DB

辽 宁 省 地 方 标 准

DB21/T 1628-2008

个人信息保护规范

Personal Information Protection Specification

2008-06-16 发布　　2008-07-16 实施

辽宁省质量技术监督局 发布

目录

前言

本标准依据国际、国内相关法律、法规及信息安全相关标准，遵循 OECD（世界经济合作发展组织 Organization for Economic Co-operation and Development）《关于保护隐私和个人数据跨国流通的指导原则》，参考国际通行的个人信息保护相关法规和行业自律模式制订。

本标准由大连市信息产业局提出。

本标准由辽宁省信息产业厅归口。

本标准主要起草单位：大连软件行业协会、辽宁省信息安全与软件测评认证中心。

本标准主要起草人：郎庆斌、孙鹏、王开红、郭玉梅、曹剑、李倩、李舒明、王占昌、张弩、潘玉景、邢轶男。

本标准发布日期：属首次发布。

个人信息保护规范

1 范围

本标准规定了个人信息保护相关术语和定义、个人信息保护原则、个人信息主体权利、个人信息管理者的义务、个人信息保护体系的建立、个人信息保护实施、个人信息保护的安全机制、持续改进、个人信息保护评价等基本规则和要求。

本标准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 术语和定义

2.1 个人信息

与特定个人相关、并可识别该个人的信息，如数据、图像、声音等，包括不能直接确认，但与其他信息对照、参考、分析仍可间接识别特定个人的信息。

2.2 个人信息数据库

为实现一定的目的，按照某种规则组织的个人信息的集合体。包括：

a）可以通过自动处理检索特定的个人信息的集合体，如磁介质、电子及网络媒介等；

b）可以采用非自动处理方式检索、查阅特定的个人信息的集合体，如纸介质，声音，照片等；

c）除前 2 项外，法律规定的可检索特定个人信息的集合体。

2.3 个人信息主体

可通过个人信息识别的特定的自然人。

2.4 个人信息管理者

获个人信息主体授权，基于特定、明确、合法目的，管理、处理、使用、利用个人信息的机关、企业、事业、社会团体等组织及个人。

2.5 收集

基于特定、明确、合法的目的获取个人信息的行为。

2.6 处理

自动或非自动处置个人信息的过程，如录入、加工、编辑、存储、检索、交换、传输、输出等行为及其它处置行为。

个人信息的自动处理是利用计算机及其相关和配套设备、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进行信息收集、加工、存储、传输、检索、咨询、交换等业务。

个人信息的非自动处理是按照一定的应用目的和规则，人工进行信息收集、加工、存储、传输、检索、咨询、交换等业务。

2.7 使用

基于特定、明确、合法的目的，运用个人信息的行为。

2.8 利用

基于特定、明确、合法的目的，提供、委托第三方处理、使用个人信息及其它因某种利益处理、使用个人信息的行为。

2.9 保护

社会生活中为尊重、保护个人人格权，个人信息管理者对基于特定、明确、合法目的收集、保存、管理、处理、使用、利用的个人信息采取相应的安全管理措施，并组织、开展个人信息安全的宣传、教育；制定个人信息保护的基本规章制度；监督个人信息保护的实施。

2.10 个人信息主体同意

收集、处理、使用、利用个人信息，应通知个人信息主体并征得个人信息主体的明确同意。通知形式包括：

a）以书面形式通知个人信息主体；

b）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通知个人信息主体。

3 原则

3.1 目的明确

个人信息收集应有明确的目的，不得超范围处理、使用、利用。

3.2 主体权利

个人信息主体对相关个人信息享有权利。

3.3 信息质量

个人信息应在收集、处理目的范围内保持准确性、完整性和最新状态。

3.4 使用限制

个人信息收集、处理、利用应采用合理、合法的手段和方式，并保持公开的形式。

3.5 安全保障

应采取必要、合理的管理和技术措施，防止未经授权的个人信息检索、使用、公开及丢失、泄露、损毁、篡改等行为。

4 个人信息主体权利

4.1 知情权

a）确认个人信息数据库中与个人信息主体相关的信息；
b）确认个人信息收集、处理、使用、利用的相关信息；
c）查阅个人信息数据库中与个人信息主体相关的个人信息。

4.2 支配权

a）收集、处理、使用、利用个人信息，必须经个人信息主体以书面形式明确同意，并签字盖章。下述情况视为默认的个人信息主体的意愿：

- 由监护人代表未成年的或无法做出正确判断的成年的个人信息主体表达的意愿；
- 个人信息管理者与个人信息主体签订合同中确认了相关个人信息处理的规定，个人信息主体同意履行合同；

