ICS 35.020
CCS L70

DB21

辽 宁 省 地 方 标 准

DB 21/T XXXX—XXXX

信息安全技术 数据管理规范

Information security technology-Specification for data management

（征求意见稿）

（本草案完成时间：2021-09-14）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

辽宁省市场监督管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中共辽宁省委网络安全和信息化委员会办公室提出并归口。

本文件起草单位：大连软件行业协会、大连交通大学、大连华信计算机技术股份有限公司、大连奥远电子股份有限公司、辽宁省信息中心、大连理工现代工程检测有限公司、大连市计算机学会。

本文件主要起草人：郎庆斌、尹宏、刘宏、胡剑锋、于青、杨万清、杨莉、才昊、司丹、孙毅、王小庚。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

本文件归口单位通讯地址：沈阳市和平区光荣街26号甲，联系电话：024-81680033

本文件起草单位通讯地址：大连市高新园区火炬路32号创业大厦A座5层，联系电话：0411-83655207

引　言

由于一般数据与个人信息（自然人个体数据）存在特征差异，二者的安全特征、管理特征亦存在差异，因此，一般数据与个人信息的管理规范不能混为一谈。

个人信息管理规范，已发布实施DB21/T 1628系列标准，因此，本文件中“数据”不包含个人信息。

信息安全技术 数据管理规范

1 范围

本文件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。

本文件适用于IT服务组织，其它组织可参照执行。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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/T22080 信息技术 安全技术 信息安全管理体系 要求

GB/T22081 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

数据 data

未经处理的客观事物的原始记录，描述客观事物的性质、状态、属性、相互关系等。数据对象可以是连续的，如声音、图像等，也可以是离散的，如符号、数字、文字等。

注：数据也可以是虚拟世界中虚拟事物的原始记录。

3.2

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），及其它需要保护的商业相关数据。

3.3

数据主体 data subject

享有数据权益的数据所有者或合法拥有数据，并享有该数据权益的组织。

注：组织是为实现其目标而具有其自身职能、职责、权限和相互关系的个人或一组人的群体（ISO9001）。

3.4

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。

3.5

数据管理者 data controller

获数据主体授权，基于明确、合法目的，管理、使用数据的组织。

3.6

数据生命周期 data lifecycle

当数据主体同意直接取得（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，如间接取得应是数据生命周期内存在的新的生命周期。

3.7

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、评估、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。

3.8

数据管理策略 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。数据管理策略确立了数据管理的目标、原则、方法、措施等。

