ICS ×××××

CCS W ××

**团 体 标 准**

T/YNIS 00X—20XX

信息安全技术 移动互联网应用程序(App)

个人信息保护合规指南 总则

**Information security technology — Mobile internet application personal information protection compliance guide general principal**

（待审稿）

2024-××-××发布 2024-××-××实施

云南省互联网协会 发布

目次

[前言 III](#_Toc163342349)

[1 范围 1](#_Toc163342350)

[2 规范性引用文件 1](#_Toc163342351)

[3 术语和定义 1](#_Toc163342352)

[4 缩略语 7](#_Toc163342353)

[5 个人信息处理基本原则 7](#_Toc163342354)

[5.1 合法正当原则 7](#_Toc163342355)

[5.2 目的明确原则 7](#_Toc163342356)

[5.3 告知同意原则 7](#_Toc163342357)

[5.4 最小必要原则 8](#_Toc163342358)

[5.5 公开透明原则 8](#_Toc163342359)

[5.6 安全保障原则 8](#_Toc163342360)

[5.7 主体参与原则 8](#_Toc163342361)

[5.8 用户设计原则 8](#_Toc163342362)

[6 个人信息的收集 9](#_Toc163342363)

[6.1 明确收集范围和要求 9](#_Toc163342364)

[6.2 个人信息告知同意 9](#_Toc163342365)

[6.3 个人敏感信息 12](#_Toc163342366)

[6.4 间接获取个人信息 13](#_Toc163342367)

[6.5 第三方应用收集个人信息 13](#_Toc163342368)

[6.6 其他要求 13](#_Toc163342369)

[7 个人信息的存储 14](#_Toc163342370)

[7.1 存储个人信息的类型及数量 14](#_Toc163342371)

[7.2 存储去标识化 14](#_Toc163342372)

[7.3 个人信息存储期限 14](#_Toc163342373)

[7.4 个人敏感信息的存储 15](#_Toc163342374)

[7.5 存储地点 15](#_Toc163342375)

[7.6 其他要求 15](#_Toc163342376)

[8 个人信息的使用 16](#_Toc163342377)

[8.1 个人信息的访问控制 16](#_Toc163342378)

[8.2 个人信息的展示 16](#_Toc163342379)

[8.3 个人信息的查询 16](#_Toc163342380)

[8.4 个人信息的更正 16](#_Toc163342381)

[8.5 个人信息的撤回 17](#_Toc163342382)

[8.6 个人信息的副本 17](#_Toc163342383)

[8.7 个人信息的举报、投诉和建议 17](#_Toc163342384)

[8.8 其他要求 17](#_Toc163342385)

[9 个人信息的加工 18](#_Toc163342386)

[9.1 用户画像 18](#_Toc163342387)

[9.2 个性化展示 18](#_Toc163342388)

[9.3 信息系统自动决策机制 19](#_Toc163342389)

[9.4 人工智能服务 19](#_Toc163342390)

[9.5 其他要求 19](#_Toc163342391)

[10 个人信息的传输 20](#_Toc163342392)

[10.1 个人信息传输告知 20](#_Toc163342393)

[10.2 个人信息跨境传输告知 20](#_Toc163342394)

[10.3 App 中的个人信息传输 20](#_Toc163342395)

[10.4 App 采用第三方SDK进行数据传输的要求 21](#_Toc163342396)

[11 个人信息的提供 21](#_Toc163342397)

[11.1 委托处理 21](#_Toc163342398)

[11.2 共享和转让 23](#_Toc163342399)

[11.3 共同处理 25](#_Toc163342400)

[11.4 收购、合并、分立、解散、被宣告破产时的个人信息转让 25](#_Toc163342401)

[11.5 个人信息跨境提供 25](#_Toc163342402)

[12 个人信息的公开 25](#_Toc163342403)

[12.1 个人信息公开披露 25](#_Toc163342404)

[12.2 个人信息涉及跨境的公开 26](#_Toc163342405)

[13 个人信息的删除 26](#_Toc163342406)

[13.1 违规处理用户个人信息 26](#_Toc163342407)

[13.2 个人信息的注销 26](#_Toc163342408)

[13.3 用户个人信息保存期限已届满 27](#_Toc163342409)

[13.4 其他要求 27](#_Toc163342410)

[附录A （资料性） 个人信息及个人敏感信息 28](#_Toc163342411)

[附录B （资料性） 去标识化与匿名化 29](#_Toc163342412)

[附录C （资料性） 个人信息的监管与法律责任 32](#_Toc163342413)

[附录D （资料性） 个人信息保护相关法律、司法解释、部门规章和标准文件索引 42](#_Toc163342414)

[参考文献 49](#_Toc163342415)

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。

请注意本文件的其他内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件由XXX提出，云南省互联网协会归口。

本文件起草单位：

本文件主要起草人：

信息安全技术 移动互联网应用程序(App)

个人信息保护合规指南 总则

# 范围

本文件规范了移动互联网应用程序在个人信息处理的全生命周期的基本原则、技术规范和管理要求，包括个人信息收集、存储、使用、加工、传输、提供、公开和删除。

本文件适用于移动互联网应用程序提供者APP开发建设中的个人信息保护合规评估和管理。

# 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 25069—2022 信息安全技术 术语

GB/T 37964—2019 信息安全技术 个人信息去标识化指南

GB/T 35273—2020 信息安全技术 个人信息安全规范

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

GB/T 42460—2023 信息安全技术 个人信息去标识化效果评估指南

# 术语和定义

GB/T 25069—2022、GB/T 37964—2019、GB/T 35273—2020、GB/T 41391—2022、GB/T 42460—2023界定的以及下列术语和定义适用于本文件。

3.1

移动互联网应用程序 **mobile internet application**

为移动终端设计和开发的应用程序，包括移动智能终端预置、下载安装的应用程序和小程序，简称移动应用或 App。

[来源：GB/T 41391—2022，3.1]

3.2

移动互联网应用程序提供者 **mobile application provider**

移动互联网应用程序的所有者、开发者或运营者，简称 App 提供者。

3.3

服务类型 **service type**

移动互联网应用程序提供的业务功能分类，如地图导航、网络约车、即时通信、网上购物、网络支付等。

[来源：GB/T 41391—2022，3.5]

3.4

业务功能 **business function**

满足用户具体使用目的的功能，分为基本业务功能和扩展业务功能。

[来源：GB/T 41391—2022，3.4]

3.5

基本业务功能 **basic business function**

移动互联网应用程序实现用户主要使用目的的业务功能。

[来源：GB/T 41391—2022，3.6]

3.6

扩展业务功能 **extended business function**

移动互联网应用程序所提供基本业务功能之外的其他业务功能。

[来源：GB/T 41391—2022，3.7]

3.7

个人信息 **personal information**

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注：个人信息常见类型参见附录 A。

[来源：GB/T 35273—2020，3.1]

3.8

个人敏感信息 **personal sensitive information**

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注：个人敏感信息常见类型参见附录 A。

[来源：GB/T 35273—2020，3.2，有修改]

3.9

必要个人信息 **necessary personal information**

保障移动互联网应用程序基本业务功能正常运行所必需的个人信息，缺少该信息移动互联网应用程序即无法实现基本业务功能。

[来源：GB/T 41391—2022，3.8]

3.10

个人信息主体 **personal information subject**

个人信息所标识或关联的自然人。

[来源：GB/T 35273—2020，3.3]

3.11

用户 **user**

使用移动互联网应用程序的个人信息主体。

[来源：GB/T 41391—2022，3.9]

3.12

个人信息处理 **personal information processing**

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等行为。

3.13

个人信息处理者 **personal information processor**

在个人信息处理活动中自主决定处理目的、处理方式的组织和个人。

3.14

收集 **collect**

直接或间接获取个人信息的行为。

注 1：直接获取个人信息的行为包括个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集行为。

注 2：间接获取个人信息的行为包括通过共享、转让、搜集公开信息等间接获取个人信息等行为。

3.15

存储 **store**

记录或保存个人信息的行为。

3.16

使用 **use**

利用个人信息实现个人信息处理者或个人信息主体的特定目的的过程。

3.17

加工 **process**

对个人信息进行判别，筛选，分类，排序，分析和再造的过程。

3.18

传输 **transmit**

个人信息在业务功能系统之间流转的过程。

3.19

提供 **provide**

个人信息在个人信息处理者和其他组织或个人之间传递的过程，包括委托处理、共享和转让。

注：委托处理是指个人信息处理者将个人信息委托其他组织或个人处理的过程。共享是指个人信息处理者向其他组织和个人发送个人信息，且双方分别对个人信息拥有独立控制权的过程。转让是指将信息处理权由一个处理者向另一个处理者转移的过程。

3.20

公开 **disclose**

向社会或不特定人群发布信息的行为。

[来源：GB/T 35273—2020，3.11]

3.21

删除 **delete**

在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

[来源：GB/T 35273—2020，3.10]

3.22

去标识化 **de-identification**

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。

注 1：去标识化的信息在借助额外信息可以识别或关联个人信息主体。

注 2：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

注 3：常见去标识化方法参见附录 B。

[来源：GB/T 35273—2020，3.15]

3.23

匿名化 **anonymity**

通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。

注 1：匿名化的信息借助额外信息也无法识别或关联个人信息主体。

注 2：匿名化的信息不属于个人信息。

注 3：常见的匿名化方法参见附录 B。

[来源：GB/T 35273—2020，3.14]

3.24

微数据 **microdata**

一个结构化数据集，其中每条（行）记录对应一个个人信息主体，记录中的每个字段（列）对应一个属性。

[来源：GB/T 37964—2019，3.4]

3.25

标识符 **identifier**

微数据中的一个或多个属性，可以实现对个人信息主体的唯一识别，标识符分为直接标识符和准标识符。

[来源：GB/T 37964—2019，3.6]

3.26

直接标识符 **direct identifier**

微数据中的属性，在特定环境下可以单独识别个人信息主体。

注：常见的直接标识符参见附录 B。

[来源：GB/T 37964—2019，3.7]

3.27

准标识符 **quasi-identifier**

微数据中的属性，结合其他属性可唯一识别个人信息主体。

注：常见的准标识符参见附录 B。

[来源：GB/T 37964—2019，3.8]

3.28

重标识 **re-identification**

把去标识化的数据集重新关联到原始个人信息主体或一组个人信息主体的过程。

注：常见的重标识方法包括分离（将属于同一个个人信息主体的所有记录提取出来）、关联（将不同数据集中关于相同个人信息主体的信息联系起来）、推断（通过其他属性的值以一定概率判断出一个属性的值）等方式。

[来源：GB/T 37964—2019，3.9]

3.29

完全公开共享 **completely public sharing**

数据一旦发布，很难召回，一般通过互联网直接公开发布。

[来源：GB/T 37964—2019，3.12]

