ICS 35.020
CCS L 70

DB21

辽 宁 省 地 方 标 准

DB21/T 1628.3—2026
代替 DB21/T 1628.3-2016

信息安全技术 个人信息安全 第3部分:个人信息数据库管理指南

Information security technology—Personal information security—Part3:Managerment guidelines for personal information database

2026-01-07 发布 2026-02-07 实施

辽宁省市场监督管理局 发布

目　　次

前言 III
引言 V
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　综述 1
5　组织 2
6　环境 3
7　管理 4
8　安全管理 6
9　内审 6
10　应急管理 7
11　例外 7

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。

本文件是DB21/T 1628 的第3部分。DB21/T 1628已发布以下部分：

——第 1 部分：要求；

——第 2 部分：实施指南；

——第 3 部分：个人信息数据库管理指南；

——第 4 部分：文档管理指南；

——第 5 部分：风险管理指南；

——第 6 部分：安全技术实施指南；

——第 7 部分：内审实施指南；

——第 8 部分：过程管理指南。

本文件代替DB21/T 1628.3—2016《信息安全　个人信息数据库管理指南》。与DB21/T 1628.3—2016相比，本部分除编辑性修改外，主要技术变化如下：

a)　标准名称修改为《信息安全技术　个人信息安全　第 3 部分：个人信息数据库管理指南》；

b)　增加了个人信息数据库的论述（见第 4 章）；

c)　增加新技术应用相关数据（个人信息）相关规则（见第 7、8 章）；

d)　增加个人信息假名、个人信息匿名相关规则（见第 4、5、7、8 章）；

e)　增加个人信息生命周期内个人信息跨境收集、处理、使用相应规则等（见第 5、7、8 章）。

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专利的责任。

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、国家计算机网络应急技术处理协调中心辽宁分中心、大连交通大学、大连软信咨询服务有限公司、大连市计算机学会。

本文件主要起草人：郎庆斌、李凯、孙鹏、尹宏、丁宗安、孙毅、吕蕾蕾、杨莉、司丹、郭玉梅、王小庚、宋悦、王开红、曹剑。

本文件及其所代替文件的历次版本发布情况：

——2016 年首次发布为 DB21/T 1628.3—2016；

——本次修订为第一次修订。

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，有关单位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：0411-88255657。

引　言

DB21/T 1628.1—2016发布实施以来，在社会、经济、文化等各个领域的深刻变革中，对辽宁省个人信息安全起到了重要的指导作用。随着科学技术，特别是新一代信息技术的进步和发展，引发新的个人信息安全风险，需要在新的形势下重新审视个人信息安全标准的普适性。同时，个人信息安全相关的一些术语、概念、规则表述等存在重大差异，目前的一些表述形式，可能引发个人信息安全的潜在风险，需要新的、更加严谨、科学的规范。

无论传统的个人信息形态，还是新一代信息技术的应用（如智慧城市、云服务、大数据、物联网、智能识别、智能应用、移动应用等），管理是安全的关键。本文件再次修订，以管理为主线，以个人信息生命周期，即服务管理过程为导向，以个人信息安全和个人信息管理质量为目标，基于多年的研究和实践，严谨、科学地规范个人信息安全相关术语、概念和规则表述，制定个人信息生命周期内管理要素的约束规则。

本次修订，完善DB21/T 1628个人信息安全标准体系，遵循标准体系构建的一般规律，重新调整、归类，形成相对科学、规范的标准体系结构。修订完成的DB21/T 1628个人信息安全标准体系，以本文件为纲，提纲挈领，总括DB21/T 1628个人信息安全标准体系总体规范，以管理为主线，以个人信息生命周期为导向，以个人信息安全和个人信息管理质量为目标，分解并规范个人信息生命周期内管理要素约束规则，构成各自相对独立，又相互关联的标准子集，形成完整、系统的DB21/T 1628个人信息安全标准体系。DB21/T 1628拟由8部分构成。

——第 1 部分：要求。目的在于确立个人信息、主体、个人信息主体权利、个人信息管理者、个人信息管理、个人信息获取过程、个人信息处理过程、过程管理、安全管理和例外等的基本规则和要求。

