



中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 快递物流服务数据安全指南

Information security technology — Data security guidelines for express logistics services

（征求意见稿）

（本草案完成时间：2021年2月3日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布

XXXX - XX - XX 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	3
5 概述	3
5.1 快递物流服务组成	3
5.2 快递物流服务数据范围	3
5.3 快递物流服务数据活动	3
5.4 快递物流服务数据安全风险	4
6 基本要求	5
7 数据收集	5
7.1 数据最小化收集	5
7.2 系统权限	5
7.3 用户告知同意	5
8 数据使用	5
8.1 数据展示	5
8.2 数据访问	6
8.3 数据导出	6
8.4 数据加工处理	7
8.5 日志记录与审计	7
9 数据交换	7
9.1 委托处理	7
9.2 数据共享	8
9.3 数据出境	8
10 数据存储与传输	9
10.1 数据存储安全	9
10.2 数据传输安全	9
11 个人信息主体权利	9
12 快递物流服务典型业务场景数据安全保护	10
12.1 快递面单	10
12.2 收派员收派服务	10
12.3 用户查单	11
12.4 快件箱	11
12.5 收派移动作业终端	11

附录 A（资料性）	快递物流服务数据分级分类示例.....	13
附录 B（资料性）	快递物流服务可选个人信息收集范围及使用要求.....	17
附录 C（资料性）	快递物流服务 App 相关系统权限申请范围及使用要求.....	18
附录 D（资料性）	常见场景告知用户同意	19
附录 E（资料性）	数据脱敏方式举例	20
附录 F（资料性）	信息查询反馈规则	21
参考文献.....		24

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。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：顺丰速运有限公司、中国电子技术标准化研究院、中国邮政速递物流股份有限公司、北京京东振世信息技术有限公司、浙江菜鸟供应链管理有限公司、苏宁易购集团股份有限公司、中电长城网际安全技术研究院（北京）有限公司、中国信息通信研究院。

本文件主要起草人：刘玉霞、王森、胡影、杨玉冰、周晨炜、林崖冰、谢安明、闵京华、张林、郭琦、黎琳、吴剑锋、符薇、黄琳、康琼、曹京、王超、严少敏、杨青、洪小崇、荆伟。

信息安全技术 快递物流服务数据安全指南

1 范围

本文件规定了快递物流服务可以收集、传输、存储、使用、共享、委托处理、删除、出境的数据种类、范围、方式、条件等，以及数据安全保护要求。

本文件适用于快递物流服务运营者规范数据活动，也适用于主管监管部门、第三方评估机构对快递物流服务数据活动进行监督、管理、评估时参考。

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。

GB/T 10757—2011 邮政业术语

GB/T 25069—2010 信息安全技术 术语

GB/T 27917.1—2011 快递服务 第1部分：基本术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T AAAAA 信息安全技术 网络数据处理安全规范

GB/T BBBBB 信息安全技术 移动互联网应用（App）收集个人信息基本规范

YZ/T 0133—2013 智能快件箱

3 术语和定义

GB/T 25069—2010、GB/T 35273—2020、GB/T 10757—2011、GB/T 27917.1—2011以及YZ/T 0133—2013界定的以及下列术语和定义适用于本文件。

3.1

快递物流服务 express logistics service

从接收用户订单开始到将物品送到用户手中为止所发生的所有服务活动，保证用户的物品在顾客要求的时间内准时送达，包括下单、收件、封装、中转、派件、售后等服务。

注：本文件中所述的快递物流服务不包括纯货物运输型物流服务。

[来源：GB/T 27917.1—2011，2.1，有修改]

3.2

寄递用户 sender and addressee

向快递物流服务运营者获取快递物流服务的个人或组织，包括寄件用户和收件用户。

3.3

快递物流服务组织 express logistics service organization

在中国境内依法注册的，提供快递物流服务（3.1）的企业及其加盟企业、代理企业。

GB/T XXXXX—XXXX

[来源：GB/T 27917.1—2011，2.2，有修改]

3.4

快件 express item

由快递物流服务组织（3.3）依法递送给特定个人或者单位的信件、包裹、印刷品等的统称。

[来源：GB/T 10757—2011，5.2，有修改]

3.5

快递物流服务受理组织 express logistics service acceptance organization

通过 App、Web、小程序、公众号、客户端等方式向寄递用户提供快递物流下单服务、查询服务的中间组织，寄递用户下单数据通过该组织传递给快递物流服务组织，简称“服务受理组织”。

3.6

快件代存组织 express deposit organization

通过快件箱、快递服务站等方式向用户提供快递物流代揽收、代派件服务的组织，用户下单数据通过该组织传递给快递物流服务组织。

3.7

快递物流服务运营者 express logistics service operator

快递物流服务组织、快递物流服务受理组织、快件代存组织统称为快递物流服务运营者，简称“服务运营者”。

3.8

运营者业务合作伙伴 operation organization business partner

受快递物流服务运营者委托，处理快递物流业务中清关、保险、客服等特定事项的组织。

3.9

收派员 courier

快递物流服务组织从事上门揽收快件和投递快件工作的人员。

[来源：GB/T 27917.1—2011，4.2.1，有修改]

3.10

快件路由信息 express item tracking information

快递物流服务运营者记录快件在寄递主要环节的流转信息，并据此向用户提供的快件查询信息，流转信息包括处理时间、处理场所、处理状态和处理结果等。

3.11

智能终端设备 smart terminal

支持音频、视频、数据传输等多媒体功能的，用于信息处理的智能设备。快递物流业务中常见的智能终端设备包括快件箱、无人车、无人机、智能穿戴设备、移动作业终端等。

3.12

智能快件箱 intelligent self-express service machine

设立在公共场合，可供快递物流服务组织和用户提取快件的自助服务设备，简称“快件箱”。

[来源：YZ/T 0133—2013，3.1，有修改]

4 缩略语

下列缩略语适用于本文件：

App：移动互联网应用程序（mobile internet application）

IMEI：国际移动设备识别码（international mobile equipment identity）

MAC：媒体访问控制（media access control）

OTP：动态口令（one-time password）

5 概述

5.1 快递物流服务组成

本文件所称的快递物流服务主要包括国内快递物流服务、国际及港澳台快递物流服务、快递物流增值服务。涉及角色包括寄递用户、快递物流服务组织、服务受理组织、快件代存组织、运营者业务合作伙伴。寄递用户获取快递物流服务的途径包括由快递物流服务组织、服务受理组织、快件代存组织等提供的 App、网页、小程序、公众号、服务热线、服务点等。