3.30

受控公开共享 **completely public sharing**

通过数据使用协议对数据的使用进行约束。

[来源：GB/T 37964—2019，3.12]

3.31

领地公开共享 **completely public sharing**

在物理或者虚拟的所辖范围内共享，数据不能流出到领地范围外。

[来源：GB/T 37964—2019，3.14]

3.32

重标识风险  **re-identification risk**

标识度 **identifiability**

从数据中能识别出个人信息主体的概率。

[来源：GB/T 42460—2023，3.14]

3.33

第三方应用 **third-party application**

由移动互联网应用程序运营者之外的其他法人实体提供，通过移动互联网应用程序面向用户提供服务的应用程序。

注1：第三方应用提供的形式，通常包括SDK、小程序、Web页面等。如果SDK没有直接向用户提供服务，则不属于本文件所称的第三方应用。

注2：虽与App运营者属于不同法人实体，但与App运营者属于同一企业集团，且遵守同一套管理制度、统一进行安全和运维管理的，不属于App运营者的第三方。关联公司通常属于App运营者的第三方。

[来源：GB/T 41391—2022，3.17]

3.34

定向推送 **targeted push**

基于某一个人信息主体的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息，利用算法向该个人信息主体展示信息内容、提供商品或服务的搜索结果、推荐产品或服务、推送内容信息、广告营销等活动。

注：定向推送也称为个性化展示或个性化推荐。

[来源：GB/T 41391—2022，3.12]

3.35

自启动 **self-start**

移动互联网应用程序自动启动的行为。

3.36

关联启动 **associated start**

在一个移动互联网应用程序打开时，其他关联的应用程序自动启动的行为。

# 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

BSSID：基本服务集标识（Basic Service Set Identifier）

GPS:全球定位系统(Global Positioning System)

ICCID：集成电路卡识别码（Integrate Circuit Card Identity）

IMEI：国际移动设备识别码（International Mobile Equipment Identity）

IMSI：国际移动用户识别码（International Mobile Subscriber Identity）

MAC: 媒体访问控制 (Media Access Control)

MEID：移动设备识别码（Mobile Equipment Identifier）

OAID: 匿名设备标识符 (Open Anonymous Device Identifier)

SDK：软件开发工具包（Software Development Kit）

SN：设备序列号（Serial Number）

SSID：服务集标识（Service Set Identifier）

WAP：无线应用协议（Wireless Application Protocol）

Web：全球广域网（World Wide Web）

RSA：一种基于大整数因子分解问题的公钥密码算法（Rivest-Shamir-Adleman Algorithm）

# 个人信息处理基本原则

## 合法正当原则

个人信息处理者处理个人信息必须有合法依据，且处理个人信息的方式应当符合相关法律规范的规定。个人信息处理者在不损害个人权益的前提下进行个人信息的处理，明确不得以误导、欺诈、胁迫等方式取得个人的同意或违法违规进行个人信息处理，不应从非法渠道获取个人信息。

## 目的明确原则

个人信息处理者处理个人信息需要有明确、清晰、具体的目的，并且处理的信息应当与处理目的直接相关，不得在没有具体业务目的的情况下扩大处理个人信息的范围。

## 告知同意原则

个人信息处理者处理个人信息时，应向个人信息主体明示个人信息处理目的、方式、范围等规则，征求其授权同意后方能处理相关个人信息，该同意应当由个人在充分知情的前提下自愿、明确做出。个人信息处理者应把个人信息主体自主做出的肯定性动作，如主动点击、勾选、填写等，作为产品或服务的特定业务功能的开启条件。若处理的个人信息为个人敏感信息，应取得个人信息主体的单独同意。

## 最小必要原则

个人信息处理者处理个人信息应具有明确、合理的目的，应限于在为了实现处理目的所必要的最小范围内，不得收集与所提供服务无关的个人信息。并且采取对个人权益影响最小的方式进行，包括类型范围、数量范围、频率范围、精度范围、权限范围、使用期限等。

## 公开透明原则

公开透明原则要求个人信息处理者应以真实准确、清晰易懂、显著、合理的方式公开其处理个人信息的范围、目的、方式、规则等，获得个人的知情同意并接受公众监督。个人信息处理者应公开 App 个人信息保护政策、收集个人信息清单以及第三方共享个人信息清单，并且对App 接入的第三方应用、API、SDK 进行安全管理。

## 安全保障原则

个人信息处理者处理个人信息时，具备与所面临的安全风险相匹配的安全能力，具备健全的常态化机制和有效的应急响应机制，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性。

## 主体参与原则

个人信息处理者处理个人信息时，应向个人信息主体提供能够查询、更正、删除其个人信息，以及撤回授权同意、注销账户、投诉等方法，在向个人信息主体提供业务功能过程中使用个性化展示的，应显著区分个性化展示的内容和非个性化展示的内容。

## 用户设计原则

移动互联网应用程序在设计时，除了满足上述合法、正当、必要原则外，还应以用户体验为导向，将上述原则与产品设计相融合。

# 个人信息的收集

## 明确收集范围和要求

App 收集个人信息应在满足 GB/T 41391—2022 中 6.1、6.2、6.3、6.5要求的基础上，遵守以下要求：

1. App 提供者应按照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》明确 App 的服务类型，并根据服务类型划分 App 的基本业务功能和扩展业务功能，并确定必要个人信息范围和使用要求。要求用户必须提供的个人信息不应超出必要个人信息范围，满足信息收集的最小必要原则。
2. App 收集日历信息、应用程序列表、设备信息、短信信息、通话记录信息、通讯录信息、位置信息、生物识别信息、录音及拍摄录像信息、传感器信息、相册信息、存储文件等特定类型个人信息，应按照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》附录 C 的要求进行收集。
3. App 申请系统权限，应参考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》附录 E ，按照 App 的服务类型进行权限的申请。

## 个人信息告知同意

### 个人信息保护政策（隐私政策）

App应公开 App 个人信息保护政策（隐私政策），且应遵守以下要求：

1. 应以独立的页面形式存在。
2. 应便于访问，从进入应用后到访问隐私政策不应超过4次点击。
3. 应便于阅读，宜用白底黑字展示，正文字号不小于12号字，字体宜采用宋体，段落宜采用首行缩进2字符，分段清晰，行间距不少于1.5倍。
4. 应明确标识隐私政策发布、生效和更新日期，需列出更新说明和摘要内容。
5. 应对APP 提供者基本情况进行描述，至少包括：公司名称、公司常用/注册地址、个人信息保护相关负责人联系方式。
6. 应对APP 提供者在个人信息保护方面采取的措施和具备的能力进行说明，如身份鉴权、数据加密、访问控制、恶意代码防范、安全审计等。
7. 应对个人敏感信息进行显著标识，如字体加粗、标星号、下划线、斜体、颜色突出。
8. 应根据实际情形，逐一说明涉及收集个人信息的业务功能以及收集的目的、处理方式、个人信息种类、保存期限，不应使用“等、例如”等方式概括说明，且业务功能与个人信息类型应一一对应。
9. 应便于理解，文字段落描述宜清晰简洁，避免出现错别字、语病或带有歧义的描述。在使用专业术语时，宜对专业术语进行补充解释。
10. 应避免存在仅以用户改善功能、优化体验、定向推送信息、研发新产品、增强安全性等单独作为业务功能为由收集个人信息的描述。
11. 如有存在个人信息对外共享、转让、公开披露等情况，隐私政策应明确：
	1. 对外共享、转让、公开披露个人信息的目的；
	2. 涉及的个人信息类型；
	3. 接收方类型或身份。
12. 应对以下用户操作方法提供说明，且能进行有效操作：
13. 个人信息查询；
14. 个人信息更正；
15. 个人信息删除；
16. 用户账户注销；
17. 撤回已同意授权；
18. 获取个人信息副本的方法；
19. 对信息系统自动决策结果进行投诉的方法；
20. 响应个人信息主体的请求。
21. 应对征得个人信息主体授权同意的例外情形进行说明，如：
22. 与个人信息处理者履行法律法规规定的义务相关的；
23. 与国家安全、国防安全直接相关的；
24. 与公共安全、公共卫生、重大公共利益直接相关的；
25. 与刑事侦查、 起诉、审判和判决执行等直接相关的；
26. 出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；
27. 所涉及的个人信息是个人信息主题自行向社会公众公开的；
28. 根据个人信息主体要求签订和履行合同所必需的；
29. 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道；
30. 维护所提供产品或服务的安全稳定运行所必需的，如发现、处置产品或服务的故障；
31. 个人信息控制者为新闻单位，且其开展合法的新闻报道所必需的;
32. 个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的。
33. 应避免在隐私政策文件中出现免除自身责任（出现情况不承担责任）、加重用户责任、排除用户主要权利条款。
34. APP内如有收集儿童（14岁以下未成年人）的个人信息相关业务功能，应单独制定针对儿童个人信息保护规则的儿童版隐私政策，与隐私政策并列展示。

### 收集个人信息清单和第三方共享个人信息清单（双清单）

App应公开收集个人信息清单和第三方共享个人信息清单（双清单），在满足 6.2.1 中 a)、b)、c)、d)、e)、f)要求的基础上，还应满足以下要求：

1. 收集个人信息清单应清晰简洁列出已经收集到的个人信息基本情况，包括信息种类、使用目的、使用场景等，设计个人敏感信息的需要明确标识或突出显示。
2. 第三方共享个人信息清单应明示（包括委托的第三方或嵌入的第三方代码、SDK、插件）名称、开发者、版本号、主要名称、收集使用个人信息的目的、方式、范围、官网地址、隐私政策等基本信息的清单，同时还应提供对外委托、共享、转让、公开披露个人信息的目的、涉及的个人信息类型、使用场景、接收个人信息的第三方类型、信息处理方式、隐私政策或安全和法律责任清单等。

### 通用要求

App收集个人信息应在满足 GB/T 41391—2022 中 6.1、6.2、6.3、6.4、6.5、6.6、6.7要求的基础上，遵守以下：

1. App 首次运行时，应采用显著方式（如弹窗、图文、动画等）向用户告知隐私政策的主要内容，帮助用户理解该产品或服务的个人信息处理范围和规则，提示用户阅读隐私政策，并决定是否继续使用该产品或服务。
2. 隐私政策发生变更时，应采用显著方式（如弹窗、图文、动画等）向用户告知变更内容，提示用户阅读隐私政策，并取得用户的同意。
3. App 在征求用户同意隐私政策或其他个人信息相关协议条款时，需提供明确的同意或拒绝按钮，且不能使用“好的”“我知道了”等词语，不应设置默认勾选同意。
4. App 的服务或功能收集个人信息时，应同步告知用户该服务或功能收集使用个人信息的目的、处理方式、个人信息种类、保存期限，目的的描述应明确具体、通俗易懂。

