ICS 35.020
L70

DB21

辽 宁 省 地 方 标 准

DB21/T 1628.2—2018
代替 DB21/T 1628.2-2013

信息安全 个人信息安全管理体系 第 2 部分：实施指南

Information security-Personal information security management system-Part2: Implementation guidelines

2018－01－22 发布　　2018－02－22 实施

辽宁省质量技术监督局　发布

目　　次

前　言

DB21/T 1628 分为 8 部分：

——信息安全 个人信息保护规范（信息安全 个人信息安全管理体系 第 1 部分：通用要求）

——信息安全 个人信息安全管理体系 第 2 部分：实施指南

——信息安全 个人信息安全管理体系 第 3 部分：个人信息数据库管理指南

——信息安全 个人信息安全管理体系 第 4 部分：个人信息管理文档管理指南

——信息安全 个人信息安全管理体系 第 5 部分：个人信息安全风险管理指南

——信息安全 个人信息安全管理体系 第 6 部分：安全技术实施指南

——信息安全 个人信息安全管理体系 第 7 部分：内审实施指南

——信息安全 个人信息安全管理体系 第 8 部分：过程管理指南等。

本部分是 DB21/T 1628 的第 2 部分。

本部分按照 GB/T 1.1—2009《标准化工作导则　第 1 部分：标准的结构与编写》给出的规则起草。

本部分代替 DB21/T 1628.2-2013《信息安全 个人信息安全管理体系实施指南》。与 DB21/T 1628.2-2013 相比，本部分除编辑性修改外，主要技术变化如下：

——根据 DB21/T 1628.1-2016 修改标准结构；

——标准粒度修订，适当增加细粒度；

——分解解析个人信息定义；

——分解解析个人信息主体定义；

——解读个人信息生命周期；

——分解解析个人信息管理者；

——按照个人信息生命周期修订生命周期各个阶段的约束细则，以为规范的补充；

——基于社会和技术进步，增加个人信息二次开发、交易的约束细则；

——适当跟踪新技术的发展，特别规范移动设备的管理规则。

本部分由大连市质量技术监督局提出。

本部分由辽宁省工业和信息化委员会归口。

本部分主要起草单位：大连软件行业协会、大连交通大学、大连市计算机学会。

本部分主要起草人：郎庆斌、孙鹏、尹宏、丁宗安、董晶、杨万清、杨莉、郭玉梅、曹剑、司丹、孙毅、王小庚。

DB21/T 1628.2-2013《信息安全 个人信息安全管理体系实施指南》于2013年8月首次发布。本次修订为第一次修订。

引　言

0.1　个人信息管理

个人信息是与特定个人相关并可识别特定个人的数据、图像、声音等信息，是自然人非常重要的人格要素之一，其属性特征与自然人的日常生活、社交、工作等密不可分。如果公开这些信息，与个人有关或无关的其他自然人，可以根据信息直接定位于特定的个人，并根据自己的需要加以利用，因此，需要采取适宜的技术、管理等手段妥善保护。随着互联网技术的发展和普及，滥用、泄漏、公开、非法传播个人信息的威胁日趋严重，这种保护尤显重要。

个人信息的存在是多样态的，可以以纸质、电子、磁介质、光介质、网络等多种媒介打印（书写）、存储、传播。无论以何种存在形式使用、处理、存储个人信息，均应采取相应的管理措施。

个人信息管理是基于特定、明确、合法目的，以有效、能动、可控、安全为目标、针对个人信息及相关资源、环境、管理体系等的相关活动或行为，是个人信息管理者向个人信息主体提供服务的过程，这个过程构成个人信息全生命周期，包括个人信息获取过程、个人信息处理过程、基于生命周期的过程管理等三个环节，通过计划、组织、协调个人信息资源需求与个人信息主体的符合性，采取相应的规范化、系列化控制策略和控制措施，保证个人信息的安全。

个人信息获取过程：基于特定、明确、合法目的，直接、间接收集个人信息（个人信息主体同意）；

个人信息处理过程：个人信息的加工、使用、处置过程；

基于生命周期的过程管理：在个人信息生命周期内，采用 PDCA 模式管理针对个人信息及相关资源、环境、管理体系等的活动或行为。

0.2　网络信息管理

网络信息管理是一般意义信息管理在网络空间中的延伸。网络空间是虚拟的，进入网络空间的个人，可以拥有自己的虚拟生活领域，自主确定个人数据的使用、处理和控制。然而，个人的网络行为和活动，包括个人网站、信息发布、电子商务、电子邮件等产生的个人信息，可以轻易地采用现代信息技术手段监控、收集、利用。

无论何种社会形态，无论何种个人信息存在形态，个人信息安全形态是相似的：

a）所拥有、管理的个人信息的生命周期是相同的；

b）个人信息管理职能，包括计划、组织、控制、协调等是相同的；

c）保障个人信息主体权益，约束个人信息管理者的责任和义务是相同的。

因而，实现个人信息安全的核心是服务管理。以管理为主线，考虑个人信息生命周期不同阶段个人信息的特征，强化生命周期内服务管理能力、服务管理质量，通过质量管控实现个人信息安全。

本指南确定的基于个人信息生命周期的个人信息管理规则，具有普适意义，既适用于不同社会形态的行业特征，亦适用于不同的个人信息存在形态（如网络信息管理）。

0.3　个人信息管理的必要性

随着社会经济的发展，个人信息的收集、处理、使用、利用，愈加方便、容易，对个人信息的侵害也愈加频繁，愈加呈现多样性。个人的身份证号码、信用卡号码、电话号码、手机号码等信息都可能成

为被利用的工具，特别是信息技术和网络系统的进步，更使得个人信息的收集和利用变得非常容易。

在许多公共机构、政府行政机构、提供公共服务的组织合法掌握着大量的个人信息，当人们在提供自身信息的同时，个人信息泄漏和被非法利用的危险同时存在。

个人信息随着社会发展和市场经济的建立，凸显人格利益的商业价值和经济利益。构成人格利益的人格要素的商品化、利益多元化，更凸显了在现代社会、经济活动中，个人信息的无形的物质性财产权益。因此，个人信息的安全应成为每个公民的自觉意识，尊重和保护公民的人格权益，是每个公民的职责。

0.4 个人信息安全管理体系

体系是具有特定功能、由相互关联的若干要素构成、可以实现预定目标的有机整体。要素与要素、要素与体系、体系与环境之间相互作用又相互依赖。

任何体系都是一个有机的整体，它不是各个要素的机械组合或简单叠加，各个要素的有机整合，构成体系整体性能。体系中的各个要素不是孤立存在，每个要素在体系中都发挥着特定的作用。要素之间相互关联，构成不可分割的整体。如果将要素从体系整体中割离出来，它将失去要素的作用。

体系应具有：

a）明确的目标；

b）清晰、严谨的法规、规范；

c）完善的组织机构；

d）完备的管理机制；

e）持续改进、完善的过程更新能力。

建立个人信息安全管理体系的基本目的是满足个人信息管理的需要，指导个人信息管理者建立健全各类管理机制，协调各类资源，充分保障个人信息主体的权利，保障个人信息管理业务的稳定运行。

0.5 个人信息管理的要求

个人信息管理者应确定个人信息管理的要求，应包括 4 个方面：

a）法律、规范的要求。个人信息管理应符合、满足与个人信息安全相关法规、规范的要求和社会、人文环境需要；

b）实施风险评估的结果。个人信息管理者应根据其管理的需要和业务发展、流程、目标等，实施个人信息安全风险评估，识别与个人信息安全相关资源的风险、发生的可能性，并评估影响；

c）个人信息安全管理体系。个人信息管理者为在其管理和业务运行中保证个人信息的安全，应构建个人信息安全管理体系，并遵循体系的要求；

d）个人信息安全管理体系内审。个人信息管理者为保证个人信息安全管理体系的安全运行，应建立个人信息安全管理体系内审机制，并根据内审结果改进、完善。

0.6 个人信息安全管理体系实施惯例

个人信息安全管理体系通用的实施惯例，应包括：

a）明确个人信息管理目标；

b）建立个人信息管理相关组织机构；

c）制定个人信息管理方针；

d）构建个人信息安全管理体系；

e）个人信息安全风险管理；

f）制定个人信息管理相关规章；
g）个人信息安全宣传、教育；
h）个人信息管理过程；
i）个人信息安全管理体系内审；
j）过程改进。

0.7 个人信息管理的关键因素

个人信息管理的关键因素应包括：
a）最高管理者的意识和支持；
b）个人信息相关法规、标准的理解；
c）个人信息管理相关组织机构的效能；
d）个人信息管理相关机构负责人的责任；
e）个人信息安全目标、安全策略和行为；
f）个人信息安全宣传、教育的效果；
g）个人信息安全风险管理的理解；
h）个人信息安全管理体系内审效能；
i）过程改进的有效性。