b）个人信息主体有权修改、删除、完善相关个人信息，以保证个人信息的完整、准确和最新状态；
c）个人信息主体有权以其它方式利用与之相关的个人信息。

4.3 疑义和反对

a）个人信息主体有权质疑相关个人信息的准确性、完整性和时效性；
b）个人信息主体有权质疑或反对相关个人信息的使用及利用目的、处理过程等；

c）个人信息主体如果认为相关个人信息的使用及利用目的、处理过程等侵害了相关主体的权益、或其它正当理由，有权提出撤消该个人信息；撤消应经个人信息主体确认。

5 个人信息管理者义务

5.1 权利保障

个人信息管理者必须保障个人信息主体的权利。

5.2 目的明确

个人信息管理者必须保证个人信息处理、使用及利用的目的与个人信息主体的意愿一致，不能超目的、超范围处理、利用。

5.3 告知

个人信息管理者应将个人信息的使用及利用目的、处理方式、不提供个人信息的后果、查询和更正相关个人信息的权利，以及个人信息管理者本身的相关信息等告知个人信息主体。

5.4 质量保证

个人信息管理者应保证收集、管理、处理、使用、利用个人信息的完整性、准确性、可用性，并保持最新状态。

5.5 保密性

个人信息管理者必须对所管理的个人信息予以保密，并对个人信息处理、使用、利用过程中的安全负责。

6 个人信息保护体系

应构建个人信息保护体系，协调保护机制和各类资源，保障个人信息主体的权利，保障业务系统的稳定运行。体系应包括：

a）方针；

b）机构及职责；

c）目标和基本原则；

d）管理机制；

e）实施过程；

f）安全机制；
g）跟踪与评估；
h）过程模式；
i）持续改进。

7 个人信息保护方针

应是指导个人信息保护工作，符合个人信息管理者实际情况，遵守国家相关法律、法规的原则和措施，并应以简洁、明确的语言阐述，并公之于众。内容主要包括：

a）个人信息主体的权利；
b）个人信息管理者的义务；
c）个人信息保护的目的和原则；
d）个人信息保护的措施和方法；
e）个人信息保护的改进和完善。

8 个人信息保护相关机构及职责

8.1 最高管理者

个人信息管理者的最高行政领导，应重视个人信息保护工作，并选择有能力的人员组建相应的机构，在资金、资源等各个方面提供完全的支持。

8.2 个人信息保护管理机构

个人信息保护管理机构负责个人信息管理者的个人信息保护工作。机构的主要职责包括：

a）开展个人信息保护工作的组织、实施；
b）个人信息保护基本规章、制度的制定；
c）个人信息保护宣传、教育；
d）个人信息保护情况的检查、改进、完善。

8.2.1 宣传教育

宣传教育应指定专人负责，在个人信息保护管理机构的指导下开展工作。宣传教育的主要职责是：

a）组织、实施个人信息保护宣传教育；
b）制定个人信息保护宣传教育制度、计划；
c）个人信息保护宣传策略和方法的制定；
d）个人信息保护相关知识、技术的培训、教育；
e）个人信息保护宣传教育的改进和完善。

8.2.2 服务支持

服务支持应指定专人负责，在个人信息保护管理机构的领导下开展工作。服务支持的主要职责应包括：

a）提供个人信息保护相关咨询和服务；
b）提供个人信息处理、使用建议和意见；
c）接受有关个人信息保护的意见，并落实和反馈；
d）沟通、交流；
e）个人信息保护相关事项、问题处理等的发布；
f）其它应处理的问题。

