ICS 35.240.99
A 90
备案号:87942—2023

YZ

中华人民共和国邮政行业标准

YZ/T 0189—2023
代替 YZ/T 0147—2015

寄递服务用户个人信息保护要求

Requirement on personal information protection of posting and delivery service users

2023-01-04 发布　　2023-04-01 实施

国家邮政局　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由国家邮政局提出。

本文件由全国邮政业标准化技术委员会(SAC/TC 462)归口。

本文件起草单位：中国—东盟信息港股份有限公司、中国标准化研究院、广西东信易通科技有限公司、东信网安(深圳)科技有限公司、厦门通程物流有限公司。

本文件主要起草人：吕超源、曾毅、刘作、黎聪、陈智勇、熊莹、朱其剑、魏林锋、李俊峰。

寄递服务用户个人信息保护要求

1 范围

本文件规定了寄递服务用户个人信息范围,基本要求,个人信息收集,个人信息存储、销毁及删除,个人信息使用,个人信息的提供,个人权利的实现,个人信息安全事件处置以及个人信息保护技术的应用等内容。

本文件适用于寄递服务用户个人信息保护工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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。

ISO/IEC 18000-6C 信息技术 项目管理的射频识别 第6部分:860 MHz ~ 960 MHz 空中接口通信参数(Information technology—Radio frequency identification for item management—Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General)

GB/T 10757 邮政业术语

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 27917.1 快递服务 第1部分:基本术语

GB/T 29768 信息技术 射频识别 800/900 MHz 空中接口协议

GB/T 35273—2020 信息安全技术 个人信息安全规范

3 术语和定义

GB/T 10757、GB/T 27917.1 界定的以及下列术语和定义适用于本文件。

3.1

个人信息 personal information

以电子或者其他方式记录的、与已识别或者可以识别自然人有关的各种信息。

注1:个人信息包括姓名、出生日期、身份证件号码、住址、联系方式等。

注2:不包括匿名化处理后的信息。

[来源:GB/T 41479—2022,3.6,有修改]

4 缩略语

下列缩略语适用于本文件。

RFID:射频识别(Radio Frequency Identification)

App:移动互联网应用程序(Mobile Internet Application)

OTP: 一次性口令(One Time Password)

5 寄递服务用户个人信息范围

5.1 寄递服务用户个人信息应符合相关法律法规和国家标准、行业标准的规定,应限于实现处理目的的最小范围。

5.2 提供寄递服务所必要的寄递服务用户个人信息包括:

a) 寄件人姓名、地址、联系电话、证件类型和号码等;
b) 收件人姓名、地址、联系电话等;
c) 寄递物名称、类别、数量等。

5.3 除5.2外,提供国际寄递服务所必要的寄递服务用户个人信息还包括收件人证件类型、证件号码等。

6 基本要求

6.1 组织建设

关键信息基础设施运营者,以及从事国际寄递、港澳台寄递、省际、省内异地寄递业务的企业,应设立专门的个人信息保护工作部门,配备专职的个人信息保护工作人员;其他寄递企业应配备专职的个人信息保护工作人员。

6.2 人员要求

6.2.1 负责个人信息保护的人员

寄递企业负责个人信息保护的人员应满足以下要求:

a) 寄递企业的主要负责人应对个人信息安全负全面领导责任,包括为个人信息保护工作提供人力、财力、物力保障等;
b) 个人信息保护工作部门负责人应具备较强的个人信息保护知识和相关管理工作经历,个人信息保护工作人员应具备相应的专业知识;
c) 关键信息基础设施运营者个人信息保护部门负责人和关键岗位人员应接受安全背景审查。

6.2.2 一般从业人员

对一般从业人员,寄递企业应满足以下要求:

a) 明确内部涉及个人信息处理一般从业人员的安全职责,确定相应的权限,建立相应的内部制度;
b) 与快递员、邮递员、邮件快件处理员等能接触个人信息的从业人员签署保密协议;
c) 对营业场所、处理场所负责人以及具备大量访问、导出、删除身份证件等敏感个人信息权限的管理人员进行安全背景审查;
d) 定期(至少每年一次)和在个人信息保护政策发生重大变化时,对相关人员开展个人信息安全专业化培训和考核。

6.3 制度建设

寄递企业应建立健全个人信息保护制度,包括但不限于:

a) 个人信息保护政策及相关规程;
b) 个人信息安全影响评估制度;
c) 个人信息安全管理及报告制度;

d） 个人信息投诉管理制度和用户个人权利保障制度；
e） 个人信息安全事件处罚制度；
f） 个人信息安全应急处置及报告制度。

6.4 场所要求

寄递企业的营业场所、处理场所应满足以下要求：
a） 应配备符合国家标准和行业标准的安全监控设备，安排专门人员对收寄、分拣、运输、投递等环节的个人信息处理进行安全监控；
b） 应对个人信息存储载体实行集中封闭管理，确定集中存放地，采取必要的安全防护措施，确保存储安全。