0.8 个人信息安全管理体系基准

本指南应作为构建、实施、运行个人信息安全管理体系的基准，其内容并不一定适应所有个人信息管理者，也可能需要本指南未涵盖的内容。个人信息管理者宜根据个人信息安全相关法规、规范，设置所需的控制策略和措施，并与本指南的条款相互引用，将适宜评价人员的符合性、一致性和有效性评估。

0.9 指南架构

本指南依据 DB21/T 1628.1《信息安全 个人信息保护规范》确立个人信息安全管理体系：
a）个人信息安全目标和基本原则；
b）个人信息管理相关机构及职责；
c）个人信息管理方针；
d）个人信息管理机制；
e）个人信息管理过程；
f）个人信息安全管理体系内审；
g）过程改进；
h）管理和业务的连续性管理。

本指南条款基本依据个人信息安全管理体系顺序排序，但并不表明体系各项重要程度排序。根据个人信息管理者的管理、业务、环境等的需要，各条款可能均是重要的。

实践表明，构建、实施个人信息安全管理体系宜遵循“个人信息安全管理体系实施惯例”（0.6）。

0.10 与其它标准体系的兼容性

DB21/T 1628.1《信息安全 个人信息保护规范》、DB21/T 1628.2《信息安全 个人信息安全管理体系实施指南》及个人信息安全标准体系其它标准可与其它国际、国内信息安全标准及相关标准协调一致，并与这些标准相互配合或相互整合实施和运行。

DB21/T 1628.1《信息安全 个人信息保护规范》、DB21/T 1628.2《信息安全 个人信息安全管理体系实施指南》易于使个人信息安全管理体系与其它管理体系整合实施。

信息安全　个人信息安全管理体系 第2部分：实施指南

1　范围

本标准为个人信息管理者构建、实施、运行、内审、改进个人信息安全管理体系提供指导和通用准则。

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，仅所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。

DB21/T1628.1 信息安全 个人信息保护规范

DB21/T 1628.3 信息安全 个人信息安全管理体系 第3部分：个人信息数据库管理指南

DB21/T 1628.4 信息安全 个人信息安全管理体系 第4部分：个人信息管理文档管理指南

DB21/T 1628.5 信息安全 个人信息安全管理体系 第5部分：个人信息安全风险管理指南

DB21/T 1628.6 信息安全 个人信息安全管理体系 第6部分：安全技术实施指南

DB21/T 1628.7 信息安全 个人信息安全管理体系 第7部分：内审实施指南

DB21/T 1628.8 信息安全 个人信息安全管理体系 第8部分：过程管理指南

3　术语和定义

DB21/T 1628.1界定的以及下列术语和定义适用于本文件。

3.1

指南 guide

构建个人信息安全管理体系应做什么和如何做。

3.2

个人信息管理方针 policy of personal information management

个人信息管理者正式公布的个人信息管理策略、原则和措施。

3.3

个人信息管理机制 management mechanism of personal information

通过个人信息安全管理体系实施个人信息管理的机构、功能及相互关系。

注1：管理机制应包括组织机构、职责、规章、活动、资源等。

3.4

个人信息安全管理 personal information security management

通过个人信息安全管理体系实施个人信息管理采取的安全策略、安全技术和安全管理措施。

3.5

个人信息安全风险 personal information security risk

个人信息安全事故发生的可能性、后果和可能的影响。

3.6

过程管理 process management

采用PDCA模式管理个人信息的相关活动、相关资源及其相互关系。

3.7

个人信息安全事件 personal information security incident

违反个人信息管理方针或由于个人信息安全管理体系不健全引发的活动、状态。

3.8

个人信息安全事故 personal information security accident

威胁个人信息安全，损害个人信息主体权益，并可能造成一定影响的单个或一系列个人信息安全事件。

4 要求

本指南遵循 DB21/T 1628.1 确立的个人信息管理的基本原则和要求，重点描述和指导 PISMS 的构建、实施、运行。

构建、实施和运行 PISMS，应同时使用 DB21/T 1628.1 和本指南。

构建、实施和运行PISMS，亦应同时融合、使用个人信息安全标准体系其它标准。

5 过程方法

5.1 PDCA 模式

附录 A 描述了 PISMS 依据个人信息管理的要求和期望，应展开的过程管理活动。

5.2 描述

PISMS 的构建、实施、运行、监控、内审和改进，应采用附录 A 所示 PDCA 模式：

a）计划（构建 PISMS）：根据个人信息管理者的整体目标，确立个人信息管理目标和方针，实施个人信息管理计划，构建 PISMS；

b）实施（实施和运行 PISMS）：实施和运行 PISMS；

c）检查（监控和内审 PISMS）：监督、检查、控制 PISMS 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 PISMS）：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 PISMS 的持续改进。

注2：过程管理方法，参看 DB21/T 1628.8。

6 个人信息

6.1 分类

个人信息的类别可分为：

a）单一和组合信息：个人信息是由单一数据元素，如姓名，或多个数据元素构成；

b）显性和隐性信息：易于识别的个人信息，如明显的身体特征和需要借助某些技术手段获取的个人信息，如血型、基因等；

c）静态和动态信息：已经存在或过往、历史的个人信息，如教育经历和当前正在发生的个人信息，如社会活动、收入支出等；

d）真实和虚拟信息：存在于现实世界中的真实的个人信息和存在于虚拟世界的虚拟信息。

注3：不同的个人信息存在形态可包括不同类别的个人信息。

6.2 存在形态

个人信息的存在形态应包括：

a）完整的个人信息：由多个可识别的数据元素构成的组合信息，可以描绘出完整的个人信息主体的自然人形态；

b）部分完整的个人信息：由多个可识别的单一数据元素构成的信息，可以描绘出个人信息主体的自然人基本形态；

c）琐碎的个人信息：离散的、毫无关联或可能存在部分关联的个人信息，经精心收集、整理，可能拼接、组合成相对完整的个人信息，形成个人信息主体的基本形态。但这种形态可能接近真实，也可能是扭曲的；