3.9

取得 gain

指基于明确、合法目的获取数据的行为。

3.10

处理 processing

指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。

3.10.1

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。

3.10.2

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。

3.11

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。

4 缩略语

下列缩略语适用于本文件。

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。本文件用于数据管理相关活动的质量管理。

5 概述

5.1 数据管理框架

数据管理框架是基于数据全生命周期内要素之间的关联关系形成的数据管理架构，如图1所示：

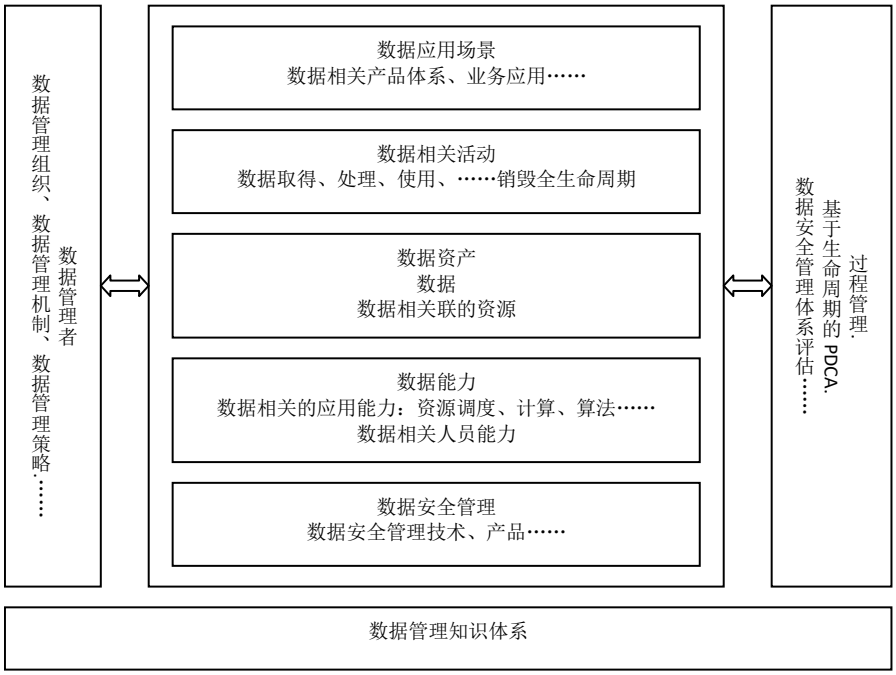

图1　数据管理框架

5.2　数据生命周期

以数据为基的相关活动，构成完整的全数据生命周期。数据生命周期应包括3个环节：

a)　数据取得过程：

1)　数据主体具有完全自主知识产权、直接生成的数据；

2)　数据主体同意，基于特定、明确、合法目的，直接或间接取得数据；

3)　其它方式取得的数据等。

b)　数据处理过程：基于取得目的的数据使用、利用过程，或基于明确目的的直接生成的数据的使用、利用过程，可划分 4 种形式：

1)　包括存储、编辑、组织、加工、检索、抽取、清洗、比对、分类、传输等不同的使用流程；

2)　包括提供、委托、交换等不同的利用过程；

3)　包括交易、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。

5.3　知识体系

5.3.1　描述

应在数据管理实践中，逐步积累、构建数据管理相关的技术、产品、模式（方法）、质量、安全、管理评估等相关知识体系，并通过体系化管理，形成最佳实践。

5.3.2　框图

数据管理知识体系，如图2示：

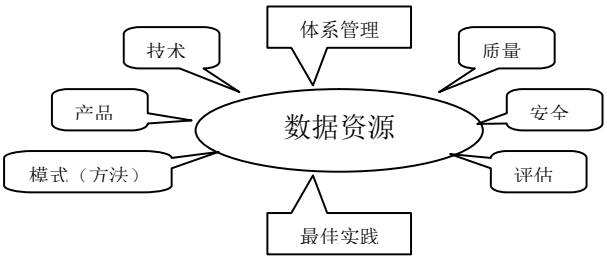

图2　数据管理知识体系

6　数据主体权利

6.1　知情权

知情权主要应包括：

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

6.2　控制权

控制权主要应包括：

a）　明确同意目的的数据采集、处理、使用；
b）　基于组织的环境、条件、运营目标等，具有完全的自主权利；
c）　有权控制、自主决定数据应用的目的、采集、处理、使用、范围和方式、方法等；
d）　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；
e）　有权自主管理、约束、监控数据的相关活动或行为；
f）　有权决定与之相关数据的携带、转移、迁移、传输等。

6.3　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它正当理由，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；
d）　数据主体有权基于自己的判断撤回数据主体同意，并与数据管理者协商同意撤销之前的工作等。

6.4　财产权

财产权主要应包括：

a）　数据主体有权决定与之相关数据的交易、交换、开发等；

b） 数据主体有权决定与之相关数据的权益、收益；
c） 数据主体有权撤销涉及与之相关数据权益的活动、行为等。

7 数据管理者

7.1 规则

数据管理者的约束规则，主要应包括：
a） 数据管理者取得、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不同的角色，如数据取得、数据控制、数据处理、数据消费等，但均应遵循第6章确立的规则，保障数据主体的权益。

7.2.2 行为模式

角色细分应是根据不同的行为模式划分的：
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，均应遵循本标准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） 数据管理者应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） 数据管理者应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） 数据管理者应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

数据管理者应保证所管理数据相关活动、行为的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

数据管理者应将所管理数据的相关活动、行为的目的、方式、不提供数据的后果、数据主体权利，以及数据管理者本身的相关信息等告知数据主体。

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的完整性、准确性、有效性和可用性。

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

数据管理者应依据本标准，协调、组织数据管理体系和各类相关资源，根据取得、处理目的，采取相应的控制策略和措施，处理、使用数据。

8.2 原则

8.2.1 目的明确

数据取得、处理、使用应基于明确、合法的目的，并应经数据主体同意。

8.2.2 主体权利

数据主体应享有本标准规定的权利。

8.2.3 数据质量

在数据管理相关行为或活动中，应保证数据的准确、完整、可用、真实、可控和可追溯。

8.2.4 使用限制

应采用合理、合法的手段和方式，取得、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、篡改等安全事件。

8.2.6 责任

应保证各项原则的有效实施。

8.3 策略

数据管理者应基于实际情况，依据国家相关法规、标准和本标准的原则、措施，制定数据管理策略。数据管理策略应以简洁、明确的语言阐述、公示，以指导数据管理工作。内容应包括：