8.3 个人信息保护监察机构

应指定专门的个人信息保护监察负责人，可以在个人信息管理者内部选聘，或聘请社会人士担任。其职能是：

a）独立、公平、公正地开展个人信息保护监督、检查、调查工作；
b）制定个人信息保护监察制度和监察计划，并按计划实施监察；
c）编制监察报告，督促、建议个人信息保护的改进、完善。

9 个人信息保护管理机制

9.1 管理制度

应制定个人信息保护的规章和制度，包括基本的个人信息保护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。

9.1.1 基本规章

个人信息保护基本规章是个人信息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。基本规章主要包括以下各项：

a）个人信息保护相关机构职能及职责；
b）个人信息收集、处理、利用等的管理；
c）个人信息保护风险和安全管理措施；
d）个人信息数据库管理；
e）个人信息保护管理体系相关文档管理；
f）个人信息保护培训教育管理；
g）个人信息保护监察管理；
h）服务支持管理；
i）应急管理；
j）违反个人信息保护相关规章的处理；
k）其它必要的管理。

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、切实可行的个人信息保护细则。

9.1.3 其它管理规定

其它业务开展或有特殊要求的业务，涉及个人信息收集、处理，应制定相应的个人信息保护规定。

9.2 宣传

9.2.1 基本宣传

个人信息管理者应在其内部向全体工作人员及其它相关人员说明实施个人信息保护的重要性和管理策略，以得到工作人员及其它相关人员对个人信息保护工作的配合和重视。

9.2.2 业务宣传

个人信息管理者处理涉及个人信息的相关业务时，应主动说明实施个人信息保护的目的、措施、方法和规定，并做出保密承诺。

9.2.3 社会宣传

个人信息管理者应在相关媒介中增加个人信息保护的相关内容，如宣传资料、网络媒介（如网站、博客、播客等）及其它相关的面向社会的电子类、纸质等材料。

9.3 培训教育

9.3.1 计划

应根据人员、机构、业务、需求等实际情况，制定个人信息保护相应的培训和教育制度，适时开展个人信息保护培训教育。

9.3.2 对象

个人信息保护培训教育的对象，应包括：

a）工作人员；

b）临时员工；

c）其他相关人员。

9.3.3 内容

个人信息保护培训教育的主要内容，应包括：

a）个人信息保护相关法律、法规、规范、标准和管理制度；

b）个人信息保护的重要性和必要性；

c）个人信息保护培训教育对象的职能和责任；

d）违反个人信息保护相关标准可能引起的损害和后果。

9.4 公示

公开、公示个人信息，应征得个人信息主体同意。通知的内容应包括：

a）个人信息管理者的相关信息；

b）公示的目的、方式、范围和内容；

c）个人信息主体的权利；

d）公示和非公示的结果。

9.5 个人信息数据库管理

9.5.1 保存

个人信息主体应明确确认其个人信息是否以简明、易懂的语言记载、存储在个人信息数据库中，并可以清楚无误地提取、拷贝这些信息。

9.5.2 时限

个人信息管理者应为个人信息的存储、保存设定一个合理的时限，并与目的充分相关。

9.5.3 管理

个人信息管理者应履行第 5 章规定的义务，建立个人信息数据库管理机制。包括：

a）个人信息数据库管理和使用制度；

b）个人信息数据库管理者的职责；

c）权限和安全管理；

d）备份和恢复；

e）维护和记录；

f）事故处理。

9.5.4 备案

应建立备案登记制度，并有专人负责。记录应包括存储、保存的目的、时限、更新时间、获取方法、获取途径、位置、使用记录、使用目的、废弃原因和方法等。

9.5.5 安全性

个人信息管理者应保证个人信息数据库存储、保存的个人信息的准确性、完整性、保密性和可用性，并随时更新，以保证信息的最新状态。

9.6 保护体系文档

9.6.1 记录

应在个人信息保护体系实施过程中记录相关个人信息保护行为的目的、时间、范围、对象、方式方法、效果、反馈等信息。如培训教育、监察、宣传等。

9.6.2 管理

应建立与个人信息保护体系相关的规章、文件、记录、合同等文档的备案管理制度，并不断改进和完善。

10 保护实施

10.1 收集

10.1.1 目的

所有个人信息收集行为，必须具有特定、明确、合法的目的，并应征得个人信息主体同意，限定在收集目的范围内。

10.1.2 方法和手段

10.1.2.1 方式

收集方式主要包括：