d）敏感的个人信息：个人信息主体具有的特殊的个人隐私信息，如身体障碍、精神障碍、犯罪史、健康、医疗、性生活等，可以描绘个人信息主体的个人隐私形态。

6.3 记录形式

记录个人信息形态的基本形式，主要应包括：

a）文字：以文字形式描述个人信息的基本形态，可以纸媒介书写、保存，也可通过自动处理形成数据；

b）数据：以数字、字符、符号等形式描述个人信息，可以自动或非自动处理方式保存、传递、处理；

c）声音：以声音形式感受、理解、描述个人信息，应辅以相应的录制工具；

d）图像：以图像形式感知、意识、描述个人信息；

注4：记录个人信息形态的基本形式可以互相转化，并可通过自动处理数字化。

6.4 识别形式

6.4.1 识别

个人信息主体的识别，应包括：

a）直接识别：根据个人信息反映的客观事实可以直接明确与个人信息主体之间的关系；

b）间接识别：某些单一数据元素构成的部分完整的个人信息，不能直接明确与个人信息主体之间的关系，需要借助各种手段对照、参考、判断、分析确定。

6.4.2 形式

个人信息主体的识别形式应包括：

a）可通过各种感官形式直接识别：

1）听觉：通过听觉器官感受与个人信息相关的声音信息，识别个人信息主体；

2）视觉：通过视觉系统观测与个人信息相关的图像信息，识别个人信息主体；

3）触觉：通过触觉系统接触、触摸、抚摸等辨别、感受与个人信息相关的敏感信息，识别个人信息主体；

4）其它形式：可通过除1）、2）、3）之外的其它形式感知个人信息，识别个人信息主体；

b）可借助各种手段，对照、参考、分析与个人信息主体相关的信息：

1）部分个人信息不能直接识别个人信息主体，可与个人相关的其他信息对照、参考、分析；

2）部分个人信息不能直接识别个人信息主体，可借助合法、适当的科学技术手段参考、判断、分析。

注5：不应拼接琐碎的个人信息间接识别个人信息主体。

7 个人信息主体

7.1 个人

个人是自然人个体的基本特征，应包括：

a）基于自然规律出生，具有生物学意义和法理人格；

b）法律赋予民事主体资格，具有民事权利能力。

7.2 主体

7.2.1 特征

个人信息主体的特征应包括：

a）法律赋予的民事主体资格，享有民事权利并承担民事义务；

b）具有独立的人格，享有自然人应有的人格权。

注6：人格权是包括生命健康、人格尊严、人身自由、个人隐私等等维护人格主体的独立的人格利益所必备的各种权利。

7.2.2 义务

人格权义务应包括：

a）国家有保护自然人个体的人格权的义务；

b）个人维护自身人格权的同时，应接受法律允许的监督、审查，自觉遵守法律、制度；

c）个人应尊重、保护他人的人格权。

7.2.3 唯一性

基于人格权的人身依附性，个人信息主体的人格权具有唯一性，不能转让、继承。

7.3 人格利益

7.3.1 构成

人格利益的构成应包括：

a）物质性人格要素：由个人信息主体的生物遗传特征构成，如面部、身体、指纹、手纹、虹膜、血型、语音、DNA、性别……；

b）精神性人格要素：是个人信息主体在社会实践中形成的，如姓名、健康、名誉、荣誉、肖像、住宅、职业、教育、精神、社会活动、隐私、自由，及个人使用的号码、标志和其它符号（身份证号码、社会保险号码、银行卡等）……。

7.3.2 权益

人格利益的属性包括：

a）人格利益应是基于人格权形成的个人的人格权益；

b）人格要素具有财产权益，可在社会活动中展现价值特征。

7.3.3 唯一性

人格利益具有惟一性：

a）基于人格权的唯一性，人格利益应由个人信息主体唯一拥有；

b）人格要素的商业化、非商业化使用，不应发生个人信息主体权利转让；

c）在个人信息主体授权许可范围内，可发生人格要素的使用权转让。

注7：虚拟空间中存在的人格利益亦应具有唯一性。

7.4 权利

7.4.1 描述

DB21/T 1628.1第5章确立了个人信息主体应享有的权利：

a）个人信息主体应主张并享有DB21/T 1628.1第5章确立的知情、支配、质疑等个人信息权利；

b）个人信息主体可按照自己的意愿自由行使权利，以在法律允许范围内保障、实现自身权益。

7.4.2 时效

个人信息主体主张、行使权利的时效，应包括：

a）个人信息全生命周期内；

b）形成新的个人信息生命周期。

7.4.3 追溯

个人信息生命周期完结后，如发现个人信息侵权行为未予追究，个人信息主体可主张、行使权利。

8 个人信息生命周期

8.1 描述

个人信息生命周期应是个人信息管理者向个人信息主体提供服务管理的过程，即自个人信息直接收集开始到个人信息彻底销毁的服务管理过程。

8.2 服务能力

在个人信息全生命周期内，个人信息管理者应具有内部各类个人信息管理所需相关资源的转换能力和管理职能的组织能力，以保证个人信息管理的有效性。

8.3 服务质量

在个人信息全生命周期内，保证服务管理质量应包括：

a）形成有效的管理机制，包括个人信息管理相关的环境、人员、设备、技术、信息等资源的管理；

b）建立有效的服务管理体系PISMS。

8.4 服务过程

8.4.1 获取过程

8.4.1.1 约束

在个人信息获取过程中，应保证：

a）特定、明确、合法的目的；

b）个人信息主体明确同意；

c）个人信息质量；

d）收集公开的个人信息，亦应设定明确的目的。

8.4.1.2 形式

个人信息获取过程可包括3种形式：

a）基于特定、明确、合法的目的，经个人信息主体明确同意，直接收集个人信息；

b）新的个人信息生命周期内的间接收集或直接收集；

c）被动收集个人信息是一种收集的特例。

注8：新的个人信息生命周期是在个人信息生命周期过程中形成的。

8.4.2 处理过程

8.4.2.1 约束

在个人信息处理过程中，应保证：

a）明确收集目的；

b）个人信息质量；

c）安全保障。

8.4.2.2 形式

个人信息处理形式，可包括：

a）使用：基于收集目的的个人信息处理，包括编辑、加工、检索、存储、传输等不同的流程；

b）利用：因某种利益使用个人信息的处理行为，如提供、委托、交换等过程；

c）利用：以某种利益形式挖掘或有偿转让个人信息的行为，如二次开发、交易等过程；

d）后处理：个人信息处理后应采取的相应的安全处理过程。

8.4.3 过程管理

8.4.3.1 约束

基于个人信息生命周期的过程管理，应保证：

a）个人信息全生命周期的过程管理；

b）个人信息及相关资源、环境、管理体系等活动或行为的管理；

c）个人信息管理过程与个人信息管理者内部管理融合。

8.4.3.2 过程方法

应遵循第5章建立的过程管理模式，运用各种管理机制、管理策略，持续改进、完善个人信息管理过程。

9 个人信息管理者

9.1 主体

9.1.1 特征

个人信息管理者是个人信息管理的主体，其特征应包括：

a）合法、有效、独立的机关、企业、事业、社会团体等组织；

b）个人；

c）具有民事权利和民事能力，享有民事义务，承担民事责任；

d）具有公共管理职能。

9.1.2 责任和义务

9.1.2.1 责任

遵循DB21/T 1628.1 6.4的约束规则，个人信息管理者应承担个人信息管理的相应责任包括：

a）社会责任：个人信息主体明确同意并授权个人信息管理者管理个人信息，个人信息管理者应承担和履行的职责；

b）法律责任：个人信息主体明确同意并授权个人信息管理者管理个人信息，个人信息管理者应承担和履行的法律责任，包括民事责任、行政责任、刑事责任、赔偿责任等。

9.1.2.2 义务

遵循DB21/T 1628.1 6.4的约束规则，个人信息管理者应承担个人信息管理的相应义务，应包括：

a）社会义务：个人信息管理者为承担和履行社会责任，保障个人信息主体权益实施的行为和活动；

b）法律义务：个人信息管理者为承担和履行法律责任，保障个人信息主体权益，应遵循的相关法规、标准。

9.2 角色

9.2.1 行为模式

DB21/T 1628.1 6.2的角色细分，应是根据不同的行为模式划分的：

a）9.1.1限定个人信息管理者为合法、有效的个人信息管理组织或个人；

b）个人信息管理者的细分角色，根据目的、动机、方法等的不同存在行为差异；

c）个人信息管理者细分角色的行为差异，存在合法和非法的可能性；

d）个人信息管理者的细分角色可在条件、利益满足时转化。

9.2.2 约束

个人信息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DB21/T 1628.1第6章确立的规则、责任和义务。

10 个人信息管理

10.1 概述

10.1.1 要求

个人信息管理者在个人信息管理中，应依据DB21/T 1628.1第7章确立个人信息管理的目标，同时：

a）个人信息管理者应具有第7章规定的服务能力和服务质量管理能力；

b）个人信息管理者应依据DB21/T 1628系列标准的规定，采取相应的管理、技术措施，管理个人信息。

10.1.2 原则

DB21/T 1628.1第7章确立了个人信息管理者应遵循的个人信息管理的基本原则，个人信息管理者应依据实际明确原则实施的细节，以延展、扩大个人信息主体权益的覆盖面。