5.2 快递物流服务数据范围

快递物流服务涉及的数据类别为：用户数据、企业运营数据，具体数据类别及对应示例参见附录表 A.1。

- a) 用户数据：指业务开展过程当中涉及到的个人用户及企业用户相关数据。
 - 1) 个人用户数据：指业务开展过程中涉及的个人寄递用户数据。
 - 2) 企业用户数据：指业务开展过程中涉及的企业客户数据、供应商数据等企业用户相关数据。
- b) 企业运营数据：指经营活动中产生的各类业务经营相关的数据，包括但不限于寄递物品及费用信息、配送信息、签收信息、客服售后信息、营业场所信息、财务信息、营销运营信息等。

5.3 快递物流服务数据活动

快递物流服务数据活动主要围绕着快递物流服务的业务功能开展，包括：寄递用户会员注册、寄件、收件、快件信息查询、个人信息主体权利实现等；服务运营者的收货、中转、清关、派送等。

快递物流服务中，寄递用户通过服务运营者提供的各类途径进行寄件下单，经过服务运营者中转，最后完成派送。快递物流服务数据活动示意如图 1 所示。

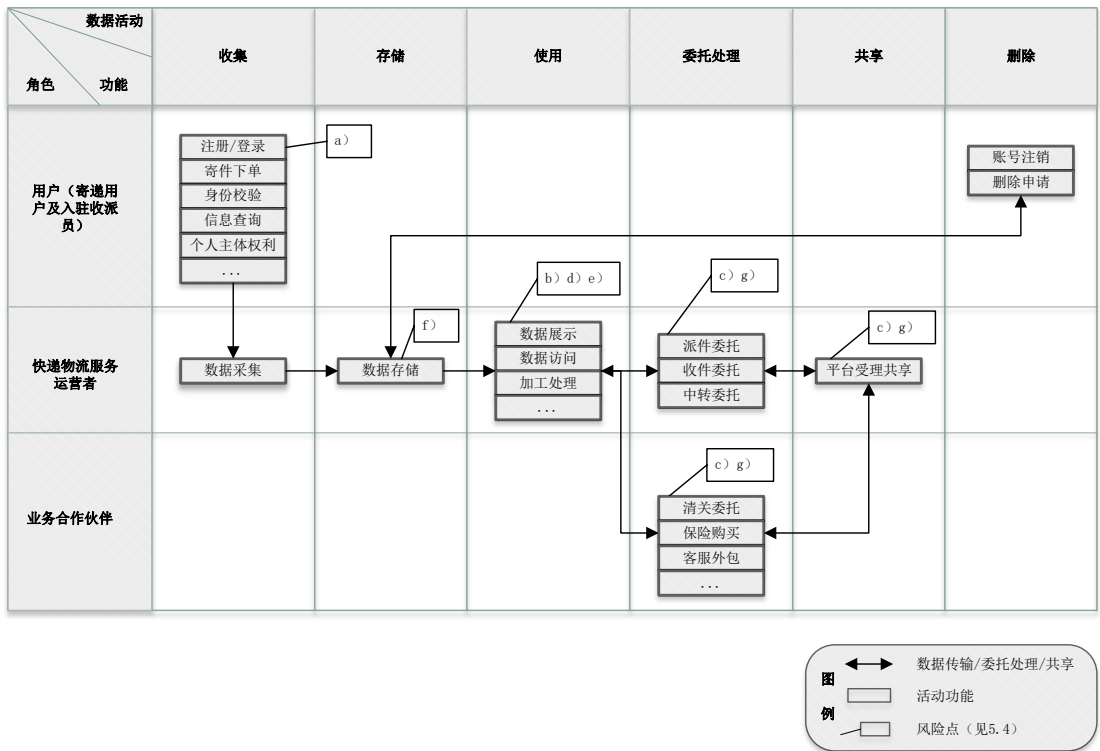


图 1 快递物流服务数据活动示意图

5.4 快递物流服务数据安全风险

快递物流服务主要面临以下数据安全风险：

- a) 服务运营者在提供服务时，过度收集寄递用户、入驻收派员的个人信息，或通过 App 过度获取系统权限所导致的个人信息被过度采集的风险；
- b) 服务运营者以业务营销、业务风险控制、提升服务质量为目的分析个人信息，对用户进行画像和信息推送所带来的个人利益损害和生活干扰等风险；
- c) 在偏远地区和跨国快件转寄、清关委托、快递保险购买、客服外包等场景下，与第三方共享或委托处理数据时，服务运营者对数据接收方的尽职调查和数据活动监督不足或缺失，数据未得到同等保护而导致数据泄露或滥用风险；
- d) 在快件的中转过程中因工作开展需接触寄件用户个人信息的内部人员多，如收派员、客服人员、仓管人员、财务人员、报关人员等，管理难度大，可能出现内部人员有意或无意泄露寄递用户信息的风险；
- e) 因纸质面单暴露个人信息，在快递面单丢失、经手人员泄露、客户丢弃快递包装等场景下带来的数据泄露风险；
- f) 快递物流服务中使用快件箱、无人车、无人机、智能穿戴设备、移动作业终端（收派巴枪、手机）等智能终端设备的场景下，因设备丢失或设备保护措施不足等导致的数据泄露风险；
- g) 跨境快递物流服务的场景中，需将国际快递运单信息传输给境外国家/地区的关联公司、快递物流服务组织、运营者业务合作伙伴，构成数据出境，可能存在数据未授权出境或出境未得到同等保护的风险。

6 基本要求

快递物流服务运营者应满足以下基本要求：

- a) 快递物流服务的数据活动应符合GB/T AAAAAA要求；
- b) 快递物流服务的个人信息处理活动应符合GB/T 35273—2020要求，快递物流App的个人信息收集活动应符合GB/T BBBBBB要求；
- c) 快递物流服务运营者应识别数据活动涉及的数据，形成数据保护目录，并对快递物流服务数据进行分级分类保护。快递物流服务数据分级分类示例见附录A。

7 数据收集

7.1 数据最小化收集

快递物流服务收集个人信息应遵守 GB/T 35273—2020 中 5.1 和 5.2 规定的要求，快递物流服务可选个人信息收集范围及使用要求参见附录 B。

7.2 系统权限

提供快递物流服务时，App 获取的系统权限、调用权限条件应在实现业务功能所需的最低合理范围内。快递物流服务 App 相关系统权限申请范围及使用要求参见附录 C。

7.3 用户告知同意

服务运营者收集信息应遵守 GB/T 35273—2020 中 5.4 规定的要求，同时还应满足以下要求：

- a) 服务运营者提供寄件服务时，在收集个人信息前应通过快递物流服务协议、用户协议、个人信息保护政策等方式告知收集、使用个人信息的目的、方式和范围等规则，并获得用户明示同意。典型场景（清关、转运）的告知同意示例参见附录 D；
- b) 在寄递服务实名认证、收派员入驻实名认证、快件箱收件用户身份识别时，应单独征得用户的明示同意（如单独弹框等），如需获取个人生物识别信息，应同时提供其他非生物识别信息的实名认证方式；
- c) 服务运营者提供增值服务时，应独立进行增值服务声明（如增值服务条款），告知个人信息主体增值服务所需收集的个人信息、收集使用的目的和方式等，并获得用户的明示同意；
- d) 服务运营者应保留用户的授权同意记录，包括但不限于同意的个人信息主体、时间、范围、方式等。

