ICS 35.020
L 70

DB21

辽　宁　省　地　方　标　准

DB21/T 1628.3—2016

信息安全 个人信息数据库管理指南

Information Security-guidelines for personal information database managerment

2016－09－27 发布　　2016－11－27 实施

辽宁省质量技术监督局　发布

目　　次

前　言

DB21/T1628 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实施指南

——信息安全 个人信息数据库管理指南

——信息安全 个人信息管理文档管理指南

——信息安全 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安全技术实施指南

——信息安全 个人信息安全管理体系内审实施指南等

——信息安全 个人信息安全管理体系过程管理指南等。

本部分是 DB21/T1628 的第 3 部分。

本部分按照 GB/T1.1-2009《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。

本部分由大连市经济和信息化委员会提出。

本部分由辽宁省经济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。

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

信息安全　个人信息数据库管理指南

1　范围

本标准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。

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。

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 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

DB21/T 1628.5 信息安全 个人信息安全风险管理指南

3　术语和定义

DB21/T 1628.1、DB21/T 1628.2、DB21/T 1628.5界定的以及下列术语和定义适用于本标准。

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　要求

本指南遵循DB21/T 1628.1确立的个人信息安全原则和要求，亦遵循DB21/T 1628.2确立的实施细则，重点描述和指导个人信息数据库构建、管理、运行的约束规则和评估、监控、改进的方法。

个人信息数据库管理，应同时使用DB21/T 1628.1、DB21/T 1628.2和本指南，并参照DB21/T 1628系列其它标准。

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，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，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、DB21/T 1628.2，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）；

b）个人信息管理者业务相关的个人信息；

c）移动的个人信息等；

d）其他与个人信息主体权益相关的信息。

注1：1）个人信息管理者拥有的所有可识别的个人信息，不应由个人信息管理者的员工以各种方式保有；

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、DB21/T 1628.2，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。

注2：个人信息管理者拥有的所有可识别的个人信息均宜构成统一的个人信息数据库。

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）个人信息管理者基于管理、工作等需要形成的个人信息存储（如人力资源管理等）；

2）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）；

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）除自动处理外其它个人信息保存形式；

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。

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3：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、DB21/T 1628.2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，如严格的规章制度等；

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。

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 7.5和DB21/T 1628.2第7章的规定，由个人信息管理者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者的职责，主要应包括：

a）明确个人信息数据库的分布和组织形式；

b）建立个人信息数据库管理事务；

c）制定个人信息数据库管理规章；

d）个人信息数据库备案管理；

e）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；

f）个人信息数据库相关文档管理等。

7.1.3 制度

应遵循DB21/T 1628.2 11.1.1.6的规定，建立个人信息数据库管理相关规章制度，内容应包括：

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）个人信息数据库的管理策略和事务；

d）个人信息数据库合法、合理、有效保存/存储个人信息的措施；

e）个人信息数据库的时效规定；

f）个人信息数据库的管理和使用；

g）个人信息数据库管理责任者的任命和职责；

h）个人信息数据库使用权限和安全管理；

i）个人信息数据库备案登记；

j）个人信息数据库的备份和恢复；

k）个人信息数据库的维护和记录；

l）个人信息数据库使用后的处理措施；

m）个人信息数据库的事故处理；

n）其它必要的安全管理措施。

注4：改写DB21/T 1 628.2 11.1.1.6。

7.1.4 控制

应遵循DB21/T 1628.1和DB21/T 1628.2的规定，制定相应的管理策略、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 8.5，记录与个人信息数据库相关的行为，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。

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。

7.2.3 后处理

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 10.7和DB21/T 1628.2 12.3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 二次开发

基于个人信息主体同意并授权，二次开发个人信息数据库，应遵循DB21/T 1628.1 10.5的规定。

7.4 备案管理

应根据DB21/T 1628.1 8.4.4，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第11章和DB21/T 1628.5的规定，评估个人信息数据库的风险，主要包括：

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）个人信息后处理风险；

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DB21/T 1628.1 第11章的规定。

9 内审

9.1 审计

应根据DB21/T 1628.1 12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者代表。

10 应急管理

应遵循DB21/T 1628.1 12.3的规定，建立个人信息数据库应急处理机制。

11 例外

遵循DB21/T 1628.1第13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。