10.2 方针

10.2.1 要求

实施个人信息管理方针，应保证：

a）依据 DB21/T 1628.1 7.3，确立与管理、业务需求一致，符合个人信息安全相关法规、规范，为个人信息安全管理体系实施、运行提供指导和支持的原则和措施；

b）个人信息管理者在构建 PISMS 时，应首先制定清晰、简洁、明确的个人信息管理方针，并在其内、外部公开发布，阐明个人信息管理措施和承诺。

10.2.2 内容

个人信息管理方针应由最高管理者批准。其内容宜包括：

a）个人信息安全的目标及重要性；

b）个人信息主体的权利；

c）个人信息管理者的责任和义务；

d）个人信息安全相关法规、规范的要求；

e）个人信息管理采取的保护措施和方法；

f）违反个人信息管理方针的处理；

g）个人信息安全建议、意见的处理和反馈（应有相应的责任主体、联系方式等说明）；

h）改进和完善 PISMS 的措施等。

10.2.3 改进

个人信息管理方针应适时改进：

a）个人信息管理方针应随时间的变化或管理、业务、环境等发生重大变化时适时改进，以保证方针的适宜性和有效性；

b）个人信息管理者代表应适时评估方针的适宜性和有效性，并根据时间、环境、管理、业务、技术、法律等的变化适时改进。

10.3 管理边界

个人信息管理者依据 DB21/T 1628.1 6.4 履行个人信息管理责任，应限定管理边界：

a）层级和权责：个人信息管理者内部管理、业务层次和权限、责任；

b）部门间：个人信息管理者内部各部门之间的关联、影响；

c）外部：个人信息管理者与客户、社会组织之间的关联和影响；

d）个人：个人信息管理者的员工行为和责任。

10.4 计划

依据 DB21/T 1628.1 7.4，应制定个人信息管理计划：

a）明确个人信息管理者的管理、业务目标；

b）确定个人信息管理形式、方法、策略及资源需要等；

c）收集个人信息前的准备，包括来源、目的、方式、方法、安全措施等；

d）识别与个人信息管理相关的资源，包括信息系统、行政管理、业务流程、工作环境、外部环境等相关资源；

e）评估个人信息安全风险的方法和措施；

f）评估管理状况和效果，包括管理目标、管理边界、管理方式、资源配置、体系建设和运行等及管理缺陷的处理方式；

g）评估计划的实施情况，包括计划执行过程中，随时检查、分析计划执行情况和计划执行完毕检查、总结、分析计划执行情况。

注9：个人信息管理计划应由个人信息管理者组织制定。

10.5 组织

10.5.1 相关机构及职责

10.5.1.1 要求

依据 DB21/T 1628.1，个人信息管理者应根据管理计划，建立个人信息管理机构：

a）DB21/T 1628.1 7.5 确立的个人信息管理相关机构是个人信息安全的组织保障，应首先在最高管理者授意下组建；

b）依据个人信息管理计划组建个人信息管理相关机构，应是构建 PISMS 的首要任务；

c）个人信息管理相关机构应在个人信息生命周期全过程实施符合相关法规、标准的管理，组织个人信息管理活动或行为。

10.5.1.2 最高管理者

应是个人信息管理者构建 PISMS、实施并持续完善、改进个人信息管理的决策者。依据 DB21/T 1628.1 7.5.2.1，其责任应包括：

a）确立个人信息安全、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、有利于实施个人信息管理的内部环境；

c）组建个人信息管理机构，选择有能力的管理者代表，并赋予相应权限，确保 PISMS 的实施和运行；

d）为实施、运行 PISMS 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 PISMS 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）对 PISMS 实施、运行制定合理、适宜的激励机制；

g）对 PISMS 的持续改进提供决策支持；

h）组建 PISMS 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 PISMS

的实施和运行；

i）批准个人信息管理相关责任主体的职责分配、个人信息管理方针、个人信息管理规章、个人信息安全宣传教育计划等管理机制，并协调、组织实施 PISMS。

10.5.1.3 管理机构

10.5.1.3.1 个人信息管理者代表

应是最高管理者指定的个人信息管理机构责任主体，依据 DB21/T 1628.1 7.5.2.2，其职责应包括：

a）代表最高管理者提出并制定个人信息管理计划；

b）代表最高管理者负责个人信息管理机构的组建和日常工作；

c）制定个人信息管理方针；

d）负责 PISMS 构建、实施和运行；

e）确定组织、构建和实施 PISMS 的资源需要和资源分配；

f）组织制定、实施个人信息管理的基本规章制度，推进个人信息管理工作的开展；

g）部署个人信息安全宣传，指导个人信息安全的培训和教育；

h）监督个人信息安全管理机制的构建和实施；

i）监督、指导 PISMS 各项文档的管理；

j）PISMS 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。

10.5.1.3.2 机构职责

应根据DB21/T 1628.1 7.5.2.2的规定，按照个人信息管理者的实际，将个人信息管理机构职责分解为具体、可操作的活动，并落实到相关责任主体。

10.5.1.3.3 责任主体

依据DB21/T 1628.1 7.5.2.2，个人信息管理机构宜包括：

a）宣传教育：宜指定责任主体，在个人信息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 PISMS 宣传、教育；

2）制定 PISMS 宣传、教育制度、计划；

3）制定 PISMS 宣传策略和方法；

4）个人信息相关知识、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，在个人信息管理者代表指导下开展个人信息安全管理工作。其主要职责应包括：

1）个人信息安全风险管理；

2）制定个人信息安全管理策略、措施；

3）实施个人信息安全管理措施；

4）改进、完善个人信息安全管理；

c）服务台：宜指定责任主体，在个人信息管理者代表领导下提供个人信息相关的服务。其主要职责应包括：

1）提供个人信息管理、安全的相关咨询和服务；

2）提供个人信息处理、使用建议和意见；

3）接受有关个人信息管理、安全的意见，并落实和反馈；

4）沟通、交流；

5）个人信息管理、安全相关事项、问题处理等的发布；

6）其它应处理的问题；

d）个人信息管理责任主体，宜包括个人信息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。

10.5.1.3.4 协调

根据 DB21/T 1628.1 7.5.2.2 确立个人信息管理机构的责任主体职责，应注意：

a）宣传教育应注意协调部门、人员、管理、业务、资源及外部因素等；

b）个人信息安全管理应注意协调整体信息安全与个人信息安全的关联；

c）各责任主体具体责任人的职责，宜根据个人信息管理者需要确定。

10.5.1.3.5 职责分配

应明确、清晰地定义、分配所有个人信息管理相关责任主体的职责：

a）职责定义、分配应与个人信息管理目标、方针一致；

b）职责分配应形成相应职责说明的文件；

c）职责分配应明确定义授权形式，并形成相应文件；

d）已分配职责的人员，如将相关任务委托其他人员，仍应负有责任，并应确认被委托任务是否正确完成、涉及的个人信息是否完整、准确；

e）职责应随管理、业务的变化、内审意见等适时补充、改进和完善。

10.5.1.4 内审机构

依据 DB21/T 1628.1 7.5.2.3，PISMS 内审机构的主要职责应包括：

a）明确 PISMS 内审的目的，编制内审制度和内审计划；

b）明确内审代表的职责；

c）跟踪、评估 PISMS 构建、实施过程的合理性、充分性和完整性；

d）评价管理人员、工作人员的意识、行为、活动；

e）评估 PISMS 运行的效率和效果；

f）及时发现缺陷，提出适宜的改进、完善建议。

注10：内审代表的职责，宜根据个人信息管理者和其内部各部门的需要确定。

10.5.2 构建和管理 PISMS

依据 DB21/T 1628.1 7.5.3，个人信息管理者代表应组织构建 PISMS，以满足个人信息管理的需要：

a）建立个人信息管理相关机构，明确机构职责和机构责任主体的责任；

b）明确个人信息管理目标，确立个人信息管理的基本原则；

c）制定个人信息管理方针，阐明个人信息管理的指导原则；

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 PISMS 范围；

e）实施风险管理，识别风险源和安全隐患，确定 PISMS 的控制目标和控制方式（参见 DB21/T1628.5）；

f）建立个人信息管理机制：

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

2）个人信息管理策略、管理模式，包括个人信息存储、保存、处理、使用、利用等；

3）制定个人信息安全宣传策略，在内、外部宣传个人信息安全的重要性和所采取的管理策略；

4）制定个人信息安全培训教育计划，对全体员工实施个人信息安全相关知识的教育，并跟踪培训教育的效果；

5）其它个人信息相关管理事务等；

g）管理过程。在个人信息管理过程中，采用相应的管理、技术手段，保证与目的的一致性、符合性，保证个人信息的安全和个人信息主体的权益；

h）个人信息安全管理（参见 DB21/T 1628.6）；

i）基于个人信息生命周期的过程管理（参见 DB21/T 1628.7、DB21/T 1628.8）：

1）建立 PISMS 内审机制。检查、评估 PISMS 实施和运行过程，持续改进和完善体系；

2）跟踪、监控PISMS实施、运行，随时改进、完善；

k）应急管理。建立应急预案，对可能发生的个人信息安全事件或个人信息安全事故，及时采取相应的应对措施等。

10.5.3 协调

个人信息管理者内部行政、财务、人力资源、业务等各不同部门宜有负责个人信息安全的代表。PISMS 实施和运行，应在这些代表间协调和合作。协调活动应保证：

a）各个部门个人信息管理的目的同一性、实施有效性；

b）与个人信息管理方针的一致性；

c）风险管理过程和方法的准确性、有效性及风险评估的充分性；

d）个人信息管理规章的充分性和有效性；

e）个人信息安全宣传教育的针对性、完全性、有效性；

f）个人信息管理的有效性；

g）PISMS 的充分性、有效性；

h）PISMS 内审的协调性、充分性和有效性等。

10.5.4 相关团体的联系

个人信息管理机构应与个人信息安全相关专家、团体，如行业协会等，保持联系：

a）获得关于个人信息安全的最新进展、最佳实践和更新知识；

b）PISMS 实施和运行过程中的疑问、意见、建议等的沟通；

c）相关团体关于个人信息安全、PISMS 认证的意见、修正、改进等；

d）个人信息安全事故的报告、处理等。

11 资源管理

11.1 相关资源

根据 DB21/T 1628.1 7.1，应识别与管理、业务涉及个人信息部分关联的各种资源，主要应包括：

a）信息资产：个人信息数据库及相应文件、合同和协议；个人信息管理文档等个人信息管理者运营、服务涉及个人信息的数据、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：个人信息管理相关的各种技术及支撑手段；

