DB

辽 宁 省 地 方 标 准

DB21/T 1522-2007

软件及信息服务业个人信息保护规范

Personal Information Protection Regulations for Software and Information Service Industry

2007-06-13 发布　　2007-08-01 实施

辽宁省质量技术监督局 发布

目　录

前　言

本标准是依据我国信息管理及信息安全相关法规和标准，并参考世界经济合作发展组织OECD《关于保护隐私和个人数据跨国流通指导原则》和日本JIS Q 15001-2006《个人信息保护管理系统—要求》制定的。

本标准由大连市信息产业局提出。

辽宁省信息产业厅归口。

本标准起草单位：大连软件行业协会、大连市质量技术监督局。

本标准主要起草人：孙鹏、薛源福、汤玉杰、王开红。

本标准2007年6月首次发布。

软件及信息服务业个人信息保护规范

1 范围

本标准规定了个人信息保护相关术语和定义，原则、负责人及责任、方针、风险分析与基本规章、运行与实施、检查、持续改进等单位个人信息保护体系建立所应具备的基本框架及要求。

本标准适用于软件及信息服务行业的企业、事业、社会团体等单位，其它相关行业可参照执行。

2 术语和定义

2.1 个人信息

个人信息是指业已存在的与个人相关的，并且可用于识别特定个人的信息。如：姓名、出生日期、分派给个人的号码、标志以及其它符号、可以识别个人的图像或生物信息等（包括某些单独使用时无法识别，但与其他信息进行对比后，能够由此识别特定个人的信息）。

2.2 信息主体

根据特定信息进行识别或者能够识别的对象。文中指拥有该个人信息的本人。

2.3 个人信息取得

是指为明确目的而获取个人信息的行为。

2.4 个人信息处理

是指利用计算机和相关配套设备及软件对个人信息进行录入、存储、编辑、修改、检索、删除、输出、传输和销毁等行为。

2.5 信息主体同意

信息主体对与自身相关的个人信息的取得以及使用表示同意,原则上以信息主体的签名、盖章为准，下述情况视为已取得信息主体同意：

a ）未成年人和无法对事情做出正确判断的成年人应由家长或监护人代表同意；

b ）在取得个人信息时，单位与信息主体签订的合同中规定了个人信息的使用，而且信息主体同意履行合同。

3 原则

3.1 取得与使用

个人信息取得应采用合理合法手段,并应征得信息主体的同意。个人信息取得和使用应有明确目的，不得超范围使用。

3.2 安全保障

应采取必要的安全保护措施，防止个人信息的丢失、泄漏、篡改和破坏等事件发生。除信息主体同意外，个人信息不得提供给第三方。

3.3 信息主体权利

信息主体有权确认个人信息状态。并拥有对个人信息提出删除、修改和完善的权利。

3.4 信息内容更新

个人信息应确保在使用目的范围内的正确性和完整性，并做到及时更新。

4 负责人及责任

建立和维护个人信息保护管理体系，须明确各负责人的权限及责任，形成文件并公布。

4.1 最高管理者

单位最高管理者应重视个人信息保护工作，选择有能力的人员作为个人信息保护负责人，并在资金和资源上给予支持。

4.2 个人信息保护负责人

单位个人信息保护负责人负责单位个人信息保护工作的开展；组织制定与实施基本规章制度；组织各部门个人信息保护责任人共同制定部门管理细则；指导培训教育工作的开展；负责检查单位个人信息保护运行状况并写出报告。

4.3 监查负责人

单位应设置专门的个人信息保护监查负责人，监查负责人可以在本单位内部选拔任命，也可以由外面聘请。监查负责人应具有独立性，并站在客观、公正的立场上开展工作。监查负责人负责制定监查规定和监查计划，按照计划对单位个人信息保护情况进行监查，负责写出监查报告并提出改进意见。

4.4 培训教育负责人

单位应任命个人信息保护培训教育负责人，负责制定培训教育规定和培训教育计划，并负责计划的实施。

4.5 客户负责人

单位应任命客户负责人，负责接受客户或消费者的意见和建议，提出处理意见并促进意见的落实和反馈，在出现问题时负责与客户或消费者沟通，讨论解决办法。

4.6 其它责任人

单位应指定各部门的个人信息保护责任人，负责制定和实施本部门个人信息保护工作管理细则。

5 方针、风险分析与基本规章

5.1 方针

由个人信息保护负责人制定本单位个人信息保护方针，方针应以简洁、明确的语言予以阐述。方针的制定应注意以下事项：

a）内容应是符合单位实际情况的个人信息保护原则和基本措施；

b）遵守国家相关法律、法规；

c）符合本规范的要求。

个人信息保护方针应让本单位所有人员知道、理解和执行，并向社会公布。

5.2 风险分析

单位应对所有已经涉及到和可能涉及到的个人信息进行确认，并制作个人信息风险分析流程图，通过流程图对个人信息的取得、使用、传输、委托、保管过程中可能会出现的问题予以确认和分析，制定风险对策和措施，为个人信息保护规章的建立提供参考。

