大连软件及信息服务业个人信息保护规范

1 适用范围

适用于利用计算机及其相关和配套设备（含网络），按照一定的应用目的和规则对信息进行收集、加工、存储、传输、检索等处理业务的企业、事业、社会团体等单位。

2 定义

2.1 个人信息

个人信息是指存在的与个人相关的，并且可用于识别特定个人的信息。包括姓名、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声音等（包括某些单独使用时无法识别，但能与其他数据进行对照参考，并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。这里指拥有该个人信息的本人。

2.3 个人信息取得

是指为建立个人信息资料而取得个人信息的行为。

2.4 个人信息处理

是指利用计算机或软件对个人信息进行录入、存储、编辑、修改、检索、删除、输出、传输或其它处理的过程。

2.5 个人信息使用

指单位将自己拥有的个人信息在单位内部使用或提供给第三者。

2.6 个人信息委托

单位为了委托信息处理业务，而将自己拥有的个人信息委托给第三者。

2.7 信息主体同意

信息主体对与自己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和口头承诺为准，下述情况包括在默认范围之内：

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；

b 信息主体已经确切得到了通知，而且没有表示反对；

c 在取得个人信息时，信息管理者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

个人信息应遵循以下原则加以保护。

3.1 取得和使用

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。个人信息取得应有明确目的，不得超范围使用。

3.2 安全保障

应采取合理的安全保护措施，避免个人信息的丢失、泄漏、篡改和破坏等现象发生。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所在。信息主体有权对个人信息提出删除、修改和完善。

3.4 信息内容最新状态

个人信息应确保在目的范围内的正确性和完整性，并保持最新状态。

4 负责人及责任

为了建立和维护个人信息保护管理体制，应明确各责任人的权限及责任，形成文档，并让从业者周知。

4.1 单位领导者

单位领导者应重视个人信息保护工作，选择有能力的人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

4.3.1 监查负责人的指定

单位应设置专门的个人信息保护监查负责人，监查负责人可以在单位内部指定，也可以从外面聘请。监查负责人应具有独立性，并站在公平、公正的立场上开展工作。

4.3.2 监查负责人的责任

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 客户窗口负责人

单位应指定客户窗口负责人，负责接受客户或消费者的意见和建议；提出处理意见和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和讨论补偿办法。

4.6 其它负责人

单位应指定各部门的个人信息保护负责人，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单位个人信息保护方针，方针应以简洁、明确的语言阐明单位个人信息保护的政策与基本措施。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 不能违背国家相关法律、法规；

c 符合本规范的要求。

个人信息保护方针应让单位所有人员知道、理解和执行，并向社会与公众公布。

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流程图，通过流程图对单位个人信息取得、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，为单位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，并维持及改进：

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 个人信息保护技术物理安全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

向全体员工宣传个人信息保护的重要性和策略，以得到员工对个人信息保护工作的配合和重视。

6.1.2 对外

在单位宣传资料或网站上增加个人信息保护相关内容。在承接有个人信息的业务时，应主动向客户和消费者宣传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

部门管理细则是单位各部门根据本部门特点而制定的具体个人信息保护措施，部门管理细则应与单位基本规章相一致，应切实可行，而且要求每一个具体操作人员可以理解和执行。部门管理细则最终要得到单位个人信息保护负责人的同意。

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实施。

6.3 个人信息取得

6.3.1 范围

个人信息取得之前应明确使用目的，并应征得信息主体的同意，在限定的目的范围内取得。从被公开的资料中取得个人信息时也应明确使用目的。

6.3.2 方法和手段

个人信息取得应采取适当的方法和合法、公正的手段。

6.3.3 限制

限制取得下列内容的个人信息（不包括信息主体明确同意或法律有特别规定的情况下）：

a 有关思想、信仰、宗教的事项；

b 有关人权、身体障碍、精神障碍、犯罪史及相关能造成社会歧视的事项；

c 有关政治权利的事项；

d 有关保健医疗及性生活的事项。

6.3.4 直接从信息主体取得个人信息

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通知信息主体，并征得信息主体的同意，通知信息主体的内容应包括：

a 企业名称、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，需注明其大体内容。

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信息可能会产生的后果。

6.3.5 间接取得个人信息

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

a 在信息主体已明确使用目的的情况下；

b 对外委托的业务而被委托保管的个人信息，应保证信息主体的利益不被侵害；

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、财产以及其它利益的情况下；

d 将使用目的通知信息主体或者发布可能会造成单位的权利或者正当利益受到损害的情况下；

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执行的情况下。

6.4 个人信息使用和提供

6.4.1 范围限定

个人信息的使用和提供应在使用目的范围之内，不可超出使用目的范围。

6.4.2 目的范围外使用和提供

在超出使用目的范围外使用和提供时，应事先征得信息主体的同意,并按照 6.3.4 的要求事项，以书面形式或代替书面形式的方式通知信息主体。但在下述情况下可以不征得信息主体的同意：