g）人力资源：PISMS 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、具有潜在利益的个人信息资源；

i）服务：资源管理、数据通信等个人信息管理者所提供的各种服务等。

11.2 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 PISMS 实施、运行中资源的敏感、关键程度；

b）在涉及个人信息的管理、业务中所关联资源的重要性；

c）涉及资源的个人信息的价值；

d）资源的安全等级等。

11.3 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个人信息相关资源的使用规定，如：

a）互联网使用规定；

b）电子邮件使用规定；

c）移动设备使用规定；

e）系统软件更新、病毒防范；

f）个人信息数据库管理；

g）文档管理；

h）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。

12 管理机制

12.1 管理制度

12.1.1 基本规章

基本规章是实施 PISMS 应遵循的行为准则，依据 DB21/T 1628.1 8.1.1，基本规章内容主要宜包括：

a）个人信息管理相关机构职能及职责：

1）机构建立的组织程序、管理层级、机构及各责任主体名称；

2）各机构、各责任主体责任人任命程序；

3）各机构、各责任主体的职能和权限；

4）各机构、各责任主体责任人的职责；

5）最高管理者的责任等；

b）个人信息管理：

1）个人信息主体的权利；

2）个人信息管理者的责任和义务；

3）应遵循的个人信息安全基本原则；

4）个人信息管理计划制定；
5）个人信息存储、保存规定；
6）个人信息收集、处理、使用、利用规则；
7）个人信息主体同意的方式和措施；
8）个人信息公示的规定；
9）特殊情况的处理；
10）记录和统计的规定等；

注11：如果个人信息管理者存在个人信息二次开发、交易等行为，应特别注意在基本规章中加以约束和限制。

c）个人信息安全风险管理：
1）目的、范围；
2）风险管理的方法和流程；
3）风险源确认方法；
4）风险分析和分类的方法；
5）风险程度和影响的评估方法和策略；
6）风险应对措施；
7）风险监控、跟踪措施；
8）风险重评估的依据、方法和策略等；

d）个人信息安全管理措施：
1）与整体信息安全的关系；
2）范围；
3）管理层安全管理措施；
4）业务层安全管理措施；
5）资产安全管理措施（包括相关的信息系统、软件应用、访问控制、权限管理、移动设备、介质等等）；
6）员工工作环境安全管理措施（包括出入管理、防灾管理、桌面管理等）；
7）员工行为管理措施；
8）特殊岗位安全管理；
9）其它必要的安全管理措施等；

e）个人信息数据库管理：
1）合法、合理、有效保存/存储措施；
2）时效规定；
3）管理和使用；
4）责任者的职责；
5）使用权限和安全管理；
6）备案登记；
7）备份和恢复；
8）维护和记录；
9）使用后的处理措施；
10）事故处理；
11）其它必要的安全管理措施等；

f）个人信息管理相关文档管理：
1）管理实施记录；
2）文档范围和分类；

3）文档编码规则和修订规则；
4）备案管理和使用；
5）备份和销毁等；
g）个人信息安全宣传教育管理：
1）培训教育目的、范围、对象说明；
2）培训教育计划制定和实施；
3）培训教育执行方式；
4）培训教育大纲、内容；
5）效果确认和跟踪（出勤、考试等）；
6）培训教育记录；
7）宣传范围、对象；
8）宣传方式；
9）宣传内容；
10）效果评估等；
h）PISMS 内审管理：
1）目的、作用、范围；
2）计划制定和实施；
3）内部审查内容（体系运行状况、各机构职责履行情况、责任人职责等）和措施；
4）实施方法；
5）内审处理措施；
6）内审记录和报告的编制规则；
7）其它必要的管理措施等；
i）服务台管理：
1）目的、作用、职责；
2）范围；
3）服务提供守则；
4）处理流程；
5）落实、反馈措施；
6）事故处理流程和措施；
7）记录管理；
8）其它管理措施等；
j）应急管理：
1）应急处理流程；
2）事故评估程序；
3）事故处理措施；
4）事故报告；
5）责任认定等；
k）过程改进管理：
1）评估方式、方法；
2）体系需改进、完善事项的确定；
3）改进流程；
4）改进和预防措施；
5）改进后的跟踪措施等；