注：例如，获取用户位置权限用于地图定位时，需要通过弹窗或浮窗方式同步告知用户该权限的用途：“需要申请定位权限用于 XX 服务的地图定位”。

1. 业务功能页面申请打开可收集个人信息权限时，应通过交互页面（如弹窗、浮层、文字说明、提示条等形式）同步告知用户收集目的，征得用户的明示同意。
2. App 在未获得用户同意前，不应提前收集个人信息。
3. 使用 Cookie 等同类技术(包括脚本、Clickstream、Web 信标、Flash Cookie、内嵌 web 链接、SDK等)收集个人信息时，应向用户明示所收集个人信息的目的、处理方式、个人信息种类、保存期限。
4. 不应通过捆绑不同类型的服务、功能，要求个人信息主体一次性同意个人信息收集请求。
5. App 应仅在用户使用业务功能期间，收集该业务功能所需的个人信息。当 App 在静默状态或后台运行，且未向用户提供服务时，不应收集用户个人信息。
6. App 更新升级后，不应更改用户原有的个人信息相关设置选项和系统权限。
7. 用户拒绝或撤回 App 个人信息收集或个人信息权限的同意时，App 应满足：
8. 不应强制退出或者关闭App；
9. 不应拒绝提供与上述个人信息无关的业务功能使用；
10. 不应频繁申请授权影响用户正常使用，除非由用户主动触发业务功能，且没有该个人信息或权限参与此业务功能无法实现。

注：频繁的形式包括不限于：

1. 单个场景在用户拒绝授权后， 48h内弹窗提示用户打开权限超过 1 次；
2. 每当用户重新打开App 或使用其他无关的业务功能时，都会再次向用户索要授权或提示用户缺少相关授权。
3. 征求用户同意时，不应通过强迫、误导欺骗、默认勾选等方式获得用户同意。

## 个人敏感信息

### 个人敏感信息收集

App 收集个人敏感信息时，在满足6.1、6.2要求的基础上，还应满足以下要求：

1. 有收集个人敏感信息的服务或功能时，应在隐私政策进行告知，还应在相应业务功能页面进行告知。
2. 业务功能页面收集个人敏感信息时，应通过交互页面（如弹窗、文字说明、提示条、提示音等形式）同步告知收集的目的、处理方式、个人信息种类、保存期限，向用户告知收集敏感个人信息的必要性以及对个人权益的影响，并取得用户的单独同意。

注：单独同意不应默认勾选，应单独向用户进行征询，如设置弹窗选项、勾选框等方式。

### 未成年人个人信息收集

App 收集未成年人个人信息时，在满足6.1、6.2、6.3.1要求的基础上，还应满足以下要求：

1. App 收集年满 14 周岁未成年人的个人信息，应征得监护人或未成年人同意；收集未满 14 周岁未成年人的个人信息，应征得其监护人的单独同意。
2. App 收集未满 14 周岁未成年人个人信息，应制定专门的个人信息保护政策，包括：
	1. 未成年人个人信息的处理目的、处理方式；
	2. 处理的未成年人个人信息种类、保存期限；
	3. 用户行使个人信息权利的方式和程序；
	4. 处理未成年人个人信息的必要性；
	5. 对未成年人个人权益的影响；
	6. App 提供者的名称、联系人姓名和联系方式。

## 间接获取个人信息

App 提供者存在间接获取个人信息的情形，应遵守以下要求：

1. 应通过合同或协议保障个人信息来源的合法性。
2. 应通过合同或协议明确告知用户通过间接渠道获取的个人信息的授权范围。
3. App提供者间接获取个人信息时，超出授权范围的，应重新征得个人信息主体的同意或通过个人信息提供方重新征得用户同意。
4. 间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。
5. 不应从非法渠道获取个人信息。

## 第三方应用收集个人信息

App 通过第三方应用收集个人信息应在满足 GB/T 41391—2022 中 6.6 要求的基础上，应遵守以下要求：

1. App 提供者应向用户明示：
	1. 第三方应用收集个人信息的目的、方式和范围；
	2. 第三方应用申请的系统权限和申请目的；
	3. App 提供给第三方应用的个人信息种类、保存期限、停止接入后的个人信息处理方式；
	4. 双方的个人信息安全责任和保护措施；
	5. 第三方应用协助 App 响应应用户个人信息权利请求的措施。
2. App 提供者应提示用户阅读第三方应用的个人信息收集使用规则，并取得用户的同意，涉及个人敏感信息收集的，需要征得用户的单独同意。
3. App未经用户同意不应私自截留用户仅向第三方应用提供的个人信息。
4. App 提供者应提供给用户撤回或关闭对第三方应用可收集个人信息权限的授权，以及向第三方应用提供个人信息的授权的功能或途径。

## 其他要求

App 收集个人信息应在满足 GB/T 41391—2022 中 6.7要求的基础上，满足以下要求：

1. App 及内嵌 SDK 未向用户告知且未经用户同意，在非服务所必需或者无合理场景下，不应自启动或者关联启动其他 App。若提供服务所必需且在合理场景下的自启动和关联启动，需向用户进行明示告知，在经用户同意且需由用户自主选择是否开启。
2. 如存在读取剪切板或公共存储区的行为，应告知用户读取的信息范围和使用目的，不应在未取得用户同意的情况下，收集剪切板中的个人信息和公共存储区中的个人信息。
3. 不应通过诱导、欺骗的方式，误导用户提供与 App 业务功能无关的个人信息或权限。
4. 未经用户主动选择同意，不得强迫下载、安装、打开 APP，不得诱导欺骗用户点击跳转或使用第三方应用。
5. 未经用户同意不应更改其设置的可收集个人信息权限状态，包括系统权限、设置选项等。
6. 向用户推荐下载 App 时应提供被下载 App 的相关信息，向用户推荐下载 App 时应同步提供取消下载的选项。

# 个人信息的存储

## 存储个人信息的类型及数量

App 提供者在存储个人信息时应满足以下要求：

1. 个人信息存储期限应为实现个人信息主体授权使用的目的所必需的最短时间，法律法规另有规定或者个人信息主体另行授权同意的除外。

注：不同行业对个人信息的存储期限另有具体规定，例如《金融机构客户身份识别和客户身份资料交易记录保存管理办法》规定：对于客户身份资料、客户交易信息，在业务关系和交易结束后，应当至少保存5年。例如《电子商务法》规定：商品和服务信息、交易信息保存时间自交易完成之日起不少于3年。

1. 存储时将个人信息和个人敏感信息进行区分，对不同类型的个人信息进行不同的访问和使用的权限管理。
2. 存储个人信息的类型及数量应遵循最小必要原则，不应超出业务场景的实际需要。法律法规另有规定的除外。
3. 隐私政策条款应明确说明：
	1. 个人信息的存放地域；
	2. 个人信息的存储期限；
	3. 个人信息的超期处理方式。

## 存储去标识化

App 收集个人信息后宜采用假名、抑制、泛化、随机化等技术立即进行去标识化处理，并采取技术和管理方面的措施，将可用于恢复识别个人的信息与去标识化的信息进行分开存储并加强访问和使用的权限管理。

## 个人信息存储期限

App 存储个人信息的期限应满足以下要求：

1. 存储个人信息的时间应遵循最小必要原则，即存储个人信息的时间，应当为实现处理目的所需的最短时间。
2. 针对个人信息的敏感性分别设立保存期限。
3. 超出个人信息存储期限后，应对个人信息进行删除或匿名化处理。
4. 法律法规另有规定或者个人信息主体另行同意的除外。

## 个人敏感信息的存储

App 存储个人敏感信息的应满足以下要求：

1. 存储个人敏感信息时，不可明文存储，应采用加密等安全措施，且所使用的加密算法应符合国家相关法律法规和行业标准。
2. 个人生物识别信息应与个人身份信息分开存储，宜分开不同的数据库进行存储，个人生物识别信息宜采用对象存储服务进行存储。
3. 原则上不应存储原始个人生物识别信息（如样本、图像、声音等），可采取的措施包括但不限于：
	1. 仅存储个人生物识别信息的摘要信息，且所使用的摘要算法应符合国家相关法律法规和行业标准；
	2. 在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能；
	3. 在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。

## 存储地点

App 存储个人信息的地点建议满足以下要求：

1. App 提供者应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。
2. 国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行安全评估。安全评估可以要求有关部门提供支持与协助。

## 其他要求

App 存储个人信息时，应满足以下要求：

1. App 提供者若委托第三方进行个人信息存储时，应向用户明示存储方及其存储规则。
2. App 提供者或委托存储方需建立个人信息安全防护和应急机制，确保个人信息存储期间的数据安全。

# 个人信息的使用

## 个人信息的访问控制

App 提供者应对个人信息的访问进行控制，需满足以下要求：

1. 应建立健全内部数据管理制度，包括数据管理、数据分级、数据访问、数据流转等，并建立和维护相关人员名单。
2. 应建立个人信息的重要操作内部审批流程，如进行批量修改、拷贝、下载等重要操作。
3. 授权访问个人信息的人员，应使用按照“最小授权，最小必要”原则的访问控制策略，使其只能访问职责所需的最小必要的个人信息，且进具备完成职责所需的最少的数据操作权限，并对访问和数据操作信息进行记录，并保存台账，包括访问人、操作行为、操作时间。
4. 应对安全管理人员、数据操作人员、审计人员的角色进行“三员分离原则”。
5. 应对个人信息操作使用的人员的操作流程建立完备的管理制度，并对流程内容进行审批，保存相关记录至少180天。
6. 涉及个人敏感信息的访问、修改等操作行为，宜在对角色权限控制的基础上，按照业务流程的需求触发操作授权。

## 个人信息的展示

App 或相关系统涉及通过界面展示个人信息的（如显示屏幕、纸面），包括App产品或服务界面以及系统管理界面，App 提供者宜对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。同时需要对个人信息进行访问权限控制，例如，在个人信息展示时，防止内部非授权人员及个人信息主体之外的其他人员未经授权获取个人信息。

## 个人信息的查询

App 提供者应向个人信息主体提供查询下列信息的方法：

1. 其所持有的关于该主体的个人信息或类型。
2. 上述个人信息的来源、所用于的目的。
3. 已经获得个人信息的第三方身份或类型。

## 个人信息的更正

个人信息主体发现 App 提供者所持有的该主体的个人信息有错误或不完整的，App 提供者应为其提供请求更正或补充信息的方法。提供人工更正的，受理和处理时间不宜超过10个工作日，最长不宜超过15个工作日。

## 个人信息的撤回

App 提供者应满足以下要求：

1. 应向个人信息主体提供方法撤回收集、使用其个人信息的同意授权。撤回同意后，App 提供者后续不应再处理相应的个人信息。
2. 应保障个人信息主体拒绝接收基于其个人信息推送的商业广告的权利，提供撤回同意的方法。
3. 对外共享、转让、公开披露个人信息，应向个人信息主体提供撤回同意的方法。