5.3 基本规章

单位应根据本规范要求和单位实际情况，参考风险分析流程图的分析，建立以下个人信息保护相关基本规章，并持续改进：

a）个人信息保护组织机构与责任规定；

b）个人信息取得、使用、提供、委托、处理等管理规定；

c）个人信息安全保护措施及文档管理规定；

d）个人信息保护培训教育规定；

e）个人信息保护监查规定；

f）违反个人信息保护规章制度的处罚规定。

6 运用与实施

6.1 宣传

6.1.1 对内

应向本单位全体员工宣传个人信息保护的重要性。

6.1.2 对外

应向社会宣传本单位的个人信息保护方针，在承接有个人信息的业务时，应主动向客户和消费者宣传本单位个人信息保护的措施和规定。

6.2 部门管理细则

6.2.1 制定

部门应根据本部门特点制定具体的个人信息保护措施，部门管理细则应与单位基本规章相一致，应切实可行，应要求每一个具体操作人员完全理解和遵照执行。部门管理细则的实施需获得本单位个人信息保护负责人的批准。

6.2.2 实施

部门管理细则由部门个人信息保护责任人负责组织实施。

6.3 个人信息取得

6.3.1 范围

单位应在个人信息取得之前明确使用目的，并征得信息主体同意，在限定的目的范围内取得。从已公开资料中取得个人信息时也应明确使用目的。

6.3.2 方法与手段

个人信息应采取科学、规范的方法和合理、合法的手段取得。

6.3.3 直接取得个人信息的告知

直接从信息主体取得个人信息时，应以书面或能代替书面的形式告知并征得信息主体的同意，告知信息主体的内容应包括：

a）取得个人信息的单位名称、信息管理者名称、职务、部门、联系电话；

b）使用目的；

c）如果将信息提供给第三者时，应明确下列事项：

——提供给第三者的目的；

——提供个人信息的项目；

——提供手段和方法；

——接受该个人信息的人或组织的种类和属性；

——如果有个人信息使用及委托的相关合同，需注明其主要内容。

d）委托保管个人信息时的信息接受者及个人信息保管合同；

e）信息主体如果拒绝提供自身个人信息可能会产生的后果。

6.3.4 间接取得个人信息的告知

间接取得个人信息时，应以书面或能代替书面的形式告知信息主体，并征得信息主体的同意，但以下情况除外：

a）信息主体已明确使用目的；

b）在保证信息主体利益不受侵害时，将被委托保管的个人信息用于对外委托的业务；

c）将使用目的通知信息主体或者公布可能会危及信息主体或者第三者的生命、身体、财产安全以及其它利益：

d）将使用目的通知信息主体或者发布时可能会造成取得单位的权利或正当利益受到损害；

e）根据国家法律、法规所必须执行的公务，通知信息主体或者发布可能会影响到公务的执行。

6.4 使用与提供

个人信息应在明确的目的范围内使用与提供。

在超出使用目的范围使用和提供时,应事先征得信息主体的同意,告知内容按照 6.3.3 的要求执行。但以下情况除外：

a）有相应的法律法规规定；

b）信息主体或公众的生命、健康、财产的重大利益需要保护；

c）为了开展公共卫生事业等特殊工作，不便征得信息主体同意；

d）根据国家法律、法规所必须执行的公务，通知信息主体或者发布可能会影响到公务执行。

6.5 委托

6.5.1 范围限定

对于委托业务中被委托保管的个人信息，应在信息主体同意的使用目的范围内或委托方提出的（合同或其它方式）使用目的范围内对信息进行处理，不可超范围使用和提供。

6.5.2 条件与监督

对于包含个人信息的委托处理业务，应制定相应的标准，选择能对个人信息实施充分保护的单位，进行适当的监督，并在委托合同中规定如下内容：

a）明确委托及受委托者责任；

b）个人信息的安全管理事项；

c）再委托时的相关事项；

d）个人信息使用状况及委托者要求报告的事项；

e）有关个人信息保护的条款；

f）违反合同时的处理办法；

g）发生事故时的责任及报告事项；

h）合同期满后，个人信息的处理办法。

6.6 信息主体权利保障

6.6.1 信息主体权利

信息主体对自身个人信息的保存和使用状况具有知情权，有权对其提出合理、合法的修改、删除和公开要求，有权确认、提取、拷贝自身的个人信息，有权对自身个人信息的使用目的提出反对意见。