l）违反个人信息管理相关规章的处理：

1）处理对象的责任认定（员工、机构、负责人等）；

2）处理依据和原则；

3）处理的决策过程；

4）处理的相关决定和措施；

5）公示等。

12.1.2 管理细则

个人信息管理者涉及个人信息的各从属机构、部门，应依据基本规章，根据管理、业务的实际需要，制定相应的管理细则。

注12：涉及个人信息的机构、部门，宜包括人力资源、财务、行政主管、相关业务部门等。

12.1.3 其它管理规定

有特殊业务要求的部门或在业务开展中有特殊要求，涉及个人信息收集、处理，应制定相应的个人信息管理规定。

注13：个人信息管理者应根据自身的特点、实际需要制定适宜的规章，但应涵盖与个人信息相关的环境、管理、业务、人员等所有因素。本标准仅提供一般性意见。

注14：制定规章的标准格式，参看 DB21/T 1628.4。

12.2 人员管理

12.2.1 人员类别

根据 DB21/T 1628.1 8.2，个人信息管理者的人员类别，应包括：

a）最高管理者和各级管理者；

b）个人信息管理者代表和 PISMS 各责任主体责任人；

c）全体工作人员；

d）其他人员。

12.2.2 职责管理

应根据 DB21/T 1628.1 8.2，明确权限和职责，应包括：

a）个人信息管理者代表和 PISMS 各责任主体责任人，应有清晰的个人信息安全意识，明确管理权限和管理职责，在 PISMS 实施、运行过程中推进个人信息管理；

b）最高管理者和各级管理者，应接受个人信息管理者代表的指导和监督，明确个人信息安全的意义，在管理、业务活动中推进个人信息管理；

c）全体工作人员和其他人员，应有个人信息主体权益意识，明确岗位职责和个人信息安全责任，避免在工作中发生个人信息安全事件。

12.3 宣传教育

12.3.1 要求

个人信息安全的宣传教育是实现个人信息管理者发展战略的重要手段，应依据 DB21/T 1628.1 8.3，制定相应的宣传教育策略、措施和方法。

12.3.2 策略

a）应基于个人信息安全的目标、重要性，在内部开展有针对性的基本宣传和培训教育，主要应包括：

1）个人信息安全的基本知识；

2）个人信息安全的重要性和必要性；

3）个人信息安全相关法规、规范及规章制度；

4）个人信息主体的权益；

5）个人信息管理者的责任和义务；

6）管理、业务与个人信息安全的关系；

7）个人信息管理的措施、方法；

8）违反个人信息安全相关法规、规范、规章的处理等；

b）基于业务开展的需要，应在涉及个人信息的业务交往中，主动宣传个人信息管理的目的、措施、方法和规定，并做出保密承诺（如招聘网站、保险、银行、业务客户等）；

c）应面向社会公开宣传实施个人信息管理的目的、措施、与个人信息管理者发展战略的关系、个人信息安全的必要性等，营造个人信息安全的环境。

12.3.3 措施和方法

个人信息安全宣传教育的措施和方法，主要应包括：

a）基本宣传和培训教育：

1）依据人员、机构、业务和需求等实际情况，制定宣传策略和培训教育制度、计划；

2）开展全员宣传和教育，包括正式员工、临时员工和相关人员；

3）培训教育的顺序应是：

•个人信息管理者的各级负责人；

•个人信息管理机构及相应责任主体、内审机构的各负责人；

•全体员工；

b）宣传形式：

应利用形象宣传、广告宣传、业务交流、展览展示、网络媒介等各种宣传形式，宣传实施个人信息管理的意识和决心；

c）培训教育计划：

1）一年至少实施一次全员培训教育；

2）较大型个人信息管理者宜根据实际采取分批实施、网上实施等多种形式；

3）新员工、新业务或业务变化时，应及时培训教育；

d）记录每次培训教育情况：

1）记录内容应包括：时间、内容、教师、对象、部门、人数、负责部门等；

2）培训人员应有登记和签名；

3）应有考试记录；

e）培训教育报告：

应根据培训教育结果形成报告，上报个人信息管理者代表，并不断改进和完善培训教育计划。

12.3.4 效果

应适时评估培训教育的效果，使全体员工认识到个人信息安全的重要性和必要性：

a）个人信息管理者的各级负责人的个人信息安全意识；

b）个人信息管理机构、内审机构责任人的个人信息安全意识；

c）全体员工的意识、行为和培训教育的有效性；

d）不合格人员的补充培训。

注15：个人信息管理者结合信息安全、新员工上岗等培训教育展开个人信息安全培训时，应有重点、有目的，结合实际需要，避免边缘化。

12.4 公示

个人信息公开、公示，应做到：

a）必须公开、公示个人信息，应依据 DB21/T 1628.1 8.6，以适当方式通知个人信息主体并获得个人信息主体明确同意；

b）如个人信息主体对公示内容提出疑义，或要求修改、删除、更新，个人信息管理者应采取必要的措施维护个人信息主体的权益；

c）如个人信息主体不同意公开或公示，个人信息管理者不应以任何形式、任何方式公开、公示。

12.5 个人信息数据库管理

12.5.1 介质

根据 DB21/T 1628.1 3.1.10，个人信息数据库是个人信息管理者在个人信息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、个人数码助理等）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、即时通讯、网站、网络视频等；

g）声音媒介：录音、录像等。

12.5.2 管理限制

根据 DB21/T 1628.1 8.4，个人信息数据库管理应满足条件：

a）各种媒介记载、存储个人信息，应简明、清晰、可识别，易于提取、拷贝；

b）各种媒介记载、存储个人信息，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、存储个人信息，应保证准确性、完整性、可用性，并在个人信息发生变化时，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，并保证个人信息数据库的保密性、安全性；

e）政府、公共服务机构等管理的特定的个人信息数据库，采用磁介质、光介质、纸介质、声音等形式存储，应在法律规定的范围内检索。

12.5.3 备案管理

应根据 DB21/T 1628.1 8.4.4，建立备案登记制度，明确责任人的职责，确定相应的管理措施。

12.5.4 个人管理

12.5.4.1 移动个人信息数据库

根据DB21/T 1628.1 8.4.5，个人信息主体保有的可移动设备、媒介等构成的移动的个人信息数据库，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存储；

b）个人信息主体随身携带的芯片卡、纸质文档等形成的个人信息储存。

12.5.4.2 安全防范

个人信息主体应在各种公共空间、网络空间、通信等等场合，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，避免个人信息泄漏。

注16：个人信息数据库管理，参见 DB21/T 1628.3。

12.6 文档管理

根据 DB21/T 1628.1 8.5.1，个人信息管理过程中，应记录与个人信息相关所有活动或行为的信息。这些记录主要应包括：

a）管理机构建立的相关文档；

b）规章、制度、法规、标准及相关文件；

c）宣传、培训教育计划、记录；

d）风险管理记录；

e）安全管理记录；

f）内审计划、记录；

g）业务活动记录和统计；

h）管理活动记录和统计；

i）公示信息记录；

j）服务台相关信息记录；

k）体系检查记录；

l）违章处理记录；

m）其它相关文件等。

并应根据 DB21/T 1628.1 8.5.2 建立备案管理制度。

注17：个人信息管理相关文档管理，参见 DB21/T 1628.4。

13 获取过程

13.1 概述

13.1.1 要求

根据 DB21/T 1628.1 第 9 章，个人信息管理者在个人信息获取过程中，应依据个人信息安全相关法规、规范、已确立的个人信息管理方针，保证个人信息安全和个人信息主体权益。

13.1.2 获取

个人信息获取过程应是个人信息收集类别、方式、方法、手段、过程、质量、效果等的管理过程。

13.2 收集类别

13.2.1 直接收集

应基于特定、明确、合法的目的，直接向个人信息主体收集个人信息，包括：

a）主动式收集：个人信息主体基于工作、生活需要主动提供，如人事信息、医疗信息、个人账户信息、购物（房、车等）、银行业务、电子商务……；

b）被动式收集：个人信息主体在不知情或不能控制情况下被收集，如网络钓鱼、木马、购物陷阱、电话诈骗……。包括：

- 采用各种IT技术和方法；
- 社会交往、商业经济等活动；
- 采用欺骗、诱惑等手段窃取；

c）过度收集：是被动收集的特例，个人信息主体在工作、生活中存在的主、被动收集情况，如购房、购物、电信、银行、网络……。

注18：采用各种技术、方法被动收集个人信息，可形成扭曲、不完整的质量缺陷，侵害个人信息主体权益。

13.2.2 间接收集

间接收集个人信息，应基于特定、明确、合法的目的，通过各种适当的方式通知个人信息主体，并获得个人信息主体明确同意，包括：

a）主动式收集：个人信息主体基于自身利益同意收集：

1）事前收集：通过各种方式通知个人信息主体，并获得个人信息主体明确同意后，采用各种方法和手段非直接收集个人信息；

2）事后收集：未经个人信息主体同意，采用各种方法和手段非直接收集个人信息，获取个人信息后通过各种方式通知个人信息主体，并获得个人信息主体谅解和明确同意；

b）被动式收集：个人信息主体不知情或不能控制，并且事前、事后均未通知个人信息主体，未获得个人信息主体的明确同意。

13.3 权利保证

13.3.1 通用权利

遵循 DB21/T 1628.1 第 9 章的规则，任何类别、方式的个人信息收集，均应保证个人信息主体的权益不被侵犯，包括：

a）应基于特定、明确、合法的目的；

b）应履行告知义务，将个人信息收集目的、范围、方法、手段、处理方式等，以各种形式清晰无误的通知、告知个人信息主体，并征得个人信息主体明确同意；

c）应采用科学、规范、合法的收集方法和手段，收集适度、适当：

1）适度：应基于个人信息收集目的使个人信息收集达到满足需要的程度；

2）适当：应基于个人信息收集目的和个人信息管理原则使所收集的个人信息达到适用；

d）收集个人信息，应事先签署保密协议或申明保护个人信息的条款，如：

1）企业招聘、新员工参加工作时；

2）向公共机构，如银行、保险等提供个人信息时；

3） 委托或受委托涉及个人信息业务时等；

e）收集个人信息的方法和措施，应予以公开；

f）如个人信息主体提出疑义，应停止任何类别、方式的个人信息收集。

注19：任何类别、方式的个人信息收集，均应遵循 DB21/T 1628.1 9.2 的限制，保证个人信息主体的权益。

13.3.2 特定权利

遵循DB21/T 1628.1 9.2的规则，不应以任何目的、方法、手段等收集移动的个人信息数据库的信息：

a）可移动设备、媒介等构成的可移动的个人信息数据库，固定在个人信息管理者内部，与个人信息管理者内部个人信息数据库融为一体，个人信息收集的权利保证适用 13.3.1；

b）可移动设备、媒介等构成的可移动的个人信息数据库处于移动状态时，不应以任何目的、方法、手段等收集个人信息。

注20：个人信息数据库管理，参见 DB21/T 1628.3。

13.3.3 个人权利

个人信息主体应遵循12.5.4的规则，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，避免个人信息泄漏。