a）主动收集：个人信息主体基于生活、工作需要主动提供。如购物（房、车等）、医疗、银行业务、电子商务等；

b）被动收集：个人信息主体不知情或不能控制情况下收集。包括：

- 采用各种网络技术和方法；
- 社会交往、商业经济等活动。

10.1.2.2 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，以保障个人信息主体的权力：

a）应将收集目的、范围、方法和手段、处理方式等清晰无误的告知个人信息主体，并征得个人信息主体同意；

b）被动收集时，应将收集目的、范围、内容、方法和手段、处理方式等以公告形式发布。如有疑义、反对，应停止收集；

c）个人信息主体应采用适当的措施，防止不正当收集个人信息。

10.1.3 类别

10.1.3.1 直接收集

直接从个人信息主体收集相关个人信息时，应征得个人信息主体同意。必须向个人信息主体提供的信息应包括：

a）个人信息管理者的相关信息；

b）个人信息收集、处理、利用的目的、方法；

c）接受并处理、利用该个人信息的第三方的相关信息；

d）个人信息主体拒绝提供相关个人信息可能会产生的后果；

e）个人信息主体的查询、修正、反对等相关权利；

f）个人信息安全和保密承诺。

10.1.3.2 间接收集

非直接地收集个人信息时，也应征得个人信息主体同意。间接收集必须保证个人信息主体利益不受侵害。必须提供的信息参照 10.1.3.1。

10.2 处理

10.2.1 同意

个人信息管理者处理个人信息之前，必须征得个人信息主体同意；或为履行与个人信息主体达成的合法协议的需要。

10.2.2 目的

个人信息管理者应在个人信息收集目的范围内处理、使用、利用个人信息，不可超出收集目的处理。

10.2.3 质量保证

个人信息管理者在处理个人信息时，应履行 5.4 款规定的义务，保证个人信息安全。

10.3 利用

10.3.1 提供

10.3.1.1 合法性

个人信息管理者所拥有的个人信息主体的相关个人信息，应是依特定、明确、合法的目的，经个人信息主体同意，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。

10.3.1.2 权益保障

个人信息管理者合法拥有的个人信息主体的相关个人信息，在向第三方提供时，应履行第 5 章个人信息管理者的义务，保障个人信息主体的合法权益。

10.3.1.3 授权许可

个人信息管理者向第三方提供个人信息主体的相关个人信息，应获得个人信息主体的授权，并在允许的目的范围内，采用合法、适当、适度的方法使用。

10.3.1.4 质量保证

第三方接受个人信息管理者提供的个人信息主体的相关个人信息，应履行 5.4 款的规定。

10.3.1.5 安全承诺

个人信息管理者向第三方提供个人信息主体的相关个人信息时，应获得第三方以书面形式（或以可见证的、有规范纪录的、满足书面形式要求的非书面形式）、保证个人信息的完整性、准确性、安全性的明确承诺，避免不正确使用或泄露。

10.3.2 委托

10.3.2.1 范围限定

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时，应在个人信息主体明确同意的，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，并将受托方相关信息提供给个人信息主体。提供的信息可参照 10.1.3.1。

10.3.2.2 委托信用

涉及个人信息委托业务时，应选择已建立个人信息保护体系的个人信息管理者，以建立相应的委托信用机制，保证不会发生个人信息泄露或个人信息滥用。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）个人信息保护安全措施和安全承诺；

d）再委托时的相关信息；

e）个人信息保护体系的相关说明；

f）个人信息相关事故的责任认定和报告；

g）合同到期后个人信息的处理方式。

10.3.3 其它

10.3.3.1 二次开发

分析、整合、整理、挖掘、加工等个人信息二次开发，应履行第 5 章个人信息管理者的义务，征得个人信息主体同意，并限定在个人信息主体同意的范围内，避免随意泄露、传播和扩散。通知的内容应包括：

a）个人信息管理者的相关信息；

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。

10.3.3.2 交易

个人信息交易应履行第 5 章个人信息管理者的义务，征得个人信息主体同意，并限制在个人信息主体同意的范围内处理使用，避免随意泄露、传播和扩散。通知的内容可参照 10.3.3.1。