6.6.2 告知义务

单位应将个人信息的使用目的、不提供信息的后果、查询和更正自身个人信息的权利告知信息主体。

6.6.3 信息主体意见与反馈

在信息主体对自身个人信息提出要求时，单位要及时做出回应，并采取相应措施。

6.6.4 个人信息公示

6.6.4.1 告知

公示个人信息时应征得信息主体同意。单位需要公示个人信息时，应以书面或能代替书面的形式告

知信息主体，内容包括：

a）公布个人信息的单位名称及管理者名称；

b）个人信息的使用目的；

c）信息主体对自身个人信息公示拥有的权利；

d）同意或者不同意公示可能产生的后果。

6.6.4.2 不应公示的条件

a）危及信息主体或第三者生命、身体、财产安全及正当利益；

b）影响单位业务的正常开展；

c）违反国家法律、法规。

出现上述情况时不应采用公示，但可采取适当方法通知信息主体：

6.6.4.3 信息主体对个人信息公示的权利

信息主体有权对公示的自身个人信息提出修改、增加、删除、公示和停止公示的要求，单位应对信息主体的要求给予及时反馈及妥善处理。

6.7 管理

6.7.1 保管

单位应在信息主体同意的使用目的范围内，以信息主体同意的形式正确及时地保管个人信息，应对个人信息的安全负全责。个人信息应有专人负责保管和记录，登记项目应包括业务类型、信息存放位置、保管期限、取得方法、取得途径、提供目的、废弃方法。

6.7.2 完整性与可用性

单位要保证所保管的个人信息在使用目的范围内的完整性与可用性，并及时更新。

6.7.3 文档

单位应对个人信息管理体系的规章、文件、计划、记录、合同等文档建立管理制度，随时更新及完善。

6.7.4 从业人员

单位应对使用个人信息的工作人员进行必要的监督和管理。

6.7.5 安全保护措施

单位应参照国家有关信息安全管理标准及法规，对本单位拥有的个人信息采取必要的安全保护措施。包括采取物理和技术手段。

6.7.5.1 权限

明确本单位涉及个人信息工作的相关人员的权限及责任。

6.7.5.2 网络与设备

对本单位计算机、网络、服务器及相关设备应采取安全防护措施，包括访问及存取控制、密钥管理、权限设置等，防止对个人信息的不当存取、非法修改、破坏、泄漏和删除等。

对外部网络和电子邮件的信息交换过程，须采取必要的预防措施，防止非法入侵和病毒破坏等。

6.7.5.3 数据备份

单位应对个人信息数据采取备份和数据恢复等保护措施，防止个人信息的破坏和丢失。

6.7.5.4 存储

对本单位存有个人信息的计算机、存储设备及其它介质要确保安全使用、妥善保存和处置。

6.7.5.5 紧急事件的预防与处理

单位应针对可能发生的个人信息丢失、泄漏、损坏事件和可能造成的经济损失及不利影响进行分析，制定相应的预防措施和处理方案：

a）制定处理流程；

b）迅速将个人信息泄漏、丢失和破坏的情况通知信息主体；

c）应把事件的发生原因、相关影响以及责任及时公布；

d）建立应急机制，制定应急方案。

6.8 培训与教育

6.8.1 实施

单位每年应制定个人信息保护培训教育计划，并对全体员工进行培训教育，培训对象应包括正式员工、临时员工和在本单位工作的其它人员等。教育内容应包括：

a）个人信息保护的重要性;

b）员工在单位个人信息保护中的职能及责任;

c）违反个人信息保护规章可能引起的损害和后果。

6.8.2 记录

对每次培训教育应有记录，内容包括培训时间、地点、教材、教师、参加人员、培训效果及员工反馈等。

6.9 意见与反馈

单位对信息主体和客户在个人信息保护方面提出的意见、建议和咨询要及时做出反馈和适当处理，并记录和保存。

7 检查

7.1 内部检查

个人信息保护负责人应定期或不定期检查本单位个人信息保护状况，形成检查报告，报送最高管理者。

7.2 监查

7.2.1 实施

监查负责人应制定监查计划，定期或不定期对单位个人信息保护状况进行监查，形成监查报告，报送最高管理者。

7.2.2 记录

每次监查都应有监查记录，内容包括：监查对象、目的、范围、时间、结果等。监查记录和监查报告由本单位保存。

8 持续改进

8.1 不符合事项的处理与预防

最高管理者应根据个人信息保护负责人和监查负责人提供的报告和业务发展情况,对不符合个人信息保护的事项进行改进，并修改完善预防措施。处理不符合事项的工作流程：

a）不符合事项的确认；

b）分析发生不符合事项的原因，制定改进办法和预防措施；

c）限定期限进行改进；

d）对不符合事项的改进过程及修订的预防措施记录备案；

e）对改进结果及修订的预防措施进行评估。

8.2 定期评估

应对本单位个人信息保护体系进行定期评估、不断改进和完善。在改进与完善过程中应参考以下内容：

a）监查负责人和个人信息保护负责人的报告；

b）投诉及内部、外部的意见及建议；

c）对每次改进和修订后执行情况的跟踪；

d）国家相关法律、法规的颁布和修改；

e）社会形势、公众意识、技术进步的变化；

f）单位业务领域及经营范围的变化。