13.4 质量保证

个人信息管理者应保证所拥有个人信息的准确性、完整性和时效性：

a）个人信息收集目的明确、合法；

b）任何方式直接或间接收集个人信息，应保证个人信息的质量：

1）准确：真实、符合事实的；

2）完整：非零散、无扭曲的；

3）形态：能够反映最新事实的状态；

c）个人信息收集应适度、与目的相关，并不超出目的范围；

d）个人信息管理者所拥有的个人信息，应随时更新、完善，保证个人信息的最新状态。

13.5 责任保证

全体工作人员、客户、第三方客户、其他相关人员均应了解其在 PISMS 中的责任，避免个人信息滥用、泄漏、丢失的危险。

a）全体工作人员、其他相关人员应了解个人信息安全的重要性；在 PISMS 中，个人的责任和权利；PISMS 的作用和意义；

b）最高管理者、各级管理者、个人信息管理相关责任人的责任，应包括：

1）根据个人信息管理方针，实施个人信息管理；

2）明确各自的职责和授权及各部门间的协调；

3）提供所需资源，以实施、运行、监控、改进、完善 PISMS；

4）向全体工作人员宣传、传达个人信息安全相关事宜；

c）与客户涉及个人信息的业务交互时，应申明 PISMS 的必要性、方法和措施及客户的责任和义务；

d）接受委托、提供业务的第三方客户，也应履行个人信息管理者的责任和义务。

13.6 安全保证

在个人信息收集过程中，应提供适当的安全保证，避免个人信息泄漏、滥用。

收集、处理应基于明确、合法的目的，征得个人信息主体明确同意：

a）直接收集应征得个人信息主体明确同意，并将相关信息告知个人信息主体；

b）间接收集时：

1）如果可以以简捷、方便的方式与个人信息主体建立联系，应征得个人信息主体明确同意，并将相关信息通知个人信息主体；

2）拥有个人信息的第三方应提供合法说明，并获得个人信息主体授权；

3）委托收集，应根据DB21/T 1628.1 10.4的规则实施。

13.7 保存

应遵循DB21/T 1628.1 8.4的规则，建立统一的个人信息数据库，保存、存储以各种形式、方式收集的个人信息。

注21：个人信息数据库管理，参见 DB21/T 1628.3。

14 处理过程

14.1 概述

14.1.1 要求

应遵循DB21/T 1628.1 10.1的规则，管控、检查个人信息处理过程，保证个人信息质量和个人信息主体权益。

14.1.2 分类

依据DB21/T 1628.1 第4章，个人信息处理过程可划分为：

a）使用：基于特定、明确、合法的目的运用个人信息的行为，如编辑、加工、检索、存储、传输等；

b）利用：基于特定、明确、合法的目的和某种利益关系使用个人信息的行为，主要包括：

1）提供：向第三方提交合法、有效、适当的个人信息，存在利益输送；

2）委托：第三方实施的合法、有效的个人信息管理相关行为，存在利益输送：

- 委托第三方采用科学、规范、合法的收集方法和手段，收集个人信息；
- 委托第三方基于特定、明确、合法的目的使用个人信息；
- 接受第三方委托基于特定、明确、合法的目的使用个人信息；

3）交换：不同角色个人信息管理者之间以个人信息为基本实物特征的有偿收益行为，存在利益转换：

- 个人信息获取能力和处理活动交换；
- 个人信息交换；
- 个人信息收集方法、手段交换；
- 个人信息消费结果交换。

c）利用：基于某种利益关系，使用个人信息的行为，应限定个人信息使用目的，保证个人信息来源合法、有效：

1）交易：以个人信息为标的物出售，获得个人信息最大使用价值，获取最大利润的有偿收益行为；

2）二次开发：通过分析、挖掘、加工等行为，获得个人信息最大使用价值，获取最大利润的有偿收益行为；

d）后处理：个人信息处理过程结束后的个人信息处理行为。

14.2 来源合法

个人信息管理者应保证所拥有个人信息的来源合法、有效：

a）个人信息收集目的明确、合法，并明确告知个人信息主体；

b）个人信息收集手段、方式合法，并明确告知个人信息主体；

c）个人信息主体明确同意。

14.3 权益保证

个人信息处理应基于明确、合法的目的，遵循DB21/T 1628.1 第10章的规则，保障个人信息主体权益：

a）个人信息管理者所拥有的个人信息应合法、有效；

b）个人信息处理应与个人信息收集目的一致，并限制在目的范围内；

c）个人信息管理者应履行DB21/T 1628.1 6.4规定的责任和义务；

d）提供、委托、交换等个人信息利用行为应获得个人信息主体的授权；

e）在提供、委托、交换等个人信息利用行为中，利益输送和转换不应损害个人信息主体的权益。

14.4 质量保证

个人信息管理者应履行 DB21/T 1628.1 6.4 的规则，保证所拥有个人信息的准确性、完整性和时效性：

a）个人信息处理目的明确、合法；

b）任何方式处理个人信息，应保证个人信息的质量：

1）准确：真实、符合事实的；

2）完整：非零散、无扭曲的；

3）形态：能够反映最新事实的状态；

c）个人信息处理应合法、适当、适度、与目的相关，并不超出目的范围；

d）个人信息管理者所拥有的个人信息，应随时更新、完善，保证个人信息的最新状态。

14.5 责任保证

在个人信息处理中，应遵循13.5的规则。

14.6 安全保证

在个人信息处理、使用、利用过程中，应征得个人信息主体同意，并提供适当的安全保证，避免个人信息泄漏、滥用：

a）处理直接收集的个人信息，应限于收集目的范围内；

b）处理间接收集的个人信息，应保证个人信息来源合法、有效；

c) 根据DB21/T 1628.1 10.3.5和10.4，提供、委托、交换等个人信息利用行为应获得书面形式的保证。

14.7 开发和交易

14.7.1 要求

个人信息二次开发和交易，应遵循 DB21/T 1628.1 10.5 和 10.6 的规则，征得个人信息主体明确同意。如不能直接征得个人信息主体同意，应采取适当方式通知个人信息主体，并取得明确意见，获得授权；未取得个人信息主体明确同意，不应发生任何针对个人信息的行为。

14.7.2 交易形式

个人信息交易行为可包括：

a）销售者以个人信息的价值特征刺激市场消费；

b）有特定需求的消费者主动的市场询购行为；

c）个人信息交换在某种利益驱动下转换为交易等。

14.7.3 二次开发形式

个人信息的二次开发行为可包括：

a）通过各种公开渠道获得个人信息的分析、整理、筛选、挖掘、加工等；

b）通过各种社会活动、商业活动获得个人信息的分析、整理、筛选、挖掘、加工等；

c）过度收集获得个人信息的分析、整理、筛选、挖掘、加工等；

d）网络共享资源、电子商务、网络空间等的各类活动获取的个人信息的分析、整理、筛选、挖掘、加工等；

e）大数据资源的分析、整理、筛选、挖掘、加工等；

14.7.4 交易方式

由于交易目的、利益、需求等的不同，个人信息交易方式也不同，如：

a）基于主体权利：个人信息主体明确同意、个人信息主体默认、未经个人信息主体同意……；

b）基于商业利益：网络、短信、社会工程（诱惑、诈骗等）……等。

14.7.5 交易缺陷

应避免个人信息交易可能存在的缺陷，如：

a）信息不对称：应以各种适当的方式，将交易双方信息、交易目的、手段、范围、安全措施等信息通知个人信息主体；

b）合约不完全：在各种商业活动中，应严格个人信息主体与个人信息管理者之间的合约，规范个人信息安全约定，避免形成个人信息交易空间，如房地产销售、汽车销售、医疗、招聘等；