注：撤回授权同意不影响撤回前基于授权同意的个人信息处理。

## 个人信息的副本

App 提供者应满足以下要求：

1. 应为个人信息主体提供获取以下类型个人信息副本的方法，或在技术可行的前提下直接将以下类型个人信息的副本传输给个人信息主体指定的第三方：
	1. 本人的基本资料、身份信息。
	2. 本人的健康生理信息、教育工作信息。
2. 应在承诺期限内完成个人信息的副本提供，不宜超过10个工作日，最长不应超过15个工作日。

## 个人信息的举报、投诉和建议

App 提供者应满足以下要求：

1. 应建立建立并公布个人信息安全投诉、举报渠道，包括不限于电话、邮箱、在线客服、在线表格、即时通信账号等。
2. 应在 App明显位置设置举报、投诉和建议入口，不宜超过 5 次点击。
3. 应在承诺期限内完成举报、投诉和建议处理，不宜超过10个工作日，最长不应超过15个工作日。

## 其他要求

App 提供者应满足以下要求：

1. 使用个人信息时，不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意。
2. App 应设置简单便捷的功能或选项，便于个人信息主体在线行使其访问、更正、删除、撤回授权同意、注销账户等权利。

# 个人信息的加工

## 用户画像

App 提供者建议应满足以下要求：

1. 应在隐私政策向用户明示告知用于加工用户画像的个人信息的类型、目的、方式和应用场景，以及个人信息保护相关规则。
2. 用户画像中对个人信息主体的特征描述，不应：
	1. 包含淫秽、色情、赌博、迷信、恐怖、暴力的内容；
	2. 表达对民族、种族、宗教、残疾、疾病歧视的内容。
3. 在业务运营或对外业务合作中使用用户画像的，不应：
	1. 侵害公民、法人和其他组织的合法权益；
	2. 危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序。

## 个性化展示

App 提供者应满足以下要求：

1. 应在隐私政策向用户明示告知用于个性化展示所需的个人信息的类型、目的、方式、应用场景以及个性化展示的内容，以及个人信息保护相关规则，以及个人信息保护相关规则。
2. App使用个性化展示时，应通过“定推、推荐、关注、猜你喜欢”的字样或设置不同的栏目、模块，显著区分个性化展示和非个性化展示的内容。
3. App 提供个性化展示的，应提供关闭个性化展示的选项。
4. 在向用户提供电子商务服务的过程中，根据用户的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的个性化展示的，应当同时向用户提供不针对其个人特征的选项。
5. 自动化决策不应根据消费者的偏好、交易习惯等特征，利用算法在交易价格等交易条件上实施不合理的差别待遇等违法行为。
6. 在向用户推送新闻信息服务的过程中使用个性化展示的，应为用户提供简单直观的退出或关闭个性化展示模式的选项。
7. 当用户退出或关闭个性化展示模式时，App 应向用户提供删除或匿名化定向推送活动所基于的个人信息的选项。
8. 当用户删除或匿名化向推送活动所基于的个人信息时，服务端需及时删除或匿名化用于定向推送的个人信息，若这些信息在其他业务功能需要用到，则应立即停止这些个人信息在定向推送方面的应用。
9. 在向用户提供业务功能的过程中使用个性化展示的，宜建立用户对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制，保障用户调控个性化展示相关性程度的能力。
10. App利用个人信息进行个性化展示时，需使得用户可自主控制用于个性化展示的个人信息类型。用户通过选择用于个性化展示的个人信息类型，可以控制个性化展示与用户本身的相关程度。

## 信息系统自动决策机制

App 提供者业务运营所使用的信息系统，具备自动决策机制且能对个人信息主体权益造成显著影响的（例如，自动决定个人征信及贷款额度，或用于面试人员的自动化筛选等），应满足以下要求：

1. 应在隐私政策或服务页面向用户明示告知自动决策机制和规则。
2. 应向个人信息主体提供针对自动决策结果的投诉渠道，并支持对自动决策结果的人工复核。
3. 应在规划设计阶段或首次使用前开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施。
4. 应在使用过程中定期（至少每年一次）开展个人信息安全影响评估，并依评估结果改进保护个人信息主体的措施。

## 人工智能服务

提供人工智能服务的App 提供者，应满足以下要求：

1. 应在隐私政策向用户明示告知人工智能服务涉及的个人信息的类型、目的、方式和应用场景，以及个人信息保护相关规则，以及个人信息保护相关规则。
2. 应依法开展预训练、优化训练等训练数据处理活动，涉及个人信息的，应当取得个人信息主体同意或者符合法律、行政法规规定的其他情形。
3. 应当加强训练数据管理，采取必要措施保障训练数据安全。
4. 对用户的输入信息和使用记录应依法履行保护义务，不应收集非必要个人信息，不应非法留存能够识别使用者身份的输入信息和使用记录，不应非法向他人提供使用者的输入信息和使用记录。
5. 提供人脸、人声等生物识别信息编辑功能的，应当提示服务使用者依法告知被编辑的个人，并取得其单独同意。

## 其他要求

App 在进行个人信息加工时，应满足以下要求：

1. 加工个人信息时，不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意。
2. 如所收集的个人信息进行加工处理而产生的信息，能够单独与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，应将其认定为个人信息。对其处理应遵循收集个人信息时获得的授权同意范围。
3. 加工处理而产生的个人信息属于个人敏感信息的，对其处理需符合对个人敏感信息的要求。

# 个人信息的传输

## 个人信息传输告知

App 提供者应满足以下要求：

1. 应告知用户所传输的个人信息的传输方式、安全措施等。
2. 如果传输的个人信息中存在个人敏感信息，则应采用个人敏感信息处理的“保护优先于利用原则”对传输的个人敏感信息情况先予以明确告知，并征得用户同意。
3. 如果通过嵌入第三方代码、插件等方式将个人信息传输至第三方服务器，应通过弹窗提示等方式明确告知用户，向用户告知第三方的身份、联系方式、处理目的、处理方式和个人信息的种类。

## 个人信息跨境传输告知

如果存在跨境信息传输情况，则传输过程应遵守《个人信息保护法》第三十八条及第四十条规定，同时需要满足《数据安全法》、《网络安全法》、《中华人民共和国反电信网络诈骗法》等法律法规及相关技术标准要求。

## App 中的个人信息传输

App与服务器的通讯中涉及个人信息的通讯数据包，均应采取安全方式传输：

1. 采用HTTPS模式：服务器端应配置数字证书，移动互联网应用程序端可选配置数字证书。通讯中，双方采用TLS安全传输协议完成单向或双向身份验证后，再进行个人信息的安全传输。TLS协议应选用1.2及以上版本，非对称算法应采用RSA2048及以上强度算法，散列算法应采用SHA-256及以上强度算法，不得使用MD4、MD5、SHA-1等高风险算法。
2. 采用Socket模式：使用TCP/UDP协议进行通信，由移动互联网应用程序开发机构自行实现传输数据的加密机制。实现数据传输加密机制中，宜使用ZUC/SM2/SM3/SM4等国密算法。
3. 采用WSS模式：
	1. 单向模式下，服务器端配置SM2withSM3算法的数字证书；
	2. 双向模式下，移动互联网应用程序及服务器端采用RSA2048及以上强度算法，散列算法应采用SHA256及以上强度算法，不得使用MD4、MD5、SHA-1等高风险算法。在该模式下，如果是移动互联网应用程序开发机构自行实现客户端与服务端，则应采用SM2withSM3算法的数字证书；
4. 采用RPC over TLS模式：移动互联网应用程序及服务器端根据接口要求自行实现安全协议，数字证书宜采用SM2withSM3算法。
5. 小程序在传输个人敏感信息的时候，应采用小程序所在平台要求的加密传输方式。

以上a)/b)/c)/d)条目中客户端宜采用TLS/SSL PINNING技术实现证书或公钥锁定，防止中间人抓取数据。

## App 采用第三方SDK进行数据传输的要求

App采用第三方SDK实现个人信息安全传输，应满足以下要求：

1. 在数据安全传输前，SDK应能够对参与通讯的实体进行单向或双向的身份认证。
2. SDK应提供接口，对传输的数据进行加密。
3. SDK不得在非授权情况下，向第三方传输数据。
4. SDK不得采用弱密码算法或存在安全漏洞的密码算法。

# 个人信息的提供

## 委托处理

### 委托处理个人信息要求

App提供者应满足：

1. 应与受托人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，并对受托人的个人信息处理活动进行监督。
2. 委托第三方处理用户个人信息，不应超出已征得用户授权同意的范围，除非委托第三方处理用户个人信息符合以下所列情形之一：
	1. 与个人信息处理者履行法律法规规定的义务相关的；
	2. 与国家安全、国防安全直接相关的；
	3. 与公共安全、公共卫生、重大公共利益直接相关的；
	4. 与刑事侦查、起诉、审判和判决执行等直接相关的；
	5. 出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；
	6. 所涉及的个人信息是个人信息主体自行向社会公众公开的；
	7. 根据个人信息主体要求签订和履行合同所必需的；

注：个人信息保护政策的主要功能为公开个人信息处理者收集、使用个人信息范围和规则，不宜将其视为合同；

* 1. 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道；
	2. 维护所提供产品或服务的安全稳定运行所必需的，如发现、处置产品或服务的故障；
	3. 个人信息处理者为新闻单位，且其开展合法的新闻报道所必需的；
	4. 个人信息处理者为学术研究机构，出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的。

### 进行个人信息安全影响评估

在委托第三方处理用户个人信息前，App提供者应对委托行为进行个人信息安全影响评估，确保受委托方已建立适当的数据安全能力，落实必要的管理和技术措施，防止个人信息的泄漏、损毁、丢失、篡改。

### 确保受托方的个人信息处理符合要求

受托方处理用户个人信息时，应满足以下要求：

1. 受托方应按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息。
2. 委托合同不生效、无效、被撤销或者终止的，受托方应将个人信息返还个人信息处理者或者予以删除，不得保留。
3. 受托方因特殊原因未按照App提供者的要求处理个人信息的，应及时向App提供者反馈；
4. 受托方确需再次委托时，应事先征得App提供者的授权；
5. 受托方应协助App 提供者响应用户作为个人信息主体基于法律法规的规定提出的查阅、更正、删除、撤回、注销等权利请求；
6. 受托方在处理个人信息过程中无法提供足够的安全保护水平或发生了安全事件的，应及时向App提供者反馈；
7. App提供者应通过包括但不限于合同规定受委托方的责任和义务、对受委托方进行审计等方式，对受委托方的个人信息处理活动进行监督。