8 数据使用

8.1 数据展示

寄递用户信息展示应遵守 GB/T 35273—2020 中 7.2 规定的要求，同时还应满足以下要求：

- a) 快递纸质面单，应将寄递用户的电话号码和（或）地址进行去标识化处理；
- b) 供寄递用户使用的应用，应将历史收寄件运单详情、账户通讯簿、会员信息等界面中展示的个人身份信息、地址、电话号码等进行去标识化处理；
- c) 供收派员使用的移动作业终端（或应用），应仅展示由其收件或派件的寄递用户信息，寄递用户的个人身份信息和电话号码应进行去标识化处理。寄递用户地址，因服务所需必须查看明文信息时，展示界面应采用水印技术确保数据泄露可追踪；
- d) 供内部人员使用的业务系统，应对个人身份信息、地址、电话号码等进行去标识化处理。因业

务所需无法进行去标识化处理的，展示明文信息时，应采用水印技术确保数据泄露可追踪。常见的去标识化处理方式如数据脱敏，可参见附录 E。

注：去标识化处理可采用信息加密、数据脱敏或虚拟号码替代真实号码等方式。

8.2 数据访问

服务运营者对寄递用户个人信息访问权限的控制应遵守 GB/T 35273—2020 中 7.1 规定的要求，同时还应满足以下要求：

- a) 寄递用户或服务运营者内部人员通过线上系统查询和导出寄递用户个人身份信息、电话号码、地址等敏感信息时，应使用双因素或 OTP 进行登录认证或同级别的认证，或在敏感操作时使用不同于用户登录的验证方式进行二次认证；
- b) 寄递用户通过线下渠道，如客服热线或快递物流服务运营场所，查询寄递用户个人身份信息、电话号码、地址等敏感信息时，为防止他人仿冒寄递用户查询快件信息，应确认查询人身份后，再提供查询服务，并记录查询内容。信息查询反馈规则参见附录 F；
- c) 不同服务运营者通过系统接口进行数据访问，应仅传递业务必需的数据；
- d) 应根据数据安全级别（见附录 A）定义不同级别数据的访问权限，根据服务范围或服务对象分配内部人员的最小所需数据访问权限；

注：地区业务人员仅能查询本地区服务的运单信息，收派员仅能查询其服务范围的运单信息，客服人员仅能基于用户咨询、查阅、投诉等请求进行相关信息查询。

- e) 寄递用户仅可查询其作为寄件方或收件方的运单、快件路由、费用等信息。查询人未校验身份时，仅可通过运单号查询快件路由信息，且展示的快件路由信息中不应包含寄递用户个人身份信息、电话号码、地址等敏感信息；
- f) 服务运营者内部人员对于寄递用户个人身份信息、电话号码、地址等敏感信息的访问，应通过系统外呼等功能降低内部人员对敏感信息的访问范围及访问频率；

注：采用系统呼叫功能实现客服、仓库管理员、收派员等内部人员与寄递用户的语音联系，代替内部人员通过查询寄递用户明文电话号码后，手动输入寄递用户电话号码联系寄递用户的方式。

- g) 对于涉及寄递用户个人身份信息、电话号码、地址等敏感信息查询或导出的操作，应通过建立审批流、限制数据范围等措施，限制敏感信息批量查询、导出等操作功能；
- h) 服务运营者自有智能终端设备，应通过端口管控或物理设备锁等防撬起措施防止通过设备端口（包括 USB 端口、蓝牙等）提取终端数据；
- i) 服务运营者自有智能终端设备丢失时，应支持远程对设备进行锁屏、业务数据擦除等措施，防止数据被非授权访问；
- j) 服务运营者内部人员通过个人智能终端设备安装业务 App 访问组织内部敏感数据时，该 App 应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。

8.3 数据导出

服务运营者对数据导出应满足以下要求：

- a) 应根据数据安全级别（见附录 A）定义不同级别数据的导出审批流程；
- b) 应通过加密存储、加密传输、最小访问范围等方式对导出后的敏感数据进行保护；

注：加密存储可采用磁盘加密、文档加密等措施。

- c) 应对敏感数据外发权限进行管控，并对敏感数据的外发操作进行监控或阻断。

注 1：如限制邮件外发权限、USB 写权限、终端共享权限等数据外发权限，限制涉及数据上传权限的应用软件和网站。

注 2：通过终端和网络数据防泄密工具，实时监控内部人员外发敏感数据的行为，对疑似违规外发敏感数据的行为

及时阻断。

8.4 数据加工处理

8.4.1 用户画像

服务运营者基于业务风险控制等需求，进行用户画像分析时，应遵守 GB/T 35273—2020 中 7.4 规定的要求，同时还应满足以下要求：

- a) 进行个人用户画像分析活动前，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；
- b) 进行群体用户画像应用时，应通过将可用于恢复识别个人的信息与去标识化后的信息分开存储等措施，确保内部人员或数据接收方无法从群体用户画像信息中反推或还原出个人信息主体身份。

8.4.2 个性化展示的使用

服务运营者需要展示个性化推送或营销广告时，应遵守 GB/T 35273—2020 中 7.5 规定的要求，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。

8.5 日志记录与审计

服务运营者应对数据使用保留日志记录，日志记录应满足以下要求：

- a) 日志数据包含寄递用户个人身份信息、电话号码、地址等敏感信息时，应对敏感数据进行去标识化处理；
- b) 记录的日志类型宜包括但不限于：
 - 1) 登录日志：记录快递员、客服等人员成功/失败的认证/登录、正常退出、超时退出的活动；
 - 2) 用户管理日志：记录快递员、客服等人员账号密码的修改和重置等活动；
 - 3) 敏感信息操作日志：记录包括但不限于用户、员工等敏感信息的新增、查询、修改、导出、解密、删除等操作。
- c) 应对涉及寄递用户个人身份信息、电话号码、地址等敏感信息操作权限相关账号的登录和修改操作进行日志审计，及时发现异常账号；
- d) 应对跨服务范围、非工作时间、非工单触发等异常情况下，涉及寄递用户个人身份信息、电话号码、地址等敏感信息的操作进行审计，及时发现异常操作；
- e) 应对批量查询导出寄递用户个人身份信息、电话号码、地址等敏感信息的操作进行监控审计，及时发现异常操作。