c）重复利用：应尽可能减少个人信息的重复、多次使用，避免由此产生的信息失真、质量缺陷和利益链条对个人信息主体权益的损害等。

14.7.6 责任保证

在个人信息二次开发和交易中，全体相关人员均应了解保证个人信息安全的责任，避免个人信息滥用、泄漏、丢失的危险，包括：

a）应履行 DB21/T 1628.1 7.2、6.4 规定的个人信息管理原则和个人信息管理者的责任和义务；

b）应限定在法律许可范围内；

c）应通知个人信息主体并征得个人信息主体明确同意；

d）应保证个人信息主体权利唯一，仅仅发生个人信息使用权转让；

e）应保证继承个人信息相关的责任和义务；

f）应限定在个人信息主体同意的范围内使用，避免随意泄漏、传播和扩散等；

g）应规范个人信息二次开发、交易行为，保证个人信息主体的个人信息支配权。

14.7.7 质量保证

个人信息二次开发、交易应遵循 DB21/T 1628.1 6.4 的规则，保证个人信息的准确性、完整性和时效性：

a）应保证个人信息的质量：

1）准确：真实、符合事实的；

2）完整：非零散、无扭曲的；

3）形态：能够反映最新事实的状态；

b）应合法、适当、适度、有序；

c) 应随时更新、完善，保证个人信息的最新状态。

14.7.8 安全保证

在个人信息二次开发、交易中，应建立相应的安全机制，保证个人信息安全：

a）应限定在个人信息主体同意的范围内；

b）应保证个人信息来源合法、有效；

c）应建立事故处理和应急机制；

d）应获得个人信息主体有效授权。

14.8 后处理

14.8.1 分类

个人信息处理、使用后，可存在几种情况：

a）根据与个人信息主体的约定，需要继续保存；

b）根据合同约定方式，需要继续使用；

c）提供、委托业务结束后，需要按照合约返还；

d）结束个人信息生命周期，彻底销毁。

14.8.2 质量保证

个人信息处理、使用后，14.8.1a）、b）、c）均需保证个人信息质量：

a）准确：真实、符合事实的；

b）完整：非零散、无扭曲的；

c）形态：能够反映最新事实的状态；

d) 应保证个人信息的最新状态；

e）应保证合约的完整、合理、有效；

f）应避免重复使用可能产生的信息失真。

14.8.3 安全措施

个人信息处理、使用后，应根据 DB21/T 1628.1 10.7 采取相应的安全措施，如：

a）个人信息管理者在管理过程中涉及个人信息相关事务，如已与管理、业务无关，应明确继续保存的时限和方式，及超过保存时限后的销毁方式、销毁时间、销毁责任人等；

b）个人信息管理者在涉及个人信息的业务活动完成后，应根据合同约定、规章制度，采取相应的处理措施；

c）向第三方提供个人信息，应根据 DB21/T 1628.1 10.3.5 验证安全承诺，并约定处理、使用后的处理方式。获得第二方提供的个人信息，应严格遵循安全承诺和处理、使用后的处理约定；

d）委托业务（委托第三方收集个人信息或向第三方委托个人信息处理业务）完成后，应根据 DB21/T 1628.1 10.4，验证安全承诺，并按约定处理个人信息；

e）二次开发和交易完成后，应根据 DB21/T 1628.1 10.5、10.6，验证安全承诺，检验个人信息使用的方式、方法、目的、范围等，并按约定处理个人信息；

f）未取得个人信息主体明确同意，不应发生任何针对个人信息的行为。

15 个人信息安全风险管理

个人信息管理者代表应责成安全管理责任主体对个人信息及相关资源可能存在的安全风险实施风险管理。参见 DB21/T 1628.5。

16 个人信息安全管理

根据 DB21/T 1628.1 第 11 章，个人信息安全管理责任主体应根据整体信息安全需求、个人信息安全特点，采取相应的安全措施（参见 DB21/T 1628.6）。

17 内审

个人信息安全管理体系内审管理，参见 DB21/T 1628.7。

18 过程改进

18.1 服务台管理

应根据 DB21/T 1628.1 12.2，展开服务台管理：

a）明确服务宗旨、服务台功能；

b）明确相关责任人的职能和服务意识；

c）培训、提高相关责任人的服务水平、技术能力；

d）适时评估服务、相关人员的服务水平和能力。

应公布服务台管理责任人、联系方式；并记录服务过程中的所有活动或行为。

18.2 缺陷事项

根据 DB21/T 1628.1 第 12 章，在 PISMS 内审中发现不符合个人信息安全相关法规、规范、规章的缺陷事项，应在过程改进中纠正。

a）缺陷说明及内容；

b）缺陷原因；

c）缺陷纠正措施；

d）纠正跟踪。

18.3 纠正措施

在过程改进中消除缺陷事项，预防再次发生。纠正措施应包括：

a）确认缺陷事项；

b）确定缺陷事项原因；

c）确定和实施缺陷事项纠正措施；

d）评估所采取的纠正措施，评估包括纠正措施的安全性、纠正措施对个人信息管理的影响、纠正措施的有效性和可用性等。

18.4 预防措施

在过程改进中，应消除潜在的缺陷，预防发生：

a）识别并确认潜在的缺陷；

b）制定并评估预防缺陷发生需要采取的措施；

c）确定和实施缺陷预防措施；

d）评估所采取的预防措施。

识别潜在的缺陷，应结合风险管理实施。注重风险变化。

18.5 跟踪和监控

根据 DB21/T 1628.1 12.2，PISMS 内审机构应实时跟踪、监控 PISMS 的构建、实施和运行，及时发现 PISMS 潜在的安全风险、缺陷和存在的问题，提出整改建议，提请个人信息管理者代表采取相应的整改措施，推进 PISMS 的持续改进。

18.6 持续改进

根据 DB21/T 1628.1 12.2.3，应通过个人信息安全策略、个人信息安全目标、PISMS 内审、服务台反馈、跟踪和监控、纠正和预防措施，持续改进和完善 PISMS 的有效性、充分性。

注22：过程改进后应重新实施 PISMS 内审。

19 管理和业务的连续性管理

19.1 要求

个人信息管理应是个人信息管理者管理过程、业务活动的完整部分。PISMS 运行不应影响关键业务流程、中断管理过程，并能够在受到影响时及时恢复。

为避免受到影响，或在受到影响时及时恢复并将影响降到最小，应实现管理过程和业务活动的连续性管理。

19.2 连续性与风险管理

在个人信息安全风险管理中，应注意所有资源参与下的风险评估：

a）考虑个人信息安全对整体管理过程的要求，并不局限于个人信息安全；

b）考虑个人信息安全对业务活动的要求，并不局限于个人信息安全。

综合分析判断风险，包括可能产生的影响、影响时限、恢复等，采取相应的应对措施，保证管理过程和业务活动的连续性。

19.3 连续性与 PISMS

制定事故应急预案时，应考虑：

a）PISMS 运行可能对个人信息管理者的管理过程、业务活动的影响；

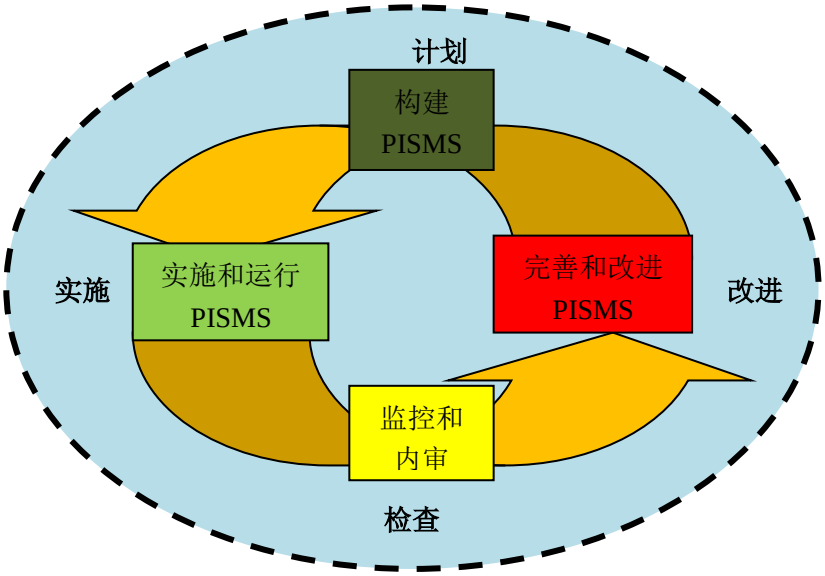
b）在要求时限内恢复；

c）可能造成损失的评估；

d）应急处理方案等。

附 录 A
（规范性附录）
过程管理图示

适于 PISMS 的 PDCA 模式，如图示。



附 录 B
（资料性附录）
DB21/T 1628.1 与 DB21/T 1628.2

表B-1列出了DB21/T 1628.1《信息安全 个人信息保护规范》第3章至第14章（A.3-A.14）的规则与本实施指南的对应。表中所列可能不尽详细，个人信息管理者宜根据个人信息安全相关法规、规范和管理、业务实际增加相应的管理措施。

表 B-1 DB21/T 1628.1 要求与实施指南

规范		实施指南	
章节	规则	章节	对应
3	个人信息	6	个人信息
3	个人信息主体	7	个人信息主体
4	个人信息主体权利	7.4	权利
5	个人信息生命周期	8	个人信息生命周期
6	个人信息管理者	9	个人信息管理者
7	个人信息管理	10	个人信息管理
7.1	目的	11	资源管理
8	个人信息管理机制	12	管理机制
9	个人信息获取	13	获取过程
10	个人信息处理	14	处理过程
11.1	风险管理	15	个人信息管理安全风险管理
11	安全管理	16	个人信息安全管理
12.1	PISMS 内审	17	内审
12.2	过程改进	18	过程改进

		19	管理和业务的连续性管理