### 委托方的其它个人信息处理义务

委托方在处理个人信息时，需尽到以下义务：

1. 应在委托第三方处理用户个人信息前，向用户明示告知受托方的名称、联系方式、处理目的、处理方式和个人信息的种类，以及可能产生的后果，并事先取得用户的单独同意。
2. 应建立个人信息处理受托方名单，并定期维护。
3. 应建立受托方管理机制和工作流程，应建立相应安全评估和审计机制。
4. 应准确记录和存储委托处理个人信息的情况；
5. 得知或发现受委托方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，应立即要求受托方停止相关行为，且采取或要求受托方采取有效补救措施，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；必要时应终止与受托方的业务关系，并要求受托方及时删除从App提供者处获得的个人信息。

## 共享和转让

### 进行个人信息安全影响评估

在向第三方以共享、转让等方式提供用户个人信息前，App提供者应就上述对外提供个人信息的行为，进行个人信息安全影响评估，并依评估结果采取有效地保护用户的措施。

### 获取个人信息主体的知情同意

App 在对外提供个人信息时，需获取个人信息主体的知情同意，满足以下要求：

1. 在向第三方以共享、转让等方式提供用户个人信息前，App提供者应向用户明示告知接收方的名称、联系方式、处理目的、处理方式和个人信息的种类，以及可能产生的后果，并事先取得用户的单独同意。
2. 向第三方提供用户个人敏感信息，除a）中告知的内容外，还应向用户告知对外提供敏感个人信息的类型，必要性，对用户个人权益的影响，以及接收方的数据安全能力，并事先取得用户的单独同意。
3. 若存在以下所列情形之一，则App提供者对外提供用户个人信息，不必事先取得用户的单独同意：
	1. 与个人信息处理者履行法律法规规定的义务相关的；
	2. 与国家安全、国防安全直接相关的；
	3. 与公共安全、公共卫生、重大公共利益直接相关的；
	4. 与刑事侦查、起诉、审判和判决执行等直接相关的；
	5. 出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；
	6. 个人信息主体自行向社会公众公开的个人信息；
	7. 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道。
4. 若向第三方以共享、转让等方式提供的个人信息已经过去标识化处理，且确保数据接收方无法重新识别或关联个人信息主体，则App提供者无需获取用户知情同意。

### 共享和转让的其它义务

App 提供者通过共享和转让处理个人信息时，需尽到以下义务：

1. 应通过合同等方式规定用户个人信息接收方的责任和义务。
2. 应建立个人信息共享和转让方名单，并定期维护。
3. 应建立共享和转让方的管理机制和工作流程，应建立相应安全评估和审计机制。
4. 应准确记录和存储个人信息的对外提供状况，包括共享或转让用户个人信息的日期、规模、目的，数据接收方的基本情况等。
5. App提供者发现接收方违反法律法规要求或双方约定处理个人信息的，应立即要求数据接收方停止相关行为，且采取或要求接收方采取有效补救措施控制或消除个人信息面临的安全风险，如更改口令、回收权限、断开网络连接等。必要时App提供者应解除与接收方的业务关系，并要求接收方及时删除从App提供者获得的个人信息。
6. App提供者应承担因共享、转让个人信息发生安全时间而对个人信息主体合法权益造成损害的相应责任。
7. App提供者应帮助个人信息主体了解接收方对个人信息的保存、使用、保护方式等情况，以及个人信息主体的权利，例如个人信息的访问、更正、删除、注销账户等。
8. 个人生物识别信息原则上不应共享、转让。因业务需要，确需共享、转让的，应单独向个人信息主体告知目的、涉及的个人生物识别信息类型、接收方的具体身份、联系方式和其数据安全能力等，并征得个人信息主体的明示同意。

### 第三方接入的特定管理要求

App提供者在进行第三方产品或服务接入时，应满足以下要求：

1. 应建立第三方产品或服务接入管理机制和工作流程，应建立安全评估等机制设置接入条件。
2. 应与第三方产品或服务提供者通过合同等形式明确双方的安全责任及应实施的个人信息安全措施；妥善留存平台第三方接入有关合同和管理记录，确保可供相关方查阅。
3. 应在App业务界面明确标识产品或服务由第三方提供，且注明第三方名称、资质、个人信息处理规则等信息。
4. 应要求第三方根据11.2.2中相关要求向用户征得收集个人信息的授权同意，必要时核验其实现的方式。
5. 应建立第三方接入名单，并定期维护。
6. 应要求第三方产品或服务建立响应个人信息主体请求和投诉等的机制，以供个人信息主体查询、使用。
7. 应监督第三方产品或服务提供者加强个人信息安全管理，发现第三方产品或服务没有落实安全管理要求和责任的，应及时督促整改，必要时停止接入。
8. 产品或服务嵌入或接入第三方自动化工具（如代码、脚本、接口、算法模型、软件开发工具包、小程序等）的，宜采取以下措施：
	1. 嵌入和接入前对该工具进行安全评估，比如技术检测，确保其个人信息收集、使用行为符合约定要求；
	2. 定期对第三方嵌入或接入的自动化工具收集个人信息的行为进行审计，发现超出约定的行为，及时切断接入。

## 共同处理

当App提供者与第三方为共同个人信息处理者时，App提供者应通过合同等形式与第三方共同确定应满足的个人信息安全要求，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，并向用户明确告知。

## 收购、合并、分立、解散、被宣告破产时的个人信息转让

当App提供者因收购、合并、分立、解散、被宣告破产等原因发生变更时，应提前向用户告知有关情况，同时明示告知个人信息的处理方式。

App提供者需要转移个人信息时，应向用户告知接收方的名称或者姓名和联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的，应重新取得个人同意。

App提供者破产且无接收方的，应对用户个人信息做删除或匿名化处理。

## 个人信息跨境提供

在中华人民共和国境内运营中收集和产生的个人信息向境外提供的，App提供者应遵循国家相关规定和相关标准的要求。

# 个人信息的公开

## 个人信息公开披露

个人信息原则上不应公开披露。 App提供者经法律授权或合理事由确需公开披露时，应符合以下要求：

1. 公开披露前应对披露内容进行个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施。
2. 公开披露前应向个人信息主体告知公开披露个人信息的目的、类型，并事先征得个人信息主体的明示同意。若公开披露涉及个人敏感信息的，应告知涉及的个人敏感信息的内容。
3. 应对个人信息披露情况进行记录和存储，包括公开披露的日期、规模、目的、公开范围等。
4. App 提供者应承担因公开披露个人信息对个人信息主体合法权益造成损害的相应责任。
5. 不应公开披露个人生物识别信息，不应公开披露我国公民的种族、民族、政治观点、宗教信仰等个人敏感数据的分析结果。
6. 若公开披露的个人信息涉及去标识化处理，不同的公开共享类型对去标识化的要求如下：
	1. 完全公开共享：可能的重标识风险较高，对去标识化的要求较高；
	2. 受控公开共享：可能的重标识风险中等，对去标识化的要求中等；
	3. 领地公开共享：可能的重标识风险较低，对去标识化的要求较低。

## 个人信息涉及跨境的公开

在中华人民共和国境内运营中收集和产生的个人信息向境外提供进行公开披露的，App 提供者应遵循国家相关规定和相关标准的要求。

# 个人信息的删除

## 违规处理用户个人信息

App 提供者在下列情形中处理个人信息的，应满足以下要求：

1. App违反法律法规规定，或违反与用户的约定，收集、使用个人信息，或用户要求删除个人信息时，App提供者应提供删除功能或方式并及时删除。
2. App违反法律法规规定，或违反与用户的约定向第三方共享、转让个人信息，或用户要求删除个人信息时，App提供者应立即停止共享、转让的行为，并通知第三方及时删除。
3. App提供者违反法律法规规定，或违反与用户的约定，公开披露个人信息，且用户要求删除时，App提供者应立即停止公开披露的行为，并发布通知要求相关接收方删除相应信息。

## 个人信息的注销

### 提供便捷的注销方法

通过注册账户提供产品或服务的App 提供者应满足以下要求：

1. 应向用户提供注销账户的方法，注销操作按钮方便找到，不宜超过 5 次点击。
2. 注销前应告知用户注销方式、注销时限、注销内容等信息，不应设置不合理的注销条件，注销方法应简便易操作，最终注销前需取得用户的二次确认。
3. 当用户提交注销后，App 提供者应在承诺期限内完成注销，不宜超过10个工作日，最长不应超过15个工作日。

注1：多个产品或服务之间存在必要业务关联关系的，例如，一旦注销某个产品或服务的账户，将会导致其他产品或服务的必要业务功能无法实现或者服务质量明显下降的，需向个人信息主体进行详细说明。

注2：产品或服务没有独立的账户体系的，可采取对该产品或服务账号以外其他个人信息进行删除，并切断账户体系与产品或服务的关联等措施实现注销。

### 注销核验过程中的个人敏感信息删除

注销账户的过程需收集个人敏感信息核验身份时，应明确对收集个人敏感信息后的处理措施，如达成目的后立即删除或匿名化处理等。

### 注销账户后的个人信息删除

用户注销账户后，应及时删除其个人信息或匿名化处理。因法律法规规定需要留存个人信息的，应按照对应法律法规要求进行处理，应满足用户信息处理最小必要原则，不应再次将上述个人信息用于日常业务活动中。

注：例如对于电子商务类App，其用户注销账户后，按照《中华人民共和国电子商务法》要求，用户的订单信息需要保留至少三年，因此用户的其他个人信息应及时做删除或匿名化处理，但是订单信息和交易记录需要保存，但上述信息应和用户账号解绑且不能用于日常的业务活动中。

## 用户个人信息保存期限已届满

App提供者保存个人信息的期限应为实现用户授权使用的目的所必需的最短时间，法律法规另有规定或用户另行同意的除外。

超出个人信息保存期限后，App提供者应对个人信息进行删除或匿名化处理。

## 其他要求

在以下情形，个人信息个人信息处理者应主动删除个人信息，个人信息处理者未删除的，个人有权请求删除：

1. 处理目的已实现、无法实现或者为实现处理目的不再必要。
2. 个人信息处理者停止提供产品或者服务，或者保存期限已届满。
3. 个人撤回同意。
4. 个人信息处理者违反法律、行政法规或者违反约定处理个人信息。
5. 法律、行政法规规定的其他情形。

# 附录A

# （资料性）

# 个人信息及个人敏感信息

个人信息是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，包括不限于个人基本资料、个人身份信息、个人生物识别信息、网络身份标识信息、个人健康生理信息、个人教育工作信息、个人财产信息、个人通信信息、联系人信息、个人上网记录、个人常用射别信息、个人位置信息等。个人信息不包括匿名化处理后的信息。