个人信息交易的行为，包括：

a）基于某种利益关系的个人信息交换行为；

b）基于某种利益关系的个人信息出售行为。

10.4 使用

任何使用个人信息的行为，应履行第 5 章个人信息管理者的义务，征得个人信息主体同意，并限定在个人信息主体同意的范围内，避免随意泄露、传播和扩散。通知信息参照 10.1.3.1。

10.5 目的外处理

需要超目的范围处理、使用、利用个人信息时，应得到该个人信息主体同意。通知信息参照 10.1.3.1。

11 安全机制

11.1 风险管理

应在个人信息收集、处理、使用、利用过程中，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。

11.2 物理环境管理

应根据需要采取必要的措施，保证个人信息存储、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。

11.3 工作环境管理

应注意工作人员工作环境内所有相关的个人信息的保护，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。

11.4 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、传播个人信息的行为，构建规范、科学、合理、文明的网络秩序。

11.5 信息安全管理

应在整体信息安全体系建设中，充分考虑个人信息保护的特点，加强个人信息安全防护，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。

11.6 存储管理

保存个人信息的个人计算机系统、可移动存储媒介（电子、磁、纸、网络等介质及其它非自动处理介质）应确保个人信息存储的准确性、完整性、可靠性和安全使用。

11.7 使用管理

应根据个人信息自动和非自动处理的特点，制定相应的个人信息使用管理策略，包括访问/调用控制、权限设置、密钥管理等，防止个人信息的不当使用、毁损、泄露、删除等。

11.8 备份和恢复

应制定个人数据资料备份和恢复机制，并保证备份和恢复个人信息的完整性、可靠性和准确性。

11.9 人员管理

应明确与个人信息相关人员的权限、责任，加强相关人员的监察和管理，防止未经授权的个人信息接触。

11.10 备案管理

涉及个人信息相关资料的使用、借阅，应建立登记备案制度。登记应署真实姓名、部门、使用目的、使用方法及安全承诺。违反登记备案制度，应予以处罚，并承担赔偿责任。

12 监察

12.1 计划

应根据相关法律、规范和实际需求制定个人信息保护监察计划。

12.2 实施

应根据个人信息保护监察计划，定期独立、公平、公正地监控、检查、规范个人信息保护状况，并形成监察报告。

13 意见和反馈

个人信息管理者应对个人信息主体、监察人员及其它相关机构和人员提出的个人信息保护相关意见、建议、咨询等及时反馈，并采取相应的处理措施。

14 应急管理

个人信息管理者应制定应急预案，对收集、处理、使用、利用个人信息过程中可能出现的个人信息泄露、丢失、损坏、篡改、不当使用等事件进行评估、分析，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）事件的报告制度；

f）事件的责任认定。

15 例外

15.1 收集例外

不允许收集、处理、利用个人敏感信息。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。个人敏感信息包括：

a）有关思想、宗教、信仰、种族、血缘的事项；

b）有关人权、身体障碍、精神障碍、犯罪史及相关可能造成社会歧视的事项；

c）有关政治权利的事项；

d）有关健康、医疗及性生活的相关事项等。

15.2 法律例外

基于以下目的的例外，可以不必事先征得个人信息主体同意：

a）法律特别规定的；

b）保护国家安全、公共安全、国家利益、制止刑事犯罪；

c）保护个人信息主体或公众的权利、生命、健康、财产等重大利益等。

16 持续改进

个人信息管理者应依据相关法规、监察报告、需求变化、建议、投诉等，定期评估、分析个人信息保护体系运行状况，持续改进和完善个人信息保护体系：

a）分析、判断个人信息保护实施中的缺陷和漏洞；

b）制定预防和改进措施；

c）实时预防、改进；

d）跟踪改进结果。

17 评价

为提供个人信息保护的质量保证，应对个人信息管理者实施个人信息保护的状况进行评价，以确定其与个人信息保护相关法律、法规、规范的符合性、一致性和目的有效性，并以此作为颁发个人信息保护认证证书的依据。