9 数据交换

9.1 委托处理

快递物流服务中数据委托处理应满足以下要求：

- a) 服务运营者委托第三方开展寄递服务、客诉业务、快件代存、清关、保险等业务时，应遵守 GB/T 35273—2020 中 9.1 规定的要求；

注：如转运、平台寄件、第三方呼叫中心、快件寄存快递服务站等涉及数据委托处理的业务场景。

- b) 服务运营者受委托开展寄递服务、快件代存业务时，应遵守 GB/T 35273—2020 中 9.1 规定的

要求，同时还应满足以下要求：

- 1) 个人信息进行跨境转移，应获得委托方同意；
- 2) 将服务外包给第三方时，应获得委托方同意，同时与第三方签署数据处理协议，要求其按照不低于委托方的要求进行个人信息保护；
- 3) 应配合委托方实施对数据安全及合规要求的审计；
- 4) 服务完成后，受委托方应在最小存储期限到期时删除或销毁相关个人信息，并保留操作记录以供审计，法律法规或合同另有规定的除外。

9.2 数据共享

服务运营者与第三方共享个人信息时，应遵守 GB/T 35273—2020 中 9.2 规定的要求，同时还应满足以下要求：

- a) 与关联公司数据共享时，服务组织应与关联公司签署严格的商业秘密保护协议或数据处理协议等，要求关联公司按快递物流服务协议、个人信息保护政策及其它任何相关的安全要求来处理个人信息；
- b) 寄递用户通过快递物流服务受理组织发布快递物流服务订单，服务受理组织将订单信息发送至服务运营者时，服务受理组织与服务运营者的数据共享要求包括：
 - 1) 向服务运营者共享订单信息时，如为快递物流基础服务订单，应仅共享基础服务必需收集的个人信息，包括寄件用户和收件用户的姓名、地址、电话号码和寄递物品信息。
 - 2) 向服务受理组织共享服务订单的履约信息、支付信息时，服务运营者应仅共享服务受理组织涉及订单范围信息；
 - 3) 服务运营者与服务受理组织处理快递物流服务纠纷时，仅共享必要的身份信息及纠纷处理所需信息。

9.3 数据出境

服务运营者开展国际快递物流服务时，将国际快递运单信息传输给境外国家/地区的关联公司、快递物流服务组织、运营者业务合作伙伴，构成数据出境。数据出境时应遵守相关法律法规及标准要求，同时还应满足以下要求：

- a) 事先开展数据出境安全评估，并依评估结果采取有效的保护个人信息主体权利及数据安全的措施。数据出境安全评估应包括但不限于以下内容：
 - 1) 数据出境的合法性及必要性评估；
注：不涉及国际快递物流服务的，寄递用户个人身份信息、电话号码、地址不宜传输至境外。境外仅需查询的不应将数据在境外存储。
 - 2) 涉及个人信息或重要数据的情况，包括数据类型、数量、范围、敏感程度、境外存储期限、出境目的以及接收方处理数据的目的、方式、范围等；
注：出境数据仅限提供快递物流服务所需的必要业务信息，如配送信息、清关信息等。
 - 3) 个人信息主体合法权益保障能力评估；
注：通过数据出境合同、数据跨境传输协议、数据处理协议等明确服务运营者及数据接收方的责任与义务，保障个人信息主体合法权益。
 - 4) 数据接收方是否有损害个人信息主体合法权益的历史、是否发生过重大网络安全事件，其安全保护措施、能力和水平，以及所在国家和地区的网络安全环境、数据保护法律体系的完善性等；
 - 5) 数据出境及再转移后被泄露、毁损、篡改、滥用等风险；
注：如境外快递物流服务分包给第三方，需对第三方数据活动的合规及安全风险进行评估。

- 6) 数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险。
- b) 应向个人信息主体说明数据出境的目的、范围、内容、接收方及接收方所在的国家或地区，并经其同意；
 - c) 当数据接收方出现变更，数据出境目的、范围、数量、类型等发生较大变化，数据接收方或出境数据发生重大安全事件时，应及时重新进行安全评估；
 - d) 应建立个人信息出境记录；
 - e) 应根据业务发展和运营情况，每年对数据出境至少进行一次安全评估；
 - f) 各国家/地区可能设有不同的数据保护法，甚至未设立相关法律，在此类情况下，应确保用户的个人信息得到在境内同等的保护。

10 数据存储与传输

10.1 数据存储安全

快递物流服务数据在存储过程中，应遵守 GB/T 35273—2020 中第 6 章规定的要求，同时还应满足以下要求：

- a) 服务运营者应对寄递用户的个人身份信息、电话号码、地址等敏感信息采用加密等安全措施进行存储；
- b) 寄递服务实名认证、收派员入驻实名认证、快件箱收件人身份识别等场景，如涉及收集寄递用户及收派员的个人生物识别信息（如面部识别特征、声纹等）应仅存储其摘要信息，并与个人身份信息分开存储，在实现个人信息主体授权使用目的后应删除可提取个人生物识别信息的原始图像；
- c) 智能终端设备对采集的个人信息进行离线存储，存储期限不宜超过 30 天；
- d) 智能终端设备离线存储的个人信息及取件验证码，应采取加密等安全措施保证数据存储的保密性；
- e) 服务运营者自有智能终端设备应建立失效设备资产列表，采取相关措施对失效设备存储的业务数据进行清除。

10.2 数据传输安全

快递物流服务数据在传输过程中应满足以下要求：

- a) 不同组织间通过系统接口传输敏感数据时，应至少使用白名单（IP、域名等）方式进行控制，同时应使用数字签名、开放标准认证（OAuth）等方式对调用的信息系统进行认证，确保对接口的鉴权；
- b) 通过互联网传输及线下途径传输寄递用户个人身份信息、电话号码、地址等敏感信息时，应使用安全通道或数据加密等方式进行传输。

11 个人信息主体权利

服务运营者在响应个人信息主体权利请求时，应遵守 GB/T 35273—2020 中第 8 章规定的要求，同时还应满足以下要求：

- a) 服务运营者应核实个人信息主体权利请求人的身份；
注：使用如账户、运单信息、账户绑定手机号码、收寄件用户联系电话号码、手机动态验证码等信息进行身份校验。
- b) 服务运营者应保存所有请求的响应记录；
- c) 服务运营者宜支持通过系统功能实现部分个人信息主体权利，包括但不限于：