个人敏感信息是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及未满十四周岁未成年人的个人信息。

表 A.1 给出了常见的个人信息和敏感信息举例。

表 A.1 常见个人信息与个人敏感信息举例

|  |  |
| --- | --- |
| **个人信息分类** | **个人信息举例（加粗为个人敏感信息）** |
| 个人基本资料 | 个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等 |
| 个人身份信息 | **身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等** |
| 个人生物识别信息 | **个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等** |
| 网络身份标识信息 | 个人信息主体账号、IP地址、个人数字证书等 |
| 个人健康生理信息 | **个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等**，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等 |
| 个人教育工作信息 | 个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等 |
| 个人财产信息 | **银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息** |
| 个人通信信息 | **通信记录和内容**、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等 |
| 联系人信息 | **通讯录、好友列表、群组列表、**电子邮件地址列表等 |
| 个人上网记录 | 指通过日志储存的个人信息主体操作记录，包括**网站浏览记录**、软件使用记录、点击记录、收藏列表等 |
| 个人常用设备信息 | 指包括硬件序列号、设备MAC地址、软件列表、唯一设备识别码（如IMEI/IMSI/MEID/Android ID/IDFA/Open UDID/GUID/MEID/ICCID等）、设备传感器信息等在内的描述个人常用设备基本情况的信息 |
| 个人位置信息 | 包括**行踪轨迹、精准定位信息、住宿信息、经纬度**等 |
| 其他信息 | **未满十四周岁未成年人的个人信息、婚史、宗教信仰、性取向、**未公开的违法犯罪记录等 |

# 附录B

# （资料性）

# 去标识化与匿名化

**B.1** **去标识化与匿名化的对比**

去标识化和匿名化都是对个人信息进行处理，使得处理后的信息无法单独识别个人信息主体。它们主要的区别在于，去标识化的信息仍属于个人信息，具有一定识别性，可以结合其他信息识别个人信息主体，可以复原为个人信息或重标识，而匿名化处理的信息不属于个人信息，识别结合其他信息无法识别个人信息主体，也无法复原为个人信息或重标识。

表 B.1 给出了去标识化和匿名化的对比。

表 B.1 去标识化与匿名化的对比

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 仅从该信息本身无法识别特定自然人 | 结合其他信息也无法识别特定自然人 | 处理后的信息无法复原为个人信息 | 处理后的信息无法重标识 |
| 去标识化 | √ | × | × | × |
| 匿名化 | √ | √ | √ | √ |

**B.2** **常见直接标识符和准标识符**

去标识化主要是去除标识符与个人信息主体之间的关联性。标识符分为直接标识符和准标识符。任何在特定环境下可唯一识别个人识别号码、特征或代码等属于直接标识符，任何在相应环境下无法单独唯一识别个人信息主体，但结合其他信息可唯一识别个人信息主体的属性属于准标识符。

表 B.2 给出了常见的直接标识符和准标识符举例。

表 B.2 常见直接标识符和准标识符举例

|  |  |
| --- | --- |
| **直接标识符** | **准标识符** |
| 个人姓名、详细住址、电子邮件地址、个人电话号码、传真号码、公民身份号码、护照号、驾驶证号、社会保障号码、健康卡号码、病例号码、生物识别码、全脸图片图像和其他任何可比对的图像、账号、证书号或许可证号、互联网协议地址（IP 地址）、银行账户、车牌号、车辆标识符和序列号、设备标识符和序列号等 | 性别、出生日期、年龄、民族、族裔血统、国籍、籍贯、语言、原住民身份、可见额少数民族地位、婚姻状况、职务、工作单位、部门、受教育水平、上学年限、总收入、地理范围（如邮政编码、建筑名称、地区）、事件日期（如入院、手术、访问等）、宗教信仰等 |

**B.3 去标识化和匿名化的技术**

匿名化是一种特殊的去标识化，当去标识化的程度达到无法复原和重标识关联到特定自然人时，就实现了匿名化。匿名化和去标识化的都用到假名、抑制、泛化、随机化等技术。常见的去标识化技术内容可参考 GB/T 37964—2019 附录A、附录 C。

表 B.3 给出了常见的去标识化技术举例。

表 B.3 常见去标识化技术举例

|  |  |
| --- | --- |
| **技术分类** | **对应方法** |
| 统计技术 | 数据抽样、数据聚合 |
| 密码技术 | 确定性加密、保序加密、保留格式加密、同态加密、同态秘密共享 |
| 抑制技术 | 屏蔽、局部抑制、记录抑制 |
| 假名化技术 | 基于密码技术的标识符派生假名创建 |
| 泛化技术 | 取整、顶层与底层编码 |
| 随机化技术 | 噪声添加、置换、微聚集 |
| 数据合成技术 | 人工方式产生微数据 |

**B.4 常见标识符的去标识化的参考**

常见的标识符可以按照产品或服务需要进行去标识化，表 B.4 给出了常见的标识符去标识化参考。

表 B.4 常见标识符去标识化举例

|  |  |  |
| --- | --- | --- |
| **标识符****类型** | **去标识化****技术** | **去标识化举例** |
| 姓名 | 泛化编码 | 使用概括、抽象的符号来表示，如使用“张先生”“张某某”代替“张三丰” |
| 抑制屏蔽 | 直接删除姓名或使用统一的“\*”表示，如所有姓名都使用“\*\*\*”代替 |
| 随机替代 | 使用随机生成的汉字来表示，如使用随机生成的“辰筹猎”取代“张三丰” |
| 假名化 | 构建常用人名字典表从中随机选择一个名字代替“张三丰” |
| 可逆编码 | 采用密码或者其他变换技术，将姓名转变成另外的字符，并保持可逆特性，如使用“ssdfsf” 代替“张三丰” |
| 身份证号 | 抑制屏蔽 | 直接删除身份证号或使用统一的“\*”表示，如所有身份证号都使用“\*\*\*\*\*\*”代替 |
| 部分屏蔽 | 屏蔽身份证号中的一部分，如使用“5\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*2”代替身份证号 |
| 可逆编码 | 采用密码或者其他变换技术，将身份证号转换成其他字符，并保持可逆特性，如使用“JS223XH”代替 |
| 数据合成 | 采用重新产生的数据替代原身份证号如使用数据集中的记录顺序号替代原身份证号，或随机产生符合身份证号编码规则的新身份证号代替原始值 |
| 银行卡号 | 抑制屏蔽 | 直接删除银行卡号或使用统一的“\*”表示，如所有银行卡号都使用“\*\*\*\*\*”代替 |
| 部分屏蔽 | 屏蔽银行卡中的一部分，如分别屏蔽银行卡中的发卡机构标识代码和自定义位 |
| 可逆编码 | 采用密码或者其他变换技术，将银行卡号转换成其他字符，并保持可逆特性 |
| 数据合成 | 采用重新产生的数据替代原银行卡号 |
| 地址 | 泛化编码 | 使用概括、抽象的符号来表示，如“云南省昆明市”使用“南方某地”来代替。 |
| 抑制屏蔽 | 直接删除地址或使用统一的“\*”来表示。如所有地址使用“\*\*\*\*\*\*”来代替 |
| 部分屏蔽 | 屏蔽地址中的一部分，如使用“云南省XX市XX县”来代替“云南省昆明市宜良县” |
| 数据合成 | 采用重新产生的数据替代原地址数据，数据产生方法可以采用确定性方法或随机方法，如使用“云南省昆明市西山区环城南路777号”代替“江西省吉安市安福县安平路1号” |
| 电话号码 | 抑制屏蔽 | 直接删除电话号码或使用统一的“\*”来表示。如所有电话使用“\*\*\*\*\*\*”来代替 |
| 部分屏蔽 | 屏蔽电话号码中的一部分，如使用“153\*\*\*\*2212”或“15\*\*\*\*\*\*\*12”来代替 |
| 随机替代 | 使用随机生成的一串数字来表示，如使用随机生成的“23434232”取代“15322112212” |
| 可逆编码 | 采用密码或者其他变换技术，将电话号码转换成其他字符，并保持可逆特性，如使用“15458982684”代替“15322112212” |
| 数值型标识符 | 泛化编码 | 使用概括、抽象的符号来表示，如“有四个人，他们分别是蓝色、绿色和浅褐色的眼睛”来代替“有1个人是蓝色眼睛，2个人是绿色眼睛，1个人是浅褐色眼睛” |
| 抑制屏蔽 | 直接删除数值或使用统一的“\*”来表示。如所有数值使用“\*\*\*\*\*”来代替 |
| 顶层和底层编码 | 大于或小于一个特定值的处理成某个固定值。例如，年龄超过70岁的一律用“大于70岁”描述，以保障次范围内的人数多于20000人 |
| 部分屏蔽 | 屏蔽数值的高位部分代替原有数值，如百分制考试成绩全部用去掉个位数、保留十位数的数值代替 |
| 记录交换 | 使用数据集中其他记录的相应数值代替本记录的数值，如设定规则，将记录集中的所有的身高数据取出并全部打乱位置后(其他属性数据位置不变)放回原数据集中，这种方法可以保持数据集的统计特性不变 |
| 噪声添加 | 相对原始数据，产生微小的随机数，将其加到原始数值上并代替原始数值。如对于身高1.72m，产生随机数值—0.11m，加到原始数值后将其变为1.61m |
| 数据合成 | 采用重新产生的数据替代原始数据，数据产生方法可以采用确定性方法或随机性方法。如使用“19”岁年龄代替“45”岁年龄 |
| 日期 | 泛化编码 | 使用概括、抽象的日期来表示，如使用1880年代替1880年1月1日 |
| 抑制屏蔽 | 直接删除日期数据或使用统一的“\*”来表示。如所有的数值都使用“\*年\*日”代替 |
| 部分屏蔽 | 对日期中的一部分做屏蔽，如1880年某月1日代替1880年1月1日 |
| 记录交换 | 使用数据集中其他记录的相应数值代替本记录的数值。如设定规则，将记录集中的所有的日期数据取出并全部打乱位置后(其他属性数据位置不变)放回到原数据集中。这种方法有利于保持数据集的统计特性 |
| 噪声添加 | 相对原始数据，产生微小的随机数，将其加到原始数值上并代替原始数值。如对于出生日期1880年1月1日，产生随数值 32天，加到原始数值后将其变为1880年2月2日 |
| 数据合成 | 采用重新产生的数据替代原日期数据，如使用“1972年8月12日“代替“1880 年1月1日” |
| 地理位置 | 泛化编码 | 使用概括、抽象的位置来表示，如将“春城路1号”泛化为“昆明市”，以保障次范围内的人数多于20000人 |
| 噪声添加 | 相对原始数据，产生微小的随机数，将其加到原始数值上并代替原始数值。如对中心区范围内通过加减100m 的范围，而偏远地区通过加减5km来得到充足的模糊化效果 |

