动；
d) 各种社会活动中与数据相关的各种行为、活动等。

13 过程管理

13.1 过程模式

应采取 PDCA 模式(或其他以 PDCA 为基础的相关模式)，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：

a) 计划(构建数据管理体系)：根据数据管理者的整体目标，确立数据息管理目标和方针，实施数据管理计划，构建数据管理体系；
b) 实施(实施和运行数据管理体系)：实施和运行数据管理体系；
c) 检查(监控和内审数据管理体系)：监督、检查、控制数据管理体系的实施和运行，实施内部审查和评估，报告内审结果；
d) 改进(完善和改进数据管理体系)：根据内审结果和其他相关信息，采取相应的预防、改进、完善措施，实现数据管理体系的持续改进。

13.2 内审

13.2.1 管理

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。

13.2.2 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) 内审实施步骤；

g) 其他必要的措施。

13.2.3 实施

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

13.3 过程改进

13.3.1 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。

13.3.2 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。

13.3.3 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 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方法。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。

15 例外

15.1 收集例外

15.1.1 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，按照第6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) 基因、生物特征信息；
c) 有关身体、精神等健康信息、医疗及性生活的相关事项；
d) 犯罪史及相关可能造成社会歧视的事项等；
e) 法律特别规定的。

15.1.2 商业数据收集例外

商业数据不应收集的数据，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) 法律特别规定的数据（应按照第7章的要求，采取特别的保护措施）。

15.2 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。

16 管理评价

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

附 录 A
（规范性附录）
数据管理相关资源

与管理、业务涉及数据部分关联的各种资源，主要应包括：

a） 信息资产：综合数据库及相应文件、合同和协议；数据管理文档等数据管理者运营、服务涉及数据的信息及相应的各种存储、保存媒体等；

b） 软件资产：系统软件、应用软件、工具软件、开发工具、服务等支撑管理、业务运营的存储、处理信息的软件；

c） 硬件资产：保证管理、业务等运行的基础设施，如计算机设备、网络设备、通信设备、存储设备及其他相关设备等；

d） 移动资产：移动存储设备（如移动硬盘、闪存盘、磁带等）、智能移动终端等；

e） 物理资产：门禁、监控等保证工作环境安全的物理设施；

f） 技术资产：数据管理相关的各种技术及支撑手段；

g） 人力资源：数据管理体系涵盖的各类员工；

h） 无形资产：姓名、荣誉、名誉、肖像等没有实体形态、具有潜在利益的数据资源；

i） 服务：资源管理、数据通信等数据管理者所提供的各种服务等。

参 考 文 献

[1] GB/T 20984—2007 信息安全技术 信息安全风险评估规范

[2] GB/Z 24364—2009 信息安全技术 信息安全风险管理指南

[3] GB/T 35273—2017 信息安全技术 个人信息安全规范

[4] DB21/T 1628(所有部分) 个人信息安全标准系列

[5] 中华人民共和国网络安全法

[6] 中华人民共和国保守国家秘密法

[7] 郎庆斌,等.个人信息保护概论[M].北京:人民出版社,2008.

[8] 孙毅.个人信息安全.大连:东北财经大学出版社,2010.

[9] 郎庆斌,等.个人信息安全-研究与实践.北京:人民出版社,2012.

[10] 郎庆斌,等.IT 服务标准研究-理论和实践.北京:人民出版社,2015.

[11] ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements

[12] ISO/IEC 27002:2013 Information technology—Security techniques—Code of practice for information security management

[13] BS 10012:2009 Data protection—Specification for a personal information management system

[14] 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

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

[16] General Data Protection Regulation 2016

[17] Data Protection Act 1998

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

[19] 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)