ICS 35.240.99
A 90
备案号:51181—2015

YZ

中华人民共和国邮政行业标准

YZ/T 0147—2015

寄递服务用户个人信息保护指南

Guide on Personal Information Protection of Posting and Delivery Service Users

2015-09-15 发布　　2016-01-01 实施

国家邮政局　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由国家邮政局提出。

本标准由全国邮政业标准化技术委员会(SAC/TC 462)归口。

本标准起草单位:国家邮政局发展研究中心。

本标准主要起草人:冯力虎、王学斌、耿艳、王梦影等。

寄递服务用户个人信息保护指南

1 范围

本标准规定了寄递服务用户个人信息(以下简称寄递用户信息)的组成、信息保护的基本原则及信息保护的具体要求。

本标准适用于邮政企业、快递企业和其他从事寄递服务的企业(以下统称寄递企业)所涉及的寄递用户信息保护工作。

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 18894—2002 电子文件归档与管理规范

GB/T 22239—2008 信息安全 信息系统安全等级保护基本要求

YZ 0139—2015 邮政业安全生产设备配置规范

YZ/T 0142—2015 邮政业信息系统安全等级保护定级指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

寄递服务用户个人信息 personal information of posting and delivery service users

用户在使用寄递服务过程中的个人信息。寄递用户信息可以分为个人敏感信息和个人一般信息。

3.2

个人敏感信息 personal sensitive information

一旦遭到泄露或修改,会对标识的用户造成安全隐患或不良影响的寄递用户信息。个人敏感信息包括寄(收)件人的姓名、地址、身份证件号码、电话号码、物品名称、物品价值等。

3.3

个人一般信息 personal general information

除个人敏感信息以外的寄递用户信息。

3.4

信息处理 personal information handling

处理寄递用户信息的行为,包括纸质信息和电子信息的收集、传输与保管、使用、销毁等。

3.5

纸质信息载体 paper information carrier

以纸质材料为载体,记录、传输、保存寄递用户信息的信息媒介。

3.6

电子信息载体 electronic information carrier

以胶片、磁带、磁盘、光盘、移动硬盘、网络硬盘等光电磁化材料为载体,记录、传输、保存寄递用户信

息的信息媒介。

4 信息组成

寄递用户信息主要由以下两部分组成：

a) 身份信息，指能够表明个人身份的基本信息，包括寄(收)件人的姓名、地址、身份证件号码、电话号码等。

b) 业务信息，指寄递企业向用户提供寄递服务过程中所生成的业务信息，包括物品名称及价值等。

5 信息保护基本原则

5.1 合理必要

应以确保完成寄递服务为目的，只处理与处理目的有关的必要信息，不随意扩大处理范围。

5.2 个人同意

以明确、易懂的方式如实向用户告知个人信息的处理目的、收集内容、使用范围和保管期限等信息，并征得用户同意。

5.3 安全保障

采取必要、适当的管理措施和技术手段，保护寄递用户信息安全，防止不当使用、随意泄露或者非法向他人提供寄递用户信息。

5.4 责任明确

明确寄递用户信息处理过程中各参与方的责任，采取相应的措施落实相关责任，并对寄递用户信息处理过程进行记录以便于追溯。

6 信息保护具体要求

6.1 概述

寄递企业对寄递用户信息的保护可分为组织层面、流转层面、信息系统层面等三个层面。

6.2 组织层面

6.2.1 依照国家法律、法规和本标准，制定寄递用户信息保护管理制度，落实寄递用户信息保护管理责任及奖惩措施。

6.2.2 指定专门人员或部门负责寄递用户信息的保护工作，并接受用户的投诉与建议。

6.2.3 对信息处理人员的身份、背景、专业资格和资质进行审查，并签订信息安全责任承诺书。

6.2.4 制订寄递用户信息保护的教育培训计划并组织落实，对教育培训情况和考核结果进行记录。

6.2.5 建立寄递用户信息保护的监督检查机制，定期对寄递用户信息的安全状况、保护制度及措施的落实情况进行监督检查，并形成监督检查报告。

6.2.6 制定应急预案，对收集、传输与保管、使用、销毁寄递用户信息过程中可能出现的寄递用户信息泄露、丢失、损毁、篡改、不当使用，出售或者非法向他人提供等事件进行评估、分析，采取相应的预防措施。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) 事件的报告制度；
e) 事件的责任认定及追究。

6.2.7 应依据相关法规、投诉、建议、检查报告等情况，定期评估、分析企业内部寄递用户信息保护制度运行状况，持续改进和完善寄递用户信息保护制度：

a) 分析、判断寄递用户信息保护实施中的缺陷和漏洞；
b) 实施应急预防，改进运行机制；
c) 跟踪改进效果。

6.2.8 寄递企业通过委托方式开展寄递服务的，应充分审查、评估受托方保护寄递用户信息的能力，并签订寄递用户信息安全保障协议。协议内容应包括：

a) 双方的权利和责任；
b) 寄递用户信息的使用目的和使用范围；
c) 寄递用户信息安全承诺和保护措施；
d) 寄递用户信息相关事故责任认定和追究方式；
e) 服务协议到期后寄递用户信息处理方式。