# 附录C

# （资料性）

# 个人信息的监管与法律责任

**C.1** **个人信息保护立法概况**

近年来我国个人信息保护力度不断加大，相关法律法规不断健全，目前已初步形成了多层次、多领域的个人信息保护法律体系。2012年全国人民代表大会常务委员会发布《关于加强网络信息保护的决定》，首次明确了“国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息”，并初步确立了“合法、正当、必要”原则，并一直在后续立法中得到延续。2013年，工业和信息化部出台《电信和互联网用户个人信息保护规定》（工信部24号令），对“用户个人信息”做出界定，并全面规定了信息收集和使用规范、安全保障措施、监督检查等内容。2016年《中华人民共和国网络安全法》正式发布，其中在“网络信息安全”和“网络运行安全”章节对个人信息保护作出了较为全面的规定，这是我国首次将个人信息保护提高到法律的层面，并为后续的相关立法执法工作提供了强有力的依据。2021年《中华人民共和国个人信息保护法》发布后，我国已逐步形成由法律、法规、规章及规范性文件等共同组成的结构相对完善的个人信息保护法律体系，相应的国家标准、行业标准陆续出台，以及相关领域的行业标准、团体标准、指南、规范等也为个人信息保护实践提供了具有重要的指导和参考。

**C.2** App**个人信息保护主要监管部门**

当前在App个人信息保护领域主要由国家网信部门、电信主管部门、公安部门和市场监督管理部门分别在各自职责范围，从不同侧重点进行App个人信息保护和监督管理工作。网信部门统筹协调,电信主管部门从互联网行业管理、App接入备案、公共互联网网络与数据安全、电信和互联网行业个人信息保护、反电信网络诈骗等方面履行监管职责。公安部门从网络安全保护、等级保护、互联网公共秩序和公共安全、防范惩治网络违法犯罪等方面保护App个人信息。市场监督管理部门主要从网络市场行政执法、网络商品交易及有关服务监督、网络交易平台和网络经营主体规范管理等方面着手。同时，金融、医疗等各行业由其行业主管部门根据行业特点进行有针对性的监管。

**C.3** **个人信息保护法律责任**

《中华人民共和国个人信息保护法》第七章，从行政责任、民事责任、刑事责任等多角度全方位地规定了违法违规的相关法律责任，并确定了较高的行政罚款标准，强调了法律对个人信息保护的力度，App个人信息保护的法律责任也涵盖其中。

主要的违法行为及对应法律责任整理如下：

表 C.3 给出了《中华人民共和国个人信息保护法》主要的违法行为及对应法律责任举例。

表 C.3 《中华人民共和国个人信息保护法》主要违法行为及对应法律责任

|  |  |  |
| --- | --- | --- |
| **法律责任** | **违法行为** | **违法后果** |
| 行政责任 | 违反个人信息保护法规定处理个人信息，或者处理个人信息未履行法定义务的 | •由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；•拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；•情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。 |
| 有本法规定的违法行为的 | •依照有关法律、行政法规的规定记入信用档案，并予以公示。 |
| 有个人信息保护法规定的违法行为的 | •记入信用档案，并予以公示  |
| 国家机关不履行个人信息保护法规定的个人信息保护义务的 | •责令改正•对责任人员依法给予处分  |
| 履行个人信息保护职责的部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的 | •依法给予处分 |
| 构成违反治安管理行为  | •依法给予治安管理处罚 |
| 民事责任 | 处理个人信息侵害个人信息权益造成损害 | •个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任•损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定•难以确定的，根据实际情况确定赔偿数  |
| 违反本法规定处理个人信息，侵害众多个人的权益 | •人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼  |
| 刑事责任 | 违反本法规定，构成犯罪的 | •依法追究刑事责任 |

**C.4** **数据安全保护法律责任**

App个人信息的保护也涉及数据安全的范畴，《中华人民共和国数据安全法》第六章从法律责任的角度对违法违规的行为进行了约束，让数据安全的保护力度得到加强。

主要的违法行为及对应法律责任整理如下：

表 C.4 给出了《中华人民共和国数据安全法》主要的违法行为及对应法律责任举例。

表 C.4 《中华人民共和国数据安全法》主要违法行为及对应法律责任

|  |  |  |
| --- | --- | --- |
| **法律责任** | **违法行为** | **违法后果** |
| 行政责任 | 开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的 | •责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；•拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。 |
| 违反国家核心数据管理制度，危害国家主权、安全和发展利益的 | •由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。 |
| 违反本法第三十一条规定，向境外提供重要数据的 | •由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；•情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。 |
| 从事数据交易中介服务的机构未履行本法第三十三条规定的义务的 | •由有关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足十万元的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 |
| 违反本法第三十五条规定，拒不配合数据调取的 | •由有关主管部门责令改正，给予警告，并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 |
| 违反本法第三十六条规定，未经主管机关批准向外国司法或者执法机构提供数据的 | •由有关主管部门给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；造成严重后果的，处一百万元以上五百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上五十万元以下罚款。 |
| 违反本法规定，构成违反治安管理行为的 | •依法给予治安管理处罚。 |
| 国家机关不履行本法规定的数据安全保护义务的  | •对直接负责的主管人员和其他直接责任人员依法给予处分。 |
| 履行数据安全监管职责的国家工作人员玩忽职守、滥用职权、徇私舞弊的 | •依法给予处分。 |
| 民事责任 | 违反本法规定，给他人造成损害的 | •依法承担民事责任。 |
| 刑事责任 | 违反本法规定，构成犯罪的 | •依法追究刑事责任。 |

**C.5** **网络安全保护法律责任**

同时，App的个人信息保护也遵从《中华人民共和国网络安全法》，其中第六章对网络安全违法行为和责任进行了规范，从网络安全层面保障公民的的个人信息和相关权益。

主要的违法行为及对应法律责任整理如下：

表 C.5 给出了《中华人民共和国网络安全法》主要的违法行为及对应法律责任举例。

表 C.5 《中华人民共和国网络安全法》主要违法行为及对应法律责任

|  |  |  |
| --- | --- | --- |
| **法律责任** | **违法行为** | **违法后果** |
| 行政责任 | 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的 | •由有关主管部门责令改正，给予警告；•拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。 |
| 关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的 | •由有关主管部门责令改正，给予警告；•拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。 |
| 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的：（一）设置恶意程序的；（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；（三）擅自终止为其产品、服务提供安全维护的。 | •由有关主管部门责令改正，给予警告；•拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款： |
| 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的 | •由有关主管部门责令改正；•拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 |
| 违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的 | •由有关主管部门责令改正，给予警告；•拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。 |
| 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的 | •由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；•情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款；•单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚；•违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；•违反本法第二十七条规定，受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。 |
| 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的 | •由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；•情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。 |
| 违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的 | •由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。 |
| 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的 | •由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 |
| 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的 | •由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 |
| 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的 | •由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；•情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组；•单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。 |
| 网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的 | •由有关主管部门责令改正，给予警告，没收违法所得；•拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 |
| 电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的 | •由有关主管部门责令改正，给予警告，没收违法所得；•拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 |
| 网络运营者违反本法规定，有下列行为之一的：（一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；（二）拒绝、阻碍有关部门依法实施的监督检查的；（三）拒不向公安机关、国家安全机关提供技术支持和协助的。 | •由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款 |
| 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的 | •依照有关法律、行政法规的规定处罚。 |
| 有本法规定的违法行为的 | •依照有关法律、行政法规的规定记入信用档案，并予以公示。 |
| 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的 | •由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。 |
| 网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的 | •对直接负责的主管人员和其他直接责任人员依法给予处分。 |
| 网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的 | •依法给予处分。 |
| 违反本法规定，构成违反治安管理行为的 | •依法给予治安管理处罚 |
| 民事责任 | 违反本法规定，给他人造成损害的 | •依法承担民事责任。 |
| 刑事责任 | 违反本法规定，构成犯罪的 | •依法追究刑事责任。 |
| 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的 | •依法追究法律责任•国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。 |

**C.6** **反电信网络诈骗法律责任**

《中华人民共和国反电信网络诈骗法》第六章，从反电信网络诈骗规定了违法违规的相关法律责任，为个人信息保护加码。特别需要关注的是，《中华人民共和国反电信网络诈骗法》第二十三条明确规定“设立移动互联网应用程序应当按照国家有关规定向电信主管部门办理许可或者备案手续”，按照《工业和信息化部关于开展移动互联网应用程序备案工作的通知》（工信部信管〔2023〕105号）要求，对未履行备案程序、从事违法违规活动的App，各省、自治区、直辖市通信管理局将按照相关法律法规规定处理。

《中华人民共和国反电信网络诈骗法》主要的违法行为及对应法律责任整理如下：

表 C.6 给出了《中华人民共和国反电信网络诈骗法》主要的违法行为及对应法律责任举例。

表 C.6 《中华人民共和国反电信网络诈骗法》主要违法行为及对应法律责任

|  |  |  |
| --- | --- | --- |
| **法律责任** | **违法行为** | **违法后果** |
| 行政责任 | 组织、策划、实施、参与电信网络诈骗活动或者为电信网络诈骗活动提供帮助，尚不构成犯罪的 | •由公安机关处十日以上十五日以下拘留；没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足一万元的，处十万元以下罚款。 |
| 电信业务经营者违反本法规定，有下列情形之一的：（一）未落实国家有关规定确定的反电信网络诈骗内部控制机制的；（二）未履行电话卡、物联网卡实名制登记职责的；（三）未履行对电话卡、物联网卡的监测识别、监测预警和相关处置职责的；（四）未对物联网卡用户进行风险评估，或者未限定物联网卡的开通功能、使用场景和适用设备的；（五）未采取措施对改号电话、虚假主叫或者具有相应功能的非法设备进行监测处置的。 | •由有关主管部门责令改正，情节较轻的，给予警告、通报批评，或者处五万元以上五十万元以下罚款；•情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款 |
| 银行业金融机构、非银行支付机构违反本法规定，有下列情形之一的：（一）未落实国家有关规定确定的反电信网络诈骗内部控制机制的；（二）未履行尽职调查义务和有关风险管理措施的；（三）未履行对异常账户、可疑交易的风险监测和相关处置义务的；（四）未按照规定完整、准确传输有关交易信息的。 | •由有关主管部门责令改正，情节较轻的，给予警告、通报批评，或者处五万元以上五十万元以下罚款；•情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令停止新增业务、缩减业务类型或者业务范围、暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款。 |
| 电信业务经营者、互联网服务提供者违反本法规定，有下列情形之一的：（一）未落实国家有关规定确定的反电信网络诈骗内部控制机制的；（二）未履行网络服务实名制职责，或者未对涉案、涉诈电话卡关联注册互联网账号进行核验的；（三）未按照国家有关规定，核验域名注册、解析信息和互联网协议地址的真实性、准确性，规范域名跳转，或者记录并留存所提供相应服务的日志信息的；（四）未登记核验移动互联网应用程序开发运营者的真实身份信息或者未核验应用程序的功能、用途，为其提供应用程序封装、分发服务的；（五）未履行对涉诈互联网账号和应用程序，以及其他电信网络诈骗信息、活动的监测识别和处置义务的；（六）拒不依法为查处电信网络诈骗犯罪提供技术支持和协助，或者未按规定移送有关违法犯罪线索、风险信息的。 | •由有关主管部门责令改正，情节较轻的，给予警告、通报批评，或者处五万元以上五十万元以下罚款；•情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款 |
| 违反本法第十四条、第二十五条第一款规定的 | •没收违法所得，由公安机关或者有关主管部门处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足五万元的，处五十万元以下罚款；情节严重的，由公安机关并处十五日以下拘留。 |
| 违反本法第二十五条第二款规定 | •由有关主管部门责令改正，情节较轻的，给予警告、通报批评，或者处五万元以上五十万元以下罚款；•情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站或者应用程序，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款。 |
| 违反本法第三十一条第一款规定的 | •没收违法所得，由公安机关处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足二万元的，处二十万元以下罚款；情节严重的，并处十五日以下拘留。 |
| 民事责任 | 组织、策划、实施、参与电信网络诈骗活动或者为电信网络诈骗活动提供相关帮助的违法犯罪人员，除依法承担刑事责任、行政责任以外，造成他人损害的 | •依照《中华人民共和国民法典》等法律的规定承担民事责任。 |
| 电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者等违反本法规定，造成他人损害的 | •依照《中华人民共和国民法典》等法律的规定承担民事责任。 |
| 刑事责任 | 组织、策划、实施、参与电信网络诈骗活动或者为电信网络诈骗活动提供帮助，构成犯罪的 | •依法追究刑事责任。 |
| 反电信网络诈骗工作有关部门、单位的工作人员滥用职权、玩忽职守、徇私舞弊，或者有其他违反本法规定行为，构成犯罪的 | •依法追究刑事责任。 |