——第 2 部分：实施指南。目的在于为个人信息管理者提供个人信息管理相关指导和通用准则。

——第 3 部分：个人信息数据库管理指南。目的在于为个人信息管理者构建、管理、维护、改进个人信息数据库提供指导和通用准则。

——第 4 部分：文档管理指南。目的在于为个人信息管理者在个人信息生命周期内，建立完善的个人信息管理相关文档的管理机制提供指导和通用准则。

——第 5 部分：风险管理指南。目的在于为个人信息管理实施过程中实施风险管理提供指导和帮助。

——第 6 部分：安全技术实施指南。目的在于为个人信息管理者构建、实施、运行个人信息安全管理体系采用安全技术提供指导和通用准则。

——第 7 部分：内审实施指南。目的在于规定个人信息安全管理体系内审原则、管理、管理机制和实施的基本规则和要求。

——第 8 部分：过程管理指南。目的在于为个人信息安全管理体系构建、实施、运行的过程管理提供指导和通用规则。

信息安全技术　个人信息安全
第3部分:个人信息数据库管理指南

1　范围

本文件为个人信息管理者构建、管理、维护、改进个人信息数据库提供指导和通用准则。

本文件适用于自动或非自动处理全部或部分个人信息的机关、企业、事业、社会团体等组织及个人。

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/T 22081　信息技术　安全技术　信息安全管理实用规则

DB21/T 1628.1—2025　信息安全技术　个人信息安全　第1部分：要求

DB21/T 1628.2—2025　信息安全技术　个人信息安全　第2部分：实施指南

3　术语和定义

DB21/T 1628.1—2025 界定的以及下列术语和定义适用于本文件。

3.1

事务 transaction

个人信息存储、保存、管理、处理、使用的操作流程。

3.2

存储 storage

在不同的应用环境中，以合理、安全、有效的方式将数据储存到适宜的介质上，并保证可有效访问。本标准特指自动处理方式的个人信息储存。

3.3

保存 save

在不同的应用环境中，以合理、安全、有效的方式将数据保留到适宜的介质上，并使事物、性质、意义等继续存在，不受损失或不发生变化。本标准特指非自动处理方式的个人信息储存。

4　综述

依据DB21/T 1628.2—2025第5章，个人信息的存在形态是多样化的，随着信息技术、网络技术，特别是新兴技术的快速发展，个人信息更加多样化存在，散见于各种记录、保存方式，如纸媒体、数字媒体等。其管理方式不尽相同。

个人信息保存、存储可藉助传统数据库的形式，形成逻辑统一的个人信息数据库，适应个人信息管理者不同需求的个人信息数据库管理机制。统一个人信息的管理包括：

a)　个人信息可记录在各种媒介；

b) 个人信息可以各种形式保存、存储；
c) 个人信息可散在于个人信息管理者内部；
d) 个人信息可包括在日常管理、业务管理中；
e) 个人信息假名化后特征数据库和一般琐碎信息库；
f) 新技术应用相关大数据（含个人信息）存储等。

5 组织

5.1 介质

记录个人信息的保存、存储媒介，主要可包括：

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、网盘、云盘、邮件、即时通讯、网站、网络视频等；
g) 声音媒介：录音、录像等。

5.2 记录

依据DB21/T 1628.1—2025，在个人信息生命周期内，各类保存、存储介质记载、存储的个人信息（包括个人信息假名化后的一般琐碎信息），应简明、清晰、可识别，易于提取、修正、拷贝。

5.3 识别

依据DB21/T 1628.1—2025、DB21/T 1628.2—2025，个人信息管理者应识别所有与个人信息主体权益相关的信息，包括：

a) 个人信息管理者内部的个人信息（包括个人保有的与个人信息主体相关的所有信息）识别；
b) 个人信息管理者业务相关的个人信息识别；
c) 移动的个人信息识别等；
d) 智能识别、智能应用、物联网应用等新技术相关数据中个人信息的筛选、识别；
e) 其他与个人信息主体权益相关的信息。

注1：个人信息管理者拥有的所有可识别的个人信息、个人信息假名化后的一般琐碎信息、个人信息匿名化的琐碎信息等，不应由个人信息管理者的员工以各种方式保有；

注2：个人信息管理者应管控与个人信息主体权益相关的所有信息。

5.4 形式

依据DB21/T 1628.1—2025、DB21/T 1628.2—2025，各类保存、存储介质记载、存储的个人信息，应形成逻辑统一的个人信息数据库，并构建规范、统一的个人信息数据库事务：

a) 个人信息管理者内部的个人信息，应在管理过程中建立统一的个人信息数据库事务；
b) 个人信息管理者业务相关的个人信息，应在业务管理过程中建立统一的个人信息数据库事务；
c) 移动的个人信息也宜形成规范的个人信息数据库事务；

d) 智能识别、智能应用、物联网应用等新技术相关数据，宜建立统一、规范的个人信息数据库事务；
e) 个人信息假名化后的特征数据库、一般琐碎信息数据库应分别建立个人信息数据库事务；
f) 个人信息匿名化的琐碎信息，如需保存、存储，亦宜建立数据库事务；
g) 个人信息跨境处理形成的数据库应建立规范的个人信息数据库事务等。