- 1) 对快递物流基础服务所使用的个人信息（如联系方式、地址等）及会员信息的查询和更正权利；
 - 2) 对授权的个人信保护政策、快件路由信息推送、广告推送功能等撤回同意的权利。
 - d) 个人信息主体权利涉及由第三方协助实现时，服务运营者应确保与第三方制定权利请求响应机制，并在第三方协议中明确第三方的相关义务；
 - e) 服务运营者应提供注销提醒或注销协议，告知执行注销操作对寄递用户可能造成的影响，并及时对其个人信息进行删除或匿名化处理；
- 注 1：可造成影响包括但不限于：会员账户注销表示自愿放弃会员权益和虚拟资产；会员账户、结算账户等关联账户，注销其中某项，会导致服务不可用或质量下降；会员账户注销后不可恢复。
- 注 2：服务运营者宜设置注销删除等待期（如 30 天），在提交注销申请后的等待期内可撤销申请，并可通过重新注册复原相关个人账号信息和相关个人服务记录，超过等待期将永久删除。
- f) 若存在下列情形的，服务运营者在注销权利响应中宜设置适当的前提条件判定是否受理用户注销账号的请求：
 - 1) 账号存在未处理完毕的交易或纠纷，包括但不限于运单在途、清关、转运等；
 - 2) 账号下拥有财产权益（包括会员积分、会员等级、会员权益、优惠券等），用户明示自愿放弃相关财产权益除外；
 - 3) 法律法规要求限制或禁止注销的情形。

12 快递物流服务典型业务场景数据安全保护

12.1 快递面单

除中转、派送所必需的信息，面单不应展示除姓名、电话号码、地址以外的个人信息。

12.2 收派员收派服务

12.2.1 身份校验

收派员身份校验应满足以下要求：

- a) 收派员进行快递收派业务时使用的智能终端设备应设定设备锁屏密码，登入设备时验证使用者身份是否终端所有者；
- b) 收派员使用的收派 App 等涉及个人信息访问的系统，应采用身份校验机制，如通过“账号+密码”校验。

12.2.2 访问控制

收派员权限控制应满足以下要求：

- a) 收派员应仅能查看本人的揽件、派件信息；
- b) 历史收派件信息查询宜设置仅能查询最近 1 个月的记录。

12.2.3 数据查阅

收派员数据查询应满足以下要求：

- a) 收派员进行快件收派时，寄递用户个人身份信息、电话号码等敏感信息应采取去标识化处理后展示，收派员联系客户时，宜通过收派 App 集成隐私联系保护方案来实现一键呼叫或短信发送，以保护寄递用户敏感信息；

注：隐私联系保护方案包括但不限于：虚拟号码、短信通知平台等。

- b) 收派员与寄递用户联系的录音宜统一指定路径保存，如需调取宜通过相应流程审批。

12.3 用户查单

12.3.1 适用场景

适用于通过客服热线查询个人快件信息的场景，包括互动式语音应答及人工客服场景。

12.3.2 身份校验

为防止他人仿冒寄递用户查询快件信息，服务运营者应遵守本文件 8.2 中 b) 规定的要求，同时还应通过查询人的致电号码与所查询快件预留的寄件用户和收件用户预留的电话号码进行对比，验证查询人身份：

- a) 号码一致时，确认其身份为寄件用户或收件用户，后续根据其提供的其它信息提供不同类型的查询服务；
- b) 号码不一致时，判定查询人为第三方，需引导其提供详细的收寄方电话号码、联系人、城市名与运单进行核对，相符则受理后续查询需求。

12.3.3 访问控制

客服人员仅能基于用户咨询、查阅、投诉等请求进行相关信息查询。

12.3.4 信息查询

服务运营者应根据其预先设置的信息查询规则反馈相应信息。根据是否提供单号，查询可分为有单号查询和无单号查询，有单号查询规则参见附录 F 中表 F.1，无单号查询规则参见附录 F 中表 F.2。

12.4 快件箱

12.4.1 视频监控

快件箱安装视频监控设备采集相关视频监控信息时应满足以下要求：

- a) 快件箱视频监控范围不应超出监控服务目的实现所需的最小范围；
- b) 快件箱安装相关视频监控设备的，应提示已进入视频监控范围；
- c) 快件箱采集到的视频监控信息，应采取如基于角色或基于任务的访问控制模型，防止非授权访问、篡改、删除；
- d) 快件箱运营者，应保存视频监控信息查阅记录，包括查阅人员、查阅目的、查阅对象、查阅时间等记录。

12.4.2 硬件设备安全

快件箱硬件设备的安全应满足以下要求：

- a) 快件箱运营者应采用设备锁等方式，防止向第三方暴露智能硬件外部接口；
- b) 快件箱硬件设备和第三方应用系统传输数据时，当涉及个人身份信息、电话号码、地址等敏感信息时，应采取加密的物联网通信协议，保证数据通信安全。

12.5 收派移动作业终端

12.5.1 数据存储安全

收派移动作业终端数据存储应遵守本文件 10.1 规定的要求，还应满足以下要求：

- a) 收派移动作业终端离线存储个人身份信息、电话号码、地址等敏感信息，当完成与服务端信息同步后，应立即删除终端离线存储的敏感信息；
- b) 收派移动作业终端离线存储个人身份信息、电话号码、地址等敏感信息，当无法完成与服务端信息同步时，应设置适当有效时长，当超出有效时长时，删除终端离线存储的敏感信息。

12.5.2 数据访问安全

收派移动作业终端数据访问应遵守本文件 8.2 规定的要求，还应满足以下要求：

- a) 收派移动作业终端安装的收派类 App，应设置登录有效时长（宜不超过 24 小时），超过时长应强制退出登录，避免终端设备丢失时数据被非授权访问；
- b) 收派移动作业终端安装的收派类 App，应在用户修改密码后退出登录状态，避免终端设备丢失时数据被非授权访问；
- c) 收派移动作业终端安装的收派类 App，应在用户账号更换设备登录时，进行双因素认证，避免账号密码泄露导致数据被非授权访问。

附录 A

(资料性)

快递物流服务数据分级分类示例

A.1 快递物流服务数据分类原则

快递物流服务数据分类应遵循以下原则：

- a) 系统性原则：数据分类应基于组织内所有数据的考量，建立一套层层划分、层层隶属、从总到分的分类体系，每一次划分应有单一、明确的依据；
- b) 规范性原则：确切表达数据类目的实际内容范围，在表达相同的概念时，保证用语一致性。快递物流行业已有统一数据用语的，使用统一数据用语；
- c) 稳定性原则：应选择分类对象最稳定的本质特性作为数据分类的基础和依据；
- d) 扩展性原则：划分数据类目层级应保留适当可扩展空间，利于分类数据增加时的扩展。