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) 数据相关事件处理办法等。

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) 数据全生命周期内的目的、控制措施和策略；
b) 数据管理措施、策略；
c) 数据管理、数据生命周期内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) 其它必要的管理策略等。

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、标准和本标准的管理，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) 其它相关管理等。

8.5.2 相关机构及职责

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，基于数据管理者管理、资源、业务等能力，组建、负责适宜的数据管理相关机构，并在资金、资源等各个方面提供完全的支持。其责任应包括：

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) 组建适宜的数据管理机构，选择有能力的责任主体，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、数据管理策略、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 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) 制定数据管理策略；
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) 实施过程改进等。

8.5.2.3 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) 数据相关管理活动、行为控制，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。

8.5.2.4 责任主体

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。其主要职责应包括：
   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。其主要职责应包括：
   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) 其它应处理的问题等。
d) 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。

8.5.2.5 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。

8.5.3 数据管理体系

8.5.3.1 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) 数据管理策略；
c) 数据管理机构及职责；
d) 数据管理机制；
e) 数据取得过程；
f) 数据处理过程；
g) 数据安全管理；
h) 过程管理等。

8.5.3.2 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) 制定数据管理策略，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、员工及其它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，包括：
   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) 其它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，包括：
   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。

8.6 资源管理

8.6.1 相关资源

应识别数据相关管理、业务关联的各种数据资源，主要应包括：
a) 信息资产：各类数据库及相应文件、合同和协议；数据管理文档等数据管理者运营、业务、服务涉及数据的信息及相应的各种存储、保存介质等；
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、存储设备及其它相关设备等；
d) 移动资产：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、个人数码助理等）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：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。

8.6.2 资源分类

相关资源应分类管理，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） 在数据相关管理、业务中所关联资源的重要性；
c） 涉及资产的数据的价值；
d） 资产的安全等级等。

8.6.3 资源使用

应制定使全体员工、客户、第三方客户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） 数据库管理；
f） 文档管理；
g） 门禁管理等。
全体员工、客户、第三方客户应对所使用的资源负责。

8.7 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。

8.8 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，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。

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。

9.1.2 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。

9.1.3 其它管理规定

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介（宣传资料、网络媒介（如网站等）及其它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) 其它必要的教育。

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) 数据权属；
c) 公开、公示的目的、方式、范围和内容；
d) 数据主体的权利；
e) 公示和非公示的结果等。

9.5 数据管理文档

9.5.1 记录

9.5.1.1 管理文档

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。

9.5.1.2 过程文档

应建立数据生命周期全过程的文档管理机制，记录数据取得、处理、使用相关行为、活动的所有相关信息，包括目的、时间、内容、方式方法、安全评估等信息。

9.5.2 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。

9.6 人员管理

9.6.1 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。

9.6.2 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。

9.6.3 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，明确数据的保密原则、范围、等级、管理措施等。

10 数据取得

10.1 目的

所有数据取得行为，应具有特定、明确、合法的目的，并应以适当方式征得数据主体同意，限定在目的范围内。

10.2 限制

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

a) 应将取得数据的目的、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) 间接或被动取得数据时，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） 取得公开数据时，应明确数据权属，并遵从本条款规定；
d） 数据主体应采用适当的措施，防止不正当取得数据。

10.3 类别

10.3.1 直接取得

直接从数据主体取得相关数据时，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） 数据取得、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） 数据主体权利；
f） 数据安全和保密承诺；
g） 后处理方式等。

10.3.2 间接取得

非直接地、采用其它方式获取数据时，也应保证数据主体知悉并同意。间接收集应保证数据主体权益不受侵害。应保证数据主体知悉的信息参照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取得、处理、使用、利用数据，应保证数据主体权益不受侵害：

a）应遵循第8章、第7章确定的原则和责任义务；
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、即时通讯、网站、网络、视频等）、纸媒体等获取公开的数据，亦应遵循第7章、第6章确定的原则、责任义务，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,参照10.3.1。