注：各种形式的个人信息数据库事务，均宜构成统一的个人信息数据库管理机制。

5.5 构成

个人信息数据库应有序、可控，主要构成应包括：

a) 自动处理形成的个人信息数据库：
   1) 基于管理、工作等需要形成的个人信息存储（如人力资源管理、教育管理等）；
   2) 基于公共服务形成的个人信息存储（如社会服务、医疗卫生等）；
   3) 基于公共安全等形成的个人信息存储（如公共监控、智能识别等）；
   4) 基于新技术应用等形成的数据（个人信息）存储；
   5) 基于各种利益关系的需要形成的个人信息存储（网上活动、商业活动等）等；
b) 非自动处理形成的个人信息数据库：
   1) 自动处理形成的个人信息数据库的备份；
   2) 自动处理中以非自动处理保存的个人信息（如人力资源管理、社会服务等）；
   3) 除自动处理外其它个人信息保存形式等；
c) 移动个人信息数据库：
   1) 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；
   2) 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等；
d) 个人信息假名形成的数据库：
   1) 个人信息主体特征信息数据库；
   2) 假名化后的一般琐碎个人信息库；
e) 个人信息匿名形成的一般琐碎信息数据库；
f) 个人信息跨境处理形成的个人信息数据库：
   1) 跨境提供、交付委托个人信息收集、处理相关业务应建立特定的个人信息数据库；
   2) 接受跨境委托个人信息收集、处理相关业务应建立相关的特定个人信息数据库等。

6 环境

6.1 保存环境

保存非自动处理的个人信息介质，环境、条件应适宜，且便于提取，以保证个人信息数据库的保密性、安全性：

a) 保存空间：存放空间应保持相对独立、封闭；
b) 保存环境：应根据保存介质的不同采取相应的存放措施（如干燥、通风、避光等）；
c) 保存条件：应根据不同的保存介质采用相应的存放方法（如卷宗、文件夹等）。

注：介质内包含多种信息（含个人信息）时，亦应遵循以上规则。

6.2 存储环境

可自动处理的个人信息介质相关的IT环境，应遵循GB/T 22081和其它相关标准的规则。

6.3 移动环境

移动个人信息数据库应遵循DB21/T 1628.1—2025、DB21/T 1628.2—2025和其它相关标准的规则，根据不同的环境因素采取相应的安全防范措施：

a) 移动存储设备存放环境应保持相对独立，易于提取；
b) 移动存储设备存放环境应避免电磁等各种外来因素的影响；
c) 移动存储设备使用环境、使用平台应保证相对安全，如严格管理措施、安全措施等；
d) 随个人信息主体移动的手持移动设备、芯片卡、非自动处理介质等，一般处于较复杂的环境因素中，个人信息主体应提高安全意识，注意识别安全风险，依据不同的存在、使用环境采取不同的存放、使用措施等。

7 管理

7.1 机制

7.1.1 形式

个人信息数据库的管理形式，应参照DB21/T 1628.1—2025和DB21/T 1628.2—2025个人信息管理者、个人信息管理相关规则，由个人信息管理代表指定专人负责个人信息数据库管理，并明确管理职责。

7.1.2 职责

个人信息数据库管理责任主体的职责，主要应包括：

a) 明确个人信息数据库的分布和组织形式；
b) 明确个人信息数据库的管理形式；
c) 建立个人信息数据库管理事务；
d) 制定个人信息数据库管理规章；
e) 制定新技术应用相关数据（个人信息）库的管理形式；
f) 制定新技术应用相关数据（个人信息）库的管理规章；
g) 制定个人信息假名相关数据库管理规章；
h) 制定个人信息匿名相关数据库管理规章；
i) 制定个人信息跨境处理相关特定数据库管理规章；
j) 依据个人信息数据库的分布和组织形式明确相关责任主体；
k) 个人信息数据库备案管理；
l) 协调个人信息数据库相关的部门、人员、管理、业务、资源及外部因素等；
m) 个人信息数据库相关文档管理等。

7.1.3 制度

应依据DB21/T 1628.1—2025建立个人信息数据库管理相关规章制度，主要应包括：

a) 最高管理者的个人信息数据库认定形式；
b) 个人信息数据库的组织形式；
c) 个人信息数据库管理责任主体的任命和职责；
d) 个人信息数据库管理相关责任主体的任命和职责；
e) 个人信息数据库的管理策略和事务；
f) 新技术应用相关数据（个人信息）库的管理策略和事务；

g） 个人信息假名相关数据库的管理策略和事务；
h） 个人信息匿名相关数据库管理事务；
i） 个人信息跨境处理相关特定数据库的管理策略和事务；
j） 个人信息数据库合法、合理、有效保存/存储个人信息的措施；
k） 个人信息数据库的时效规定；
l） 个人信息数据库的管理和使用；
m） 个人信息数据库使用权限和安全管理；
n） 个人信息数据库备案登记；
o） 个人信息数据库的备份和恢复；
p） 个人信息数据库的维护和记录；
q） 个人信息数据库使用后的处理措施；
r） 个人信息数据库的事故处理；
s） 其它必要的安全管理措施等。