a 在相应的法律法规规定的情况下；

b 在信息主体或公众的生命、健康、财产的重大利益需要保护的情况下；

c 在为了维护公共卫生和推进儿童健康事业，由于某种原因很难得到信息主体同意的情况下；

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的情况下。

6.5 个人信息委托

6.5.1 范围限定

对于委托业务中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，不可随意使用和提供。

6.5.2 委托条件与监督

对于委托信息处理业务而需要寄存的个人信息，应制定统一标准，选择个人信息保护能力较强的单位并进行适当的监督，应在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向委托者报告的要求事项；

e 合同中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，个人信息的返还和消除。

6.6 保障信息主体权利

6.6.1 信息主体权利

信息主体有权知道自身信息所在位置，有权对自身信息提出修改、删除和公开的要求，有权确认、提取、拷贝自身个人信息，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

个人信息管理者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诉信息主体。

6.6.3 信息主体意见及反馈

在信息主体对自身信息提出要求的情况下，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

公示个人信息时应得到信息主体同意。单位由于适当原因需要公示个人信息时，应将下列事项以书面形式或信息主体容易得到的方式通知信息主体：

a 单位名称及管理者名称；

b 个人信息的使用目的；

c 信息主体对于公示信息的权利；

d 如果要求公示或者不同意公示可能产生的后果。

下列情况下可以不公示或者不一定必须通知信息主体，但也要尽可能通知信息主体，并说明其理由：

a 危及信息主体或第三者生命、身体、财产及正当利益时；

b 影响到单位业务的合理运行时；

c 违反法律法规时。

6.6.4.2 信息主体对公示个人信息的权利

信息主体有权对公示的自身信息提出修改、增加、删除、公示和停止公示的要求，个人信息管理者应对信息主体的要求给予及时的反馈及合理的处理。

6.7 管理

6.7.1 保管

个人信息管理者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。个人信息的保管应有明确的记录和专人负责，记录应包括业务类型、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 完整性和可用性

个人信息管理者要保证所保管的个人信息在使用目的范围内的完整性和可用性，并对信息随时更新，以保证信息的最新状态。

6.7.3 文档

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

6.7.4 从业人员

为了保证个人信息安全,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 技术和物理安全保护措施

单位应对本单位拥有的个人信息采取合理的安全保护措施。个人信息安全保护措施应参照国家有关信息安全管理标准及法规制定。安全保护措施至少应包括。

6.7.5.1 权限

明确个人信息接触人员的权限及责任，加强对相关人员的管理，防止无权者对个人信息的接触。

6.7.5.2 网络与设备

对计算机、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，要研究特别的预防措施，防止非法入侵和病毒破坏等。

6.7.5.3 数据备份

对个人信息数据应采取备份和数据恢复等措施，防止个人信息的破坏和丢失。

6.7.5.4 存储

对保存有个人信息的计算机及活动介质（包括磁带、磁盘、笔记本、输入和输出介质、程序清单、测试报告和系统文档等）要确保安全使用、保存和处置。

6.7.5.5 紧急事态的预防及处理

单位应针对可能发生个人信息丢失、泄漏、损坏事件和可能造成的经济损失和不利影响进行分析，制定相应的预防和处理措施：

a 建立处理对应流程，使其在事件发生时，把损失降到最低；

b 迅速通知泄漏、丢失和破坏的个人信息的信息主体，或者让信息主体得知事态情况；

c 为了防止类似事件的再次发生，尽可能把事件的关联、发生原因以及责任在第一时间公布；

d 建立事件关联、发生原因以及对策的相关机制。

6.8 培训与教育

6.8.1 实施

单位应制定个人信息保护培训教育计划，按照培训教育计划对全体员工进行个人信息保护的培训教育，培训对象应包括正式员工、临时员工、派遣人员等。教育的内容应包括：

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，记录应包括培训时间、地点、教材、教师、参加人员、培训效果及员工反应等内容。

6.9 意见及反馈

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随时检查单位个人信息保护状况，并对检查结果定期形成单位个人信息保护制度运行状况报告，报单位领导者。

7.2 监查

7.2.1 实施

监查负责人应制定监查计划，并按照监查计划对单位个人信息保护状况进行监查，对监查结果做出监查报告，提供给单位领导者。

7.2.2 记录

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

8 持续改善

8.1 不符合事项的处理及预防

单位领导者要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，建立预防措施。对不符合事项处理和预防措施建立如下流程：

a 不符合事项的确认；

b 发生不符合事项的原因分析，改进办法和预防措施；

c 限定期限进行改进及完善；

d 对不符合事项改进及预防措施的记录；

e 对改进及预防措施结果的评估。

8.2 重新评估

为了使单位个人信息得到良好的保护，应定期对单位个人信息保护规章制度进行重新评估、不断改进和完善。在改进与完善时应参考以下事项：

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 对上次更新结果的跟踪；

d 国家相关法律、法规的颁布和修改；

e 社会形式、公众意识、技术进步的变化；

f 企业业务领域及范围的变化。