6.5 信息系统

6.5.1 寄递企业信息系统应符合 GB/T 22239 的规定。
6.5.2 开发具有处理个人信息功能的信息系统时，宜根据国家有关标准在需求、设计、开发、测试、发布等阶段考虑个人信息保护要求，保证在系统建设时对个人信息保护措施同步规划、同步建设和同步使用。
6.5.3 认定为关键信息基础设施的系统，应按照关键信息基础设施安全保护相关规定，与关键信息基础设施同步规划、同步建设、同步使用安全保护措施，并自觉接受邮政管理部门的监督检查。
6.5.4 关键信息基础设施发生较大规模个人信息泄露、造成较大经济损失、违法信息较大范围传播等特别重大网络安全事件或者发现特别重大网络安全威胁时，寄递企业应按照有关规定及时向邮政管理部门、公安机关报告。

6.6 其他

寄递服务用户个人信息保护应遵循国家关于数据分类分级的要求。

7 个人信息收集

7.1 直接收集个人信息

寄递企业收集个人信息应遵守 GB/T 35273—2020 中 5.1、5.2、5.3、5.4 的规定，同时还应满足以下要求：
a） 收集 5.2、5.3 所列的必要个人信息前，应通过服务合同、个人信息保护政策等方式告知用户收集、使用个人信息的目的、方式和范围等；
b） 收集其他个人信息，应告知用户所需收集的个人信息，收集使用的目的和方式、范围等，并获得用户的明示同意；
c） 个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应重新取得个人同意；
d） 在公共场所安装图像采集设备，应遵守国家有关规定，并设置显著的提示标识；
e） 收集不满 14 周岁未成年人的个人信息前，应征得其监护人的明示同意；
f） 应使用符合国家要求的个人信息采集设备。

7.2 间接获取个人信息

寄递企业通过电子商务平台等途径间接获取个人信息时，应满足以下要求：
a） 应要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认；
b） 应了解个人信息提供方已获得的个人信息处理的授权同意范围，包括使用目的，用户是否授权同意转让、共享、公开披露、删除等；

c） 如开展业务所需进行的个人信息处理活动超出个人信息提供方已获得的授权同意范围，应在获取个人信息后的合理期限内或处理个人信息前征得用户的明示同意，或通过个人信息提供方征得用户的明示同意。

8 个人信息存储、销毁及删除

8.1 存储期限

个人信息存储期限应为实现处理目的所必需的最短时间，邮件详情单、快递运单、快递电子运单（以下统称“寄递运单”）的实物保存期限宜为在投递完成后不少于1年，相应的电子数据保存期限不应少于3年。

8.2 存储要求

8.2.1 寄递企业应加强营业场所、处理场所管理，避免无关人员出入以及接触、翻阅、复制、拍摄邮件快件，防止寄递运单实物信息在处理过程中泄露。

8.2.2 对于电子个人信息，寄递企业在存储过程中，应遵守GB/T 35273—2020中第6章的规定，同时还应满足以下要求：

a） 使用独立物理区域放置电子个人信息存储设备和介质，禁止非授权人员进出；

b） 建立电子个人信息存储设备和介质的使用、借用登记制度，限制设备输出接口的使用；

c） 对敏感电子个人信息采用符合国家有关规定的密码算法加密等安全措施进行存储；

d） 智能收投服务终端对采集的电子个人信息进行离线存储的，应采取加密等安全措施，存储期限不宜超过30 d。

8.3 销毁及删除要求

8.3.1 纸质寄递运单保管期满，应进行集中销毁。销毁时，应由2名及2名以上人员共同完成。

8.3.2 对电子个人信息存储设备和介质进行报废处理时，应采用物理损毁或脱敏、格式化等方式，销毁硬件并删除相关数据，确保个人信息不能被恢复。

8.3.3 依法应主动删除的个人信息，以及寄递服务用户依法要求删除的个人信息，寄递企业应及时删除。法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，寄递企业应停止除存储和采取必要的安全保护措施之外的处理措施。