7.1.4 控制

应遵循DB21/T 1628.1—2025和DB21/T 1628.2—2025的规定，制定相应的个人信息数据库、新技术应用相关数据（个人信息）库、个人信息假名相关数据库、个人信息匿名相关数据库、个人信息跨境处理相关特定数据库的管理策略、管理计划，建立管理事务，并根据管理、业务等的变化，检查、修正个人信息数据库相关管理活动和行为。

7.1.5 文档管理

应根据DB21/T 1628.1—2025的10.5.4，记录与个人信息数据库、新技术应用相关数据（个人信息）库、个人信息假名相关数据库、个人信息匿名相关数据库、个人信息跨境处理相关特定数据库相关的行为，包括目的、时间、范围、对象、方式方法等个人信息数据库事务形成的各种信息，及个人信息数据库建立、事故、维护等活动信息。

7.2 策略

7.2.1 时限

个人信息数据库记载、存储个人信息时，应根据环境、条件、业务、管理等实际需要，确定并明确适宜的管理时限。个人信息假名相关数据库、个人信息匿名相关数据库、个人信息跨境处理相关特定数据库均应设定相应的管理时限。

7.2.2 质量

个人信息数据库记载、存储的个人信息，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。个人信息假名相关数据库、个人信息跨境处理相关特定数据库亦应及时更新，保持最新状态。

7.2.3 后处理

各种构成的个人信息数据库记载、存储的个人信息达到管理时限或使用、处理后另有约定，应遵循DB21/T 1628.1—2025的13.7和DB21/T 1628.2—2025的13.9的规定，采取相应的安全措施。

7.2.4 事务

应根据个人信息数据库的分布和组织形式、个人信息数据库的构成、个人信息管理者的管理特征、个人信息的使用处理特征等，建立适宜个人信息管理者实际的个人信息数据库管理事务。

7.3 备案管理

应根据DB21/T 1628.1—2025的12.4.2，建立个人信息数据库使用、查阅备案登记制度，由专人负责，并明确责任人的职责，确定相应的管理措施。记录主要应包括责任人、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。

8 安全管理

8.1 风险评估

应遵循DB21/T 1628.1—2025第15章和DB21/T 1628其它部分的规定，评估个人信息数据库的风险，主要应包括：

a) 个人信息记载、存储时的风险隐患；
b) 个人信息数据库管理风险；
c) 个人信息提取、重入风险；
d) 新技术应用相关数据（个人信息）管理、应用风险；
e) 新技术应用相关数据（个人信息）未知、潜在风险预测、预警；
f) 个人信息假名化风险；
g) 个人信息匿名化可能存在的隐患；
h) 个人信息主体画像的偏差、差异风险；
i) 个人信息深度开发风险；
j) 个人信息跨境处理的风险；
k) 个人信息后处理风险等；

应制定相应的风险应对策略，采取风险管理措施，监控风险变化，保证个人信息数据库的安全。

8.2 安全管理

个人信息数据库安全管理，应遵循信息安全相关法规、标准和DB21/T 1628.1—2025第15章及DB21/T 1628其它部分的规定。

9 内审

9.1 审计

应根据DB21/T 1628.1—2025第14章及DB21/T 1628其它部分的规定，定期审计、评估个人信息数据库的安全性、可用性和时效性，跟踪监控安全风险，适时改进安全策略，改进、完善个人信息数据库事务。

9.2 内容

内审应基于个人信息安全管理体系的安全性设计，内容主要应包括：

a) 个人信息数据库的构成方式、管理模式的合理性、可靠性和可信性；
b) 个人信息数据库内容的有效性、规范性和质量可靠性；
c) 个人信息数据库环境、基础、管理、使用等的可适性、安全性；

d) 个人信息数据库事务的合理性、有效性和规范性等。

9.3 报告

应建立定期报告制度，个人信息数据库审计评估结果、安全风险及改进策略、事故及处理方式和结果、个人信息数据库事务改进策略等个人信息数据库动态变化及对个人信息安全管理体系的影响均应形成报告，及时上报个人信息管理代表。

10 应急管理

应遵循DB21/T 1628.1—2025的相关规则，建立个人信息数据库应急处理机制。

11 例外

遵循DB21/T 1628.1—2025第17章的规定，个人信息数据库内容不应包含敏感个人信息。经个人信息主体同意的或法律特别规定的例外，应建立独立的个人信息数据库和相应的管理机制，采取特别的保护措施，一经处理、使用完毕，立即完全、彻底销毁。