A.2 快递物流服务数据类别范围

快递物流服务涉及的数据类别为：用户数据、企业运营数据。类别示例参见表 A.1。

表 A.1 快递物流服务数据类别与示例

数据类别		示例
用户数据	个人用户数据	<ol style="list-style-type: none"> 1) 个人基础信息：姓名、生日、性别、国籍等； 2) 个人身份信息：身份证信息、驾驶证信息、军官证信息、护照信息、个人生物特征信息等； 3) 个人联系信息：个人电话号码、详细地址、电子邮箱等； 4) 个人财产信息：银行卡号、支付账号等； 5) 个人鉴权信息：账号登录密码、支付密码、密保答案、用户个人数字证书等； 6) 上网记录及通讯信息：聊天记录、网站浏览记录、通讯录等； 7) 网络身份标识信息：用户 PIN、个人设备识别号、用户 IP 地址、用户 MAC 地址、智能设备 ID 等； 8) 位置信息：精准定位信息、经纬度、行踪轨迹等。
	企业用户数据	<ol style="list-style-type: none"> 1) 企业基础信息：企业名称、营业执照、法人信息、注册地址等； 2) 企业鉴权信息：账号密码、支付密码、密保答案等； 3) 企业通信信息：联系人姓名、联系电话号码、联系邮箱、企业地址等； 4) 企业账户信息：企业账户信息、银行信息、税务登记号、付款方式等； 5) 企业信用信息：信用等级、信用账期、信用额度、信用折扣等。

表 A.1 快递物流服务数据类别与示例（续）

数据类别	示例
企业运营数据	1) 寄递物品及费用信息：物品名称、类型、性质体积、重量、数量、价值、代收金额、运费、付款方式等； 2) 配送信息：原寄地、目的地、快件路由信息、配送时间、时效类型、运输方式、运单信息等； 3) 签收信息：签收底单、电子存根等； 4) 客服售后信息：客服电话、投诉信息、客服录音、服务评价信息、退换货信息、工单处理结果等； 5) 营业场所信息：营业场所名称、营业场所地址、营业场所电话、营业场所联系人信息、监控视频等； 6) 财务信息：各项交易/财务运营数据、收入、成本、利润信息等； 7) 营销运营信息：营销策略、营销方案、广告投放等。

A.3 快递物流服务数据分级原则

快递物流服务数据分级应遵循以下原则：

- a) 就高原则：一个数据集中如存在不同等级的数据时，以最高等级的数据字段确定该数据集合的数据等级；
- b) 升级原则：在不同的业务场景、使用目的、使用范围或其他因素影响下，导致数据的重要程度及风险级别上升，或不同数据结合成一个数据集合，数据集合的重要程度及风险级别上升，需要进行升级处理。数据的安全级别升级示例参见表 A.2；
- c) 降级原则：数据经过技术处理后，如数据脱敏、数据加密、删除关键字段等，数据级别按照处理后数据的重要程度及风险级别进行降级处理。数据的安全级别降级参见表 A.2。

表 A.2 数据安全级别升降示例

措施	安全级别调整
汇聚融合	上升1级
生产数据脱敏后用于机构内部业务经营或管理工作	下降1级
汇聚融合后信息具有高安全风险	上升2级
脱敏/加密——从数据中去除能够直接定位到数据主体的内容、删除涉及商业秘密的内容后信息失去敏感性	下降2级
个人画像	上升1级

A.4 快递物流服务数据定级规则

A.4.1 数据定级要素

数据定级要素包括影响对象及影响程度。

- a) 影响对象，指数据安全属性遭到破坏后受到影响的对象，划分为：国家安全、公众权益、企业合法权益、个人合法权益。
- b) 影响程度，指数据安全属性遭到破坏后带来的影响大小，划分为：严重、中等、轻微。影响程度详细说明见表 A.3。

表 A.3 影响程度说明

影响	说明
严重	1) 可能导致全部业务无法开展,造成重大经济损失。 2) 可能引发或导致特别重大、重大安全事件。 3) 可能导致重大个人信息安全风险、侵犯个人隐私等严重危害个人权益的事件。 4) 可能引发公众广泛诉讼或集体诉讼,甚至引发群体性事件。 5) 可能导致监管部门严重处罚(包括取消经营资格、长期暂停相关业务等)的情况。
中等	1) 可能导致部分业务无法开展,造成较大经济损失。 2) 可能引发或导致较大安全事件。 3) 可能导致一定规模的个人信息泄露、滥用等安全风险,或对个人权益可能造成一定影响的事件。 4) 可能引发一定数量投资者对本机构诉讼。 5) 可能导致监管部门较严重处罚(包括一段时间内暂停经营资格或业务等)的情况。
轻微	1) 可能导致个别业务短时间无法开展,造成轻微的经济损失。 2) 可能引发或导致一般安全事件。 3) 可能导致超出个人用户授权加工、处理、使用数据的情况,对个人权益造成部分或潜在影响。 4) 可能导致至监管部门轻微处罚(包括罚款、公开批评等)的情况。 5) 可能对本机构声誉造成一定程度损害。

A.4.2 数据定级规则

依据数据定级要素及数据重要程度对快递物流服务的数据进行分级,从低到高依次划分为4级,1级是最低级,4级是最高级。

- a) 1级数据:已披露或通过公开渠道可以获取的数据,数据一旦丢失、泄露、篡改、受到破坏后对企业不会造成不利后果。
- b) 2级数据:数据一旦丢失、泄露、篡改、受到破坏后,对企业合法权益造成轻微影响,不会产生商誉损害、经济损失或法律责任。
- c) 3级数据:数据一旦丢失、泄露、篡改、受到破坏后,对公众权益或个人合法权益造成中等或轻微影响,或对企业合法权益造成中等影响。
- d) 4级数据:数据一旦丢失、泄露、篡改、受到破坏后,对国家安全造成影响,或对公众权益、企业合法权益、个人合法权益造成严重影响。