6.3 流转层面

6.3.1 概述

寄递企业对寄递用户信息的保护应贯穿于用户信息的收集、传输与保管、使用、销毁等各个阶段。

6.3.2 信息收集

6.3.2.1 收集寄递用户信息前应通过寄递单式、网站、合同等书面形式向用户明确告知以下事项：

a) 寄递用户信息的收集目的、收集内容和保管期限；
b) 寄递用户信息的使用范围；
c) 用户提供个人信息不详或错误可能导致的后果。

6.3.2.2 收集能够确保完成寄递服务的必要信息，不应收集与业务无关的其他信息。

6.3.3 信息传输与保管

6.3.3.1 纸质信息的传输与保管应满足以下要求：

a) 收寄或投递时，应将纸质信息载体放置于业务人员视线范围内或者有保管措施的区域；收寄或投递完成后，宜在当日将纸质信息载体送交营业场所保管。
b) 传输过程中，宜采用遮盖、涂抹等方式部分隐藏寄递单式上的寄(收)件人的姓名、身份证件号码、物品名称、物品价值等敏感信息；信息技术支撑能力较强的企业，可采用在寄递单式上打印或印制特定条码和代码等方式，代替寄递用户个人敏感信息。
c) 在邮件、快件处理场所，严格执行寄递用户信息保护管理制度，无关人员不应出入处理场地。
d) 纸质信息载体应集中封闭存放，由专门人员负责保管，无关人员不应出入存放地。
e) 内部人员查阅纸质信息载体时，应做好查阅登记，不应私自复制或将纸质信息载体带离存放地。
f) 纸质信息载体存放地应按照 YZ 0139 的要求配备安全生产设备。

6.3.3.2 电子信息的传输与保管应满足以下要求：

a) 对电子信息进行传输前，应对电子信息附加标识以便追溯责任主体；

b) 通过开放公共网络传输寄递用户信息时，应采取加密措施；
c) 电子信息的归档应符合 GB/T 18894 的要求；
d) 使用独立物理区域存储寄递用户信息，非授权人员不应访问该区域；
e) 指定专门人员负责电子信息存储设备和介质的管理，使用和借用存储设备和介质应获得批准并进行登记；
f) 定期开展本地备份、异地备份和电子信息恢复测试，确保数据安全可用。

6.3.4 信息使用

6.3.4.1 对信息使用人员分配最小操作权限，仅限于访问其职责范围内的寄递用户信息。信息使用人员离职或调岗时，应及时关闭、删除或调整该人员在相关信息系统中的操作权限。

6.3.4.2 对寄递用户信息的使用过程进行记录，保证寄递用户信息在使用过程中不被与处理目的无关的个人、组织和机构获知。

6.3.4.3 在对寄递用户信息进行聚合、分类、比对、分析时，应对个人敏感信息进行脱敏处理，并限制脱敏信息的使用范围和用途。

6.3.4.4 用户发现其个人信息存在缺陷、影响服务合同正常履行并要求修改时，要根据用户的要求进行核查，在保证寄递用户信息完整性的前提下，修改或补充相关信息。

6.3.5 信息销毁

6.3.5.1 建立寄递用户信息销毁管理制度，对销毁日期、销毁地点、销毁人员、销毁寄递用户信息种类和内容、销毁数量等进行记录、归档和保存。

6.3.5.2 纸质信息载体保管期满或电子信息载体报废的，应按有关规定及时销毁寄递用户信息。

6.3.5.3 寄递用户信息应进行集中销毁。销毁时，应由两名以上专门人员共同完成。

6.3.5.4 当销毁寄递用户信息可能会影响执法机构调查取证时，应采取适当的存储和屏蔽措施。

6.3.5.5 寄递企业停止经营时，应按有关规定及时销毁寄递用户信息。

6.4 信息系统层面

6.4.1 信息系统的安全保护应符合 GB/T 22239 和 YZ/T 0142 等相关要求。

6.4.2 信息系统的权限管理应满足以下要求：

a) 分别设置系统管理权限、业务操作权限和安全管理权限，并赋予各类权限单独的账号；
b) 系统管理权限只进行用户管理、权限管理、配置定制等系统级的管理，不应进行业务操作；
c) 业务操作权限只进行业务操作，不应具备任何系统级的管理权限；
d) 安全管理权限只对系统中所有的安全功能进行管理，以监督和查证系统管理权限和业务操作权限的正常行使。

6.4.3 信息系统的修补或升级应满足以下要求：

a) 定期对网络进行漏洞扫描，对于发现的漏洞，应在经过风险评估、验证测试后进行修补或升级，并进行记录；
b) 如需安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中通过测试，并对重要文件进行备份后，方可实施系统补丁程序的安装，并对系统变更进行记录。

6.4.4 涉及个人敏感信息的信息系统应采取保密措施，确保其开发与实施安全，不应将个人敏感信息用于开发和测试。

参 考 文 献

[1] GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南
[2] GB/T 27917.1—2011 快递服务 第1部分:基本术语
[3] GB/Z 28828—2012 信息安全技术公共及商用服务信息系统个人信息保护指南
[4] 中华人民共和国主席令2012年第70号 中华人民共和国邮政法
[5] 中华人民共和国主席令2013年第7号 中华人民共和国消费者权益保护法
[6] 全国人民代表大会常务委员会关于加强网络信息保护的决定(2012年12月28日)
[7] 中华人民共和国交通运输部令2011年第2号 邮政行业安全监督管理办法
[8] 寄递服务用户个人信息安全管理规定(2014年3月27日)