10.4 保存

以各种形式、方式取得（生成）的数据，应以适当方式保存或存储在相应的数据库中，并建立相应的管理机制。

11 数据处理

11.1 要求

在数据处理过程中，应遵循：

a） 应根据第 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） 涉及敏感的数据，如商业数据，应根据数据处理的要求和规则清洗、脱敏；
c） 应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) 应在取得数据的目的范围内处理、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 10.3.1。
c) 任何处理、使用数据的行为，应履行第 8 章、第 7 章规定的原则和责任、义务，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。通知信息参照 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，并不与数据取得的目的相悖。

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，参照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，应履行8.2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。

11.3.6 敏感数据

数据管理者合法拥有的商业数据等敏感数据，在向第三方提供时，数据提供合同中应包括：

a) 数据管理者与第三方的权利和责任；
b) 敏感数据的处理说明；
c) 敏感数据的清洗、脱敏说明；
d) 安全措施和承诺；
e) 敏感数据相关事故责任认定和报告；
f) 合同到期后敏感数据的处理方式；
g) 其它应说明的问题等。

11.4 委托

11.4.1 范围限定

委托第三方获取数据、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它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，并应将受托方相关信息提供给数据主体。提供的信息可参照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。

11.4.3 敏感数据

委托业务涉及敏感数据时，应遵循11.4.2，建立可信的委托信任机制。委托合同包括的信息，应参照11.4.2和11.3.6。

11.5 数据开发

分析、整合、整理、挖掘、加工等数据开发业务，应履行第8章、第7章规定的原则和责任、义务，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) 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 要求

数据交易应保证：

a) 应限定在法律许可的范围内；
b) 应明确数据权属；
c) 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；
d) 交易双方均应履行第 7 章、第 6 章规定的原则和责任、义务，保障数据主体权益。

11.6.2 信用交易

数据交易应基于明确、合法的目的，建立可信的交易信用机制，避免发生数据泄露或滥用，并依据11.6.1通知数据主体，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。

11.6.3 敏感数据

敏感数据交易应清洗、脱敏后实施，并参照11.3.6和11.6.2的通知内容，通知数据主体。

11.7 后处理

11.7.1 要求

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，应保证数据的准确性、完整性和时效性。

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、介质等及其记录的数据。

12 安全管理

12.1 要求

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） 融合个人信息安全管理体系，统一规划、设计、实施、构建数据管理体系；
c） 融合中考虑不同数据生态的安全特征和需要。

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、防盗及其它自然灾害、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) 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) 其它相关管理。

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（操作系统、数据库系统、中间件、虚拟系统及其它支撑系统运行的系统等）、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。

12.7 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、纸等介质及其它介质）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。

12.8 数据库安全

数据管理者应保证数据库存储数据及其它保存数据的准确性、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。

数据管理者应履行第5章的要求，根据数据自动和非自动处理的特点，建立数据库管理机制、策略、备份和恢复机制等，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。

12.9 移动设备安全

12.9.1 管理安全

应制定与数据相关的移动设备、媒介的管理制度，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 个人安全

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（或其它以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）：根据内审结果和其它相关信息，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

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。

13.2.2 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；
g) 其它必要的措施。

13.2.3 实施

应根据数据管理体系内审计划，定期独立、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

应建立服务台机制，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、分析取得、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。

15 例外

15.1 取得例外

15.1.1 商业数据

不应取得的商业数据，包括：

a) 数据主体认定的不应取得的商业数据；
b) 竞业禁止协议适用的商业数据；
c) 法律特别规定的。

15.1.2 数据隐私

数据主体认定的其它不宜取得的数据隐私。

15.1.3 例外

不应取得的数据，存在以下例外：

a) 法律特别规定的例外，但应采取特别的保护措施，履行第 6 章的要求，并在处理、使用之后征求数据主体的后处理意见；

b) 数据主体明确同意，但应限制在数据主体同意的处理、使用范围内，采取特别的保护措施，并在处理、使用之后征求数据主体的后处理意见。

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

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