综上所述,数据安全级别划定规则见表A.4所示。

表 A.4 数据安全级别划定规则表

影响对象	影响程度		
	严重	中等	轻微
国家安全	4	4	4
公众权益	4	3	3
企业合法权益	4	3	2
个人合法权益	4	3	3

A.4.3 数据定级示例

根据本文件所属定级规则,数据类别及其建议划分的最低安全级别的示例参见表A.5。

表 A.5 快速物流服务数据定级示例

数据类别	子类	内容	最低安全级别参考
个人用户数据	个人基础信息	姓名、生日、性别等	2
	个人身份信息	个人生物特征信息等	4
		身份证信息、驾驶证信息、军官证信息、护照信息等	3
	个人联系信息	个人电话号码、详细地址、电子邮箱等	3
	个人财产信息	银行卡号、支付账号等	3
	个人鉴权信息	账户登录密码、支付密码、密保答案、用户个人数字证书等	4
	上网记录及通讯信息	聊天记录、网站浏览记录、通讯录等	3
	网络身份识别信息	IMEI 号、IP 地址、MAC 地址等设备唯一标识	2
	个人位置信息	精准定位信息、经纬度等	3
个人账户信息	账号、昵称等	1	
企业用户数据	企业基础信息	企业名称、营业执照、法人信息、注册地址等	2
	企业鉴权信息	账号登陆密码、支付密码、密保答案等	4
	企业通信信息	企业电话、联系人姓名、联系邮箱、企业地址等	2
	企业账户信息	企业账户信息、银行信息等	3
企业运营数据	寄递物品及费用信息	物品名称、性质、类型、数量、价值、代收金额等	3
		物品体积、重量、运费、付款方式等	2
	配送信息	运单详情等	3
		原寄地（城市级别）、目的地（城市级别）、快件路由信息、配送时间、时效类型、运输方式等	2
	签收信息	电子存根、签收底单（含个人电话号码地址信息）等	3
		签收底单（无个人电话号码地址信息）等	2
	售后信息	投诉信息、客服录音、退换货信息等	3
		服务评价信息、工单处理结果等	2
		客服电话等	1
	营业场所信息	营业场所监控视频等	2
		营业场所名称、营业场所地址、营业场所电话、营业场所联系人信息等	1
	财务信息	财务运营数据、成本利润数据等	3
营销运营信息	营销策略、营销方案、广告投放等	2	

附录 B

(资料性)

快递物流服务可选个人信息收集范围及使用要求

快递物流服务运营者可选个人信息收集范围及使用要求如表 B.1 所示：

表 B.1 快递物流服务可选个人信息收集范围及使用要求

个人信息类型	使用要求
签收信息（如签收笔迹、确认收货信息等）	仅用于提供基础服务，实现快递派件
寄件用户身份证明信息（如证件图片、证件号码等）	仅用于提供基础服务和开通定期结算服务，实现寄件用户身份查验、国际件、港澳台件清关、定期结算申请用户身份查验
收件用户身份证明信息（如证件图片、证件号码等）	仅用于提供基础服务、签单返还服务、开通定期结算服务，实现收件用户身份核验登记、国际件、港澳台件清关、定期结算申请用户身份查验
寄递运单号	仅用于提供基础服务和代收代派服务，实现查询运单信息、快递运输路径、标识快件
通话录音（客服热线）	仅用于提供基础服务，实现用户纠纷处理
聊天消息（在线客服）	仅用于提供基础服务，实现用户纠纷处理
网络日志（包括 IP 地址、用户登录时间、用户退出时间等）	仅用于风险控制，实现合规及网络安全保障
手机验证码或语音验证码	仅用于开通定期结算服务，实现定期结算申请用户身份查验
签收口令	仅用于口令签收，实现收件用户签收口令验证
寄递物品价值	仅用于保价服务，实现保价服务费计算
收件用户签章或身份证件复印件	仅用于签单返还，实现收件用户身份核验登记
待收卡号/账号	仅用于提供代收货款服务
收款人姓名	仅用于提供代收货款服务
收款人身份证号	仅用于提供代收货款服务
收款银行信息（银行卡号、持卡银行等）	仅用于提供代收货款服务
收款银行绑定手机号	仅用于提供代收货款服务
返款时间	仅用于提供代收货款服务
待收金额	仅用于提供代收货款服务
口令	仅用于提供会员服务，实现注册会员口令设置
国家/地区	仅用于提供会员服务，实现服务内容匹配推荐
入驻收派员手机号码	仅用于入驻收派员注册
入驻收派员姓名	仅用于入驻收派员注册，实现收派员身份查验
入驻收派员身份证件	仅用于入驻收派员注册，实现收派员身份查验
入驻收派员面部识别信息	仅用于入驻收派员注册，实现收派员身份查验
入驻收派员工作证信息	仅用于入驻收派员注册，实现收派员身份查验
入驻收派员第三方支付平台信息	仅用于支付结算，实现交易费用结算
入驻收派员地理位置信息	仅用于入驻收派员监控，实现履约行为和服务质量监管
入驻收派员手机设备信息	仅用于入驻收派员监控，实现履约行为和服务质量监管

附录 C

(资料性)

快递物流服务 App 相关系统权限申请范围及使用要求

快递物流服务 App 相关系统权限申请范围及使用要求如表 C.1、表 C.2 所示：

C.1 Android权限范围

表 C.1 Android App 相关系统权限申请范围及使用要求

权限名称	使用要求
写入外置存储器 WRITE_EXTERNAL_STORAGE	仅用于实现运单电子存根图片保存到本地、运单发票保存到本地功能
读取外置存储器 READ_EXTERNAL_STORAGE	仅用于访问相册进行图片上传
访问粗略位置 ACCESS_COARSE_LOCATION	仅用于获取服务网点
访问精准定位 ACCESS_FINE_LOCATION	仅用于服务网点查询、下单地址获取、地址快捷填写
相机 CAMERA	仅用于实名认证、扫码寄件、扫码支付、寄件托寄物拍照、访问相册信息功能

C.2 iOS权限范围

表 C.2 iOS App 相关系统权限申请范围及使用要求

权限名称	使用要求
相机 Camera	仅用于实名认证、扫码寄件、扫码支付、寄件托寄物拍照、访问相册信息功能
位置 Location	仅用于服务网点查询、下单地址获取、地址快捷填写
照片 Photos	仅用于访问相册进行图片上传、运单电子存根图片保存到本地功能、运单发票保存到本地

附 录 D
(资料性)
常见场景告知用户同意

表 D.1 告知用户同意的内容和方式

序号	业务场景	告知内容	告知方式
1	清关	清关信息采集的告知	<p>寄递用户收取国际或港澳台快递时，服务运营者应通过弹窗、页面明显提示等方式告知用户，获得用户主动授权同意，并提供用户上传通关信息的功能。</p> <p>注：清关短信告知内容参照：尊敬的客户，您好！您有一票通过XXX寄递的快件，为了确保您的货物顺利清关至中国内地，根据《中华人民共和国海关对进出境快件监管办法》，运单号XXX需要提供身份证正反面图片，若已上传可忽略此短信，上传方式如下：1. 点击身份证上传专属通道XXX进行上传。2. 微信上传：查找并关注XXX公众号，关注成功后选择【我的】→【通关服务】上传。如有疑问可拨打客服热线XXX，谢谢！</p>
2	转运	客户委托转运或无法到达的区域委托第三方承运的告知	<p>快递物流服务组织对于快件无法到达的区域，如通过委托第三方开展寄递服务的，应通过个人信息保护政策、寄递服务协议、电话等明确告知寄递用户关于第三方处理、使用个人信息的特定用途，取得寄递用户的明示同意，并应充分审查、评估第三方保护寄递用户个人信息的能力，签订寄递用户信息安全保障协议。</p>