8.3.4 寄递企业应建立和保存销毁及删除的记录。

9 个人信息使用

9.1 总体要求

寄递服务用户个人信息只能用于寄递业务，除征得寄递服务用户同意外，不应用于其他用途，不应泄露、丢失、损毁、篡改和不当使用。

9.2 收寄和投递环节使用

在收寄和投递环节展示和使用个人信息时，应满足以下要求：

a） 快递电子运单应避免显示完整的收件人和寄件人姓名、联系电话、地址等个人信息。国内寄递，收件人姓名和寄件人姓名应隐藏1个汉字以上；联系电话应隐藏6位以上；地址应隐藏单元户室号；另有规定除外。

b) 与电商平台或者快递电子运单集成系统运营企业等第三方对接寄递信息时,应要求其对快递电子运单进行去标识化处理,并确保不影响正常寄递服务;存在寄递服务用户个人信息安全风险或者可能影响正常服务的,不应与其对接寄递信息。

c) 可采用 RFID、虚拟安全号码、电子纸等先进技术,对快递电子运单上的个人信息进行保护;采用 RFID、虚拟安全号码、电子纸等技术时,应符合附录 A 的规定。

d) 供快递员使用的移动作业终端(或 App),应仅展示由其收件或派件的寄递服务用户个人信息,姓名和电话号码宜进行去标识化处理;查看寄递服务用户地址时,应采用水印技术确保数据泄露可追踪。

e) 智能收投服务终端应采用技术手段防止无关人员通过设备端口提取终端数据。

f) 快递员联系用户时,宜通过虚拟安全号码或其他隐藏寄递服务用户真实电话号码的方式进行联系。

9.3 内部处理环节使用

9.3.1 个人信息展示

供寄递企业内部人员使用的业务系统,应对寄递服务用户姓名、地址、电话号码等个人信息进行去标识化处理。因业务所需无法进行去标识化处理的,应采用水印等技术确保数据泄露可追踪。

9.3.2 个人信息访问和导出

寄递企业对个人信息访问和导出权限的控制应遵守 GB/T 35273—2020 中 7.1 的规定,同时还应满足以下要求:

a) 应根据数据安全级别定义不同级别数据的访问和导出权限,根据工作需要分配内部人员的最小所需数据访问和导出权限,并加强对权限的监控和管控;

b) 应通过系统外呼等功能降低内部人员对个人信息的访问范围及访问频率;

c) 内部人员查询和导出个人信息时,应使用双因素或 OTP 进行登录认证或同级别的认证,或使用不同于用户登录的验证方式进行二次认证;

d) 应通过建立审批制度等方式,加强对个人信息批量查询和导出的管理;

e) 内部人员通过个人移动作业终端安装业务 App 访问内部数据时,该 App 宜支持远程擦除本地业务数据功能,防止设备丢失时发生数据非授权访问。

9.4 其他使用

9.4.1 用户画像

寄递企业在业务运营或对外业务合作中确需进行用户画像的,应严格遵守 GB/T 35273—2020 中 7.4 的规定,同时还应满足以下要求:

a) 未经寄递服务用户授权同意,不应将用户画像用于各类商业活动;

b) 利用用户画像分析进行自动化决策前,应对用户画像分析活动进行个人信息安全影响评估,降低用户画像分析活动风险;

c) 进行群体用户画像应用时,应采取措施确保无法从群体用户画像信息中反推或还原出寄递服务用户身份。

9.4.2 个性化展示的使用

寄递企业需要进行个性化推送或广告营销时,应遵守 GB/T 35273—2020 中 7.5 的规定,同时还应满足以下要求:

a） 应建立个性化推送管理机制，对个性化推送需求进行流程审批；
b） 应建立退订用户名单，包括所有退订或反对接受营销的用户，保证用户退订权利行使的有效性。

10 个人信息的提供

10.1 委托处理

寄递企业委托第三方以及其他寄递企业等开展代收代投、报关清关等业务，需要对个人信息进行委托处理时，应满足以下要求：

a） 应对委托行为进行个人信息安全影响评估，确保受委托者符合相关要求；
b） 应与受委托者约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等；
c） 委托处理的个人信息不应超出已征得寄递服务用户授权同意或业务处理目的的范围；
d） 应在数据交换前进行严格的身份验证，应采用符合国家有关规定密码算法和安全的传输协议，确保数据交换的内容不可篡改；
e） 应通过审计等方式对受委托者进行监督；
f） 应准确记录和存储委托处理个人信息的情况；
g） 得知或者发现受委托者未按照委托要求处理个人信息，或未能有效履行个人信息安全保护责任的，应立即要求受托者停止相关行为，且采取或要求受委托者采取有效补救措施（如更改口令、回收权限、断开网络连接等）控制或消除个人信息面临的安全风险。必要时寄递企业应终止与受委托者的业务关系，并要求受委托者及时删除所获得的个人信息。

10.2 跨境提供

寄递企业跨境提供寄递服务用户个人信息，应符合相关法律法规部门规章等规定。

11 个人权利的实现

寄递企业应采取措施，保证寄递服务用户依法享有对个人信息的知情权、决定权，包括查阅和复制、信息转移、更正和补充、删除等具体权利。寄递企业还应满足以下要求：

a） 在验证用户身份后，应在法律法规或承诺的时限内响应寄递服务用户对其个人信息提出的请求；如依法决定不响应寄递服务用户的请求，应告知理由，并提供投诉途径；
b） 通过网站、App、客户端软件等提供服务的，宜直接设置便捷的交互式页面提供功能或选项，便于寄递服务用户行使权利。

12 个人信息安全事件处置

12.1 个人信息安全事件应急处置和报告

寄递企业应对个人信息安全事件时，应满足以下要求：

a） 应制定个人信息安全事件应急预案；
b） 应定期（至少每年一次）组织内部相关人员进行应急响应培训和应急演练，使其掌握应急处置策略和规程；
c） 发生个人信息安全事件后，应根据应急预案进行以下处置：
1） 记录事件内容，包括但不限于：发现事件的人员、时间、地点，涉及的个人信息及人数，发生

事件的系统名称,对其他互联系统的影响,是否已联系执法机关或有关部门;

2） 评估事件可能造成的影响,并采取必要措施控制事态,消除隐患;

3） 按照国家网络安全事件应急预案等有关规定及时上报,并及时报告邮政管理部门,报告内容包括但不限于:涉及个人信息数量、内容、性质等总体情况,事件可能造成的影响,已采取或将要采取的处置措施,事件处置相关人员的联系方式;

4） 个人信息泄露事件可能会给寄递服务用户的合法权益造成严重危害的,如敏感个人信息的泄露,按照12.2的要求实施安全事件的告知;

d） 根据相关法律法规变化情况以及事件处置情况,及时更新应急预案。

12.2 安全事件告知

寄递企业进行安全事件告知时,应满足以下要求:

a） 应及时将事件相关情况以邮件、电话、推送通知等方式告知受影响的用户。难以逐一告知用户时,应采取合理、有效的方式发布公众警示信息。

b） 告知内容应包括但不限于:

1） 安全事件的内容和影响;

2） 已采取或将要采取的处置措施;

3） 用户自主防范和降低风险的建议;

4） 个人信息保护工作机构和负责人的联系方式。

附 录 A
（规范性）
个人信息保护技术的应用

A.1 虚拟安全号码的应用

寄递企业使用虚拟安全号码进行用户个人信息保护时，快递员通过虚拟安全号码与收（寄）件用户联络，应满足以下要求：

a） 虚拟安全号码在快递电子运单生成时生效；
b） 快递员与用户之间通过虚拟安全号码绑定的时长应满足投递要求；
c） 虚拟安全号码管理系统与寄递信息系统之间的报文请求与响应时间延迟应小于 1 s，用户通话延迟增加应不大于 1 s；
d） 通话录音应在通话结束后 3 min 内生成，采用加密等安全措施存储，存储时间应不少于 6 个月。

A.2 RFID 技术的应用

寄递企业可采用 RFID 标签作为个人信息载体。使用 RFID 技术应满足以下要求：

a） 用于寄递的 RFID 标签宜采用超高频无源电子标签，标签和读写器之间的空中接口通信参数应符合 GB/T 29768 或 ISO/IEC 18000-6C 的要求，工作频率范围为 840 MHz～960 MHz，宜采用 920 MHz～925 MHz；
b） 对标签存储的数据应有防篡改、防信息损坏、防非法读取等技术措施；
c） 读写设备应通过国家无线电管理委员会无线电发射设备型号核准；
d） 应能通过 RFID 标签的识读，实现快件收寄、分拣、运输、投递等作业。

A.3 电子纸技术的应用

电子纸是指通过类纸内嵌式电子显示器实时显示，显示屏幕依靠自然光的反射成像，无需外部电源即可维持静态图像不消失，并可更新寄递信息的电子运单装置。寄递企业可将电子纸技术应用于快递电子运单信息的展示。使用电子纸技术应满足以下要求：

a） 30 cm 距离裸眼可清晰辨识寄递信息；
b） 断电后，寄递信息不应丢失；
c） 完成寄递前，应有技术措施确保寄递信息不被随意修改；
d） 完成寄递后，电子纸不应显示和存储已完成寄递服务的寄递信息与数据。

参 考 文 献

[1] GB/T 41391—2022 信息安全技术 移动互联网应用程序(App)收集个人信息基本要求
[2] GB/T 41479—2022 信息安全技术 网络数据处理安全要求
[3] 中共中央网络安全和信息化委员会办公室 《国家网络安全事件应急预案》(中网办发文〔2017〕4号)