附 录 E
(资料性)
数据脱敏方式举例

表 E.1 数据脱敏方式

数据类型	脱敏方式	举例
电话号码、证件号、银行卡号， 支付账号等	10 位以上，保留前三后四明文展示	137****123， 441*****0021
	10 位及 10 位以下，保留后四位明文展示	*****6666
地址类	使用星号*隐藏后六个字	广东省深圳市南山区高新南一道 *****
邮箱类	根据业务需要，使用星号*隐藏@前面全部或部分字符，或使用星号*隐藏@前面和后面的部分字符	*****@qq.com, *****@*.com

注：常用的脱敏技术如数据屏蔽，使用时必须在服务端实现数据脱敏，不应通过前端 js 脚本实现脱敏，同时应遵循统一脱敏原则。

附 录 F
(资料性)
信息查询反馈规则

表 F.1 有单号查询信息清单

查询项		寄件方	收件方	第三方个人用户
运单基础 信息	原寄地、目的地	√	√	×
	寄件方、收件方公司名称	√	√	×
	寄件人、收件人	√	√	×
	寄件人、收件人联系方式（电话号码）	√	√	×
	寄件地址、收件地址	√	√	×
寄递物品 及费用	寄递物品内容	√	√	×
	保价、声明价值、代收金额、运费、特殊操作 费用、部分增值服务费用	√	运费仅收件方为付 款方时能提供	×
	计费重量、实际重量、付款方式	√	√	√
快件状态 信息	快件路由信息（当前快件位置、派送状态等）	√	√	√
	时间（寄件时间、预计上门派送时间、快件承 诺时效、到达网点时间等）	√	√	√
	时效类型	√	√	√
	运输方式（如飞机、火车等）	√	√	√
	签收情况	√	√	只告知是否签收， 是否本人签收，不 告知具体签收人。

注：“√”表示该查询项在有单号时可被相应角色查询，“×”表示该查询项在有单号时亦不可被相应角色查询。例如 F.1 表中“原寄地、目的地”查询项，可被“寄件方”、“收件方”查询，但不可被“第三方个人用户”查询。

表 F.2 无单号查询信息清单

查询项		寄件方	收件方	第三方个人用户
运单基础信息	运单号	引导至各查询端（例如官方 App 或小 程序等）自助查询，或由用户提供收 寄双方城市名、电话号码、联系人进 行验证，若用户无法提供或是提供错 误则婉拒。		引导用户提供运单六要素（收寄双方 电话号码、城市名、联系人）进行核 实后提供，若用于无法提供或是提供 错误则婉拒。 注：不可主动报信息与用户核实

表 F.2 无单号查询信息清单（续）

查询项		寄件方	收件方	第三方个人用户
运单基础信息	原寄地、目的地	引导至各查询端（例如官方 App 或小程序等）自助查询，或由用户提供收寄双方城市名、电话号码、联系人进行验证，若用户无法提供或是提供错误则婉拒。		×
	寄件方、收件方公司名称			
	寄件人、收件人	用户提供单号后四位进行验证后告知。		×
	寄件人、收件人联系方式（电话号码）			
寄件地址、收件地址				
寄递物品及费用	寄递物品内容	√	√	×
	保价、声明价值、代收金额、运费、特殊操作费用、部分增值服务费用	√	运费仅收件方为付款方时能提供	×
	计费重量、实际重量、付款方式	√	√	√（需通过本表第一项完成运单号查询）
快件状态信息	快件路由信息（当前快件位置、派送状态等）	√	√	√（需通过本表第一项完成运单号查询）
	时间（寄件时间、预计上门派送时间、快件承诺时效、到达网点时间等）	√	√	√（需通过本表第一项完成运单号查询）
	时效类型	√	√	√（需通过本表第一项完成运单号查询）

表 F.2 无单号查询信息清单（续）

查询项		寄件方	收件方	第三方个人用户
快件状态信息	运输方式（如飞机、火车等）	√	√	√（需通过本表第一项完成运单号查询）
	签收情况	√	√	有条件提供：只告知是否签收，是否本人签收，不告知具体签收人。（需通过本表第一项完成运单号查询）
	问题件跟进记录	√	√	有条件提供：只可告知涉与其相关的问题件跟进进度。（需通过本表第一项完成运单号查询）

注：“√”表示该查询项在无单号时可被相应角色查询，“×”表示该查询项在无单号时亦不可被相应角色查询。例如 F.2 表中“托寄物内容”查询项，可被“寄件方”、“收件方”查询，但不可被“第三方个人用户”查询。

参 考 文 献

- [1] 中华人民共和国网络安全法（2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过）
- [2] 数据安全管理办法（征求意见稿）（2019年5月28日国家互联网信息办公室发布）
- [3] 关键信息基础设施安全保护条例（征求意见稿）（2017年7月10日国家互联网信息办公室发布）
- [4] 网络安全等级保护条例（征求意见稿）（2018年6月28日公安部发布）
- [5] 信息安全技术 个人信息安全影响评估指南（征求意见稿）（2018年06月11日全国信息安全标准化技术委员会发布）
- [6] 电信和互联网用户个人信息保护规定（2013年6月28日中华人民共和国工业和信息化部第2次部务会议审议通过）
- [7] 儿童个人信息网络保护规定（征求意见稿）（2019年5月31日国家互联网信息办公室发布）
- [8] 个人信息出境安全评估办法（征求意见稿）（2019年6月13日国家互联网信息办公室发布）
- [9] 个人信息和重要数据出境安全评估办法（征求意见稿修改稿）（2017年5月19日国家互联网信息办公室发布）
- [10] 数据出境安全评估指南（征求意见稿）（2017年8月30日全国信息安全标准化技术委员会发布）
- [11] 信息安全技术 信息安全风险评估规范（征求意见稿）（2018年01月19日全国信息安全标准化技术委员会发布）
- [12] 国家网络安全事件应急预案（2017年6月27日中央网信办发布）
- [13] 个人信息和重要数据出境安全评估办法（征求意见稿修改稿）（2017年5月19日国家互联网信息办公室发布）
- [14] 信息安全技术 恶意软件事件预防和处理指南（征求意见稿）（2018年06月11日全国信息安全标准化技术委员会发布）
- [15] GB/T 10757—2011 邮政业术语
- [16] GB/T 27917.2—2011 快递服务 第2部分：组织要求
- [17] GB/T 27917.3—2011 快递服务 第3部分：服务环节
- [18] GB/T 28582—2012 快递运单
- [19] 邮政行业安全信息报告和处理规定（2014年2月28日经国家邮政局2014年第4次局长办公会议审议通过）
- [20] 寄递服务用户个人信息安全管理规定（2014年2月28日经国家邮政局2014年第4次局长办公会议审议通过）