# 附录D

# （资料性）

# 个人信息保护相关法律、司法解释、部门规章和标准文件索引

**D.1** **个人信息保护相关法律（部分）**

《中华人民共和国民法典》

《中国人民共和国刑法》

《中华人民共和国个人信息保护法》

《中华人民共和国网络安全法》

《中华人民共和国数据安全法》

《中华人民共和国未成年人保护法》

《中华人民共和国电子商务法》

《中华人民共和国消费者权益保护法》

《中华人民共和国反电信网络诈骗法》

**D.2** **个人信息保护相关司法解释（部分）**

《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》

《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》

《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》

《检察机关办理侵犯公民个人信息案件指引》

《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》

《最高人民法院关于规范和加强人工智能司法应用的意见》

《最高人民法院关于为促进消费提供司法服务和保障的意见》

**D.3** **个人信息保护相关行政法规（部分）**

《未成年人网络保护条例》

《关键信息基础设施安全保护条例》

《互联网信息服务管理办法》

《信息网络传播权保护条例》

《中华人民共和国电信条例》

《征信业管理条例》

**D.4** **个人信息保护相关部门规章及示范性文件（部分）**

《电信和互联网用户个人信息保护规定》

《儿童个人信息网络保护规定》

《规范互联网信息服务市场秩序若干规定》

《互联网视听节目服务管理规定》

《互联网新闻信息服务管理规定》

《互联网信息服务算法推荐管理规定》

《网络安全审查办法》

《网络信息内容生态治理规定》

《汽车数据安全管理若干规定（试行）》

《常见类型移动互联网应用程序必要个人信息范围规定》

《App违法违规收集使用个人信息行为认定方法》

《App违法违规收集使用个人信息自评估指南》

《移动互联网应用程序信息服务管理规定》

**D.5** **个人信息保护相关国家标准（部分）**

信息安全技术 个人信息安全规范GB/T 35273—2020

信息安全技术 个人信息去标识化指南GB/T 37964—2019

信息安全技术 个人信息安全影响评估指南GB/T 39335—2020

信息安全技术 移动智能终端个人信息保护技术要求GB/T 34978—2017

信息安全技术 网络安全等级保护基本要求GB/T 22239—2019A

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GB/T 41391—2022

信息安全技术 信息安全风险评估方法GB/T 20984—2022

信息安全技术 网络数据处理安全要求GB/T 41479—2022

信息安全技术 移动互联网安全审计指南GB/Z 41290—2022

智能家用电器 个人信息保护要求和测评方法GB/T 40979—2021

**D.6** **个人信息保护相关行业标准（部分）**

网络安全标准实践指南—移动互联网应用程序（App）个人信息保护常见问题及处置指南 TC260-PG-20203A

网络安全标准实践指南—移动互联网应用程序 (App)收集使用个人信息自评估指南 TC260-PG-20202A

网络安全实践指南—移动互联网应用基本业务功能必要信息规范 TC260-PG-20191A

网络安全标准实践指南—移动互联网应用程序（App）系统权限申请使用指南 TC260-PG-20204A

网络安全标准实践指南—移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引 TC260-PG-20205A

网络安全标准实践指南—网络数据分类分级指引 TC260-PG-20212A

金融业数据能力建设指引 JR/T 0218-2021

金融数据安全 数据安全分级指南 JR/T 0197-2020

个人金融信息保护技术规范 JR/T 0171-2020

**D.7** **个人信息保护相关团体标准（部分）**

App收集使用个人信息最小必要评估规范 总则 TTAF 077.1-2020

App收集使用个人信息最小必要评估规范 位置信息 TTAF 077.2-2020

App收集使用个人信息最小必要评估规范 第3部分：图片信息 TTAF 077.3-2022

App收集使用个人信息最小必要评估规范 终端通讯录 TTAF 077.4-2020

App收集使用个人信息最小必要评估规范 设备信息 TTAF 077.5-2020

App收集使用个人信息最小必要评估规范 软件列表 TTAF 077.6-2020

App收集使用个人信息最小必要评估规范 人脸信息 TTAF 077.7-2020

App收集使用个人信息最小必要评估规范 录像信息 TTAF 077.8-2020

App收集使用个人信息最小必要评估规范 第9部分：短信信息 TTAF 077.9-2022

App收集使用个人信息最小必要评估规范 录音信息 TTAF 077.10-2021

App收集使用个人信息最小必要评估规范 通话记录 TTAF 077.11-2021

App收集使用个人信息最小必要评估规范 好友列表 TTAF 077.12-2021

App收集使用个人信息最小必要评估规范 传感器信息 TTAF 077.13-2021

App收集使用个人信息最小必要评估规范 应用日志信息 TTAF 077.14-2021

App收集使用个人信息最小必要评估规范 房产信息 TTAF 077.15-2021

App收集使用个人信息最小必要评估规范 交易记录 TTAF 077.16-2021

App收集使用个人信息最小必要评估规范 身份信息 TTAF 077.17-2021

App用户权益保护测评规范 超范围收集个人信息 TTAF 078.1-2020

App用户权益保护测评规范 定向推送 TTAF 078.2-2020

App用户权益保护测评规范 个人信息获取行为 TTAF 078.3-2020

App用户权益保护测评规范 权限索取行为 TTAF 078.4-2021

App用户权益保护测评规范 违规使用个人信息 TTAF 078.5-2020

App用户权益保护测评规范 违规收集个人信息 TTAF 078.6-2020

App用户权益保护测评规范 欺骗误导强迫行为 TTAF 078.7-2021

App用户权益保护测评规范 移动应用分发平台管理 TTAF 078.8-2020

App用户权益保护测评规范 移动应用分发平台信息展示 TTAF 078.9-2021

App用户权益保护测评规范 自启动和关联启动行为 TTAF 078.10-2020

附录E

（资料性）

个人信息管理机制

**E.1** **组织保障**

**E.1.1** **组织架构**

App提供者应在中华人民共和国境内设立个人信息安全部门，该部门可由各业务侧负责人及相关专业人员组成，负责组织建立用户个人信息收集、使用及其相关活动的工作流程和安全管理制度，监督检查用户个人信息安全各项要求落实情况，并负责用户个人信息保护工作的日常管理。中小企业的App提供者应当明确指定一名个人信息安全负责人，该负责人负责统筹指导个人信息保护总体工作。此负责人可以是公司高层管理人员或者专门负责信息安全的员工。并应当建立相应的安全管理制度和工作流程，以确保用户个人信息的收集、使用及相关活动符合法律法规，并且应当监督检查用户个人信息安全各项要求的落实情况。

App 提供者应明确个人信息安全负责人，该角色负责统筹指导个人信息保护总体工作，指导重大用户个人信息保护事件的处理。同时App 提供者应公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

 **E.1.2** **角色职责**

个人信息安全责任组织/个人在进行用户个人信息保护工作时，建议分为统筹管理、安全合规两类角色：

1. 统筹管理的角色职责应包括但不限于:
	1. 全面统筹实施组织内部的个人信息安全工作；
	2. 组织制定用户个人信息保护管理办法、相关管理制度并督促落实;
	3. 制定、签发、实施、更新个人信息保护政策、用户协议和相关规程；
	4. 建立、维护、更新个人信息收集清单、第三方信息共享清单；
	5. 定期开展个人信息安全影响评估，提出对策建立，督促整改安全隐患;
	6. 定期进行安全审计；
	7. 与监督、管理部门保持沟通，及时报告个人信息保护和事件处置情况。
2. 安全合规的角色职责应包括但不限于：
	1. 落地执行内部制定的关于用户个人信息保护的相关规章制度的相关要求；
	2. 制定个人信息安全事件应急预案，并定期组织安全和应急演练；
	3. 强化个人数据安全能力，落实必要的管理和技术措施，防止个人信息的泄露、损毁、丢失和篡改；
	4. 在产品或服务上线发布前进行检测，提前消除个人信息安全隐患；
	5. 加强业务部门对用户个人信息的第三方合作伙伴的管控；
	6. 公布投诉、举报方式等信息并及时受理投诉举报；
	7. 组织开展用户个人信息保护意识教育及技能培训。

**E.2** **工作机制**

 **E.2.1 合规管理机制**

组织应建立内部管理机制：

* 1. 应明确用户服务和权益保护的牵头管理部门/专员和负责人，建立全生命周期个人信息保护机制，健全考核问责制度，将相关法规政策要求落实到产品研发、推广和运营各环节。
	2. 合规管理应由个人信息安全部门/专员发起，个人信息安全负责人牵头，组织协调各部门开展个人信息保护相关工作。
	3. 应建立定期开展自评估机制，进行动态评估，以确保个人信息安全工作的有效性和合规性。
	4. 当服务内容发生重大变化时，企业应当进行全面合规检查，特别关注个人信息保护方面的合规性。这包括但不限于服务范围扩大、数据处理方式变更、合作伙伴变更等情况。通过全面合规检查，企业可以及时调整个人信息保护措施，确保新的服务内容与法律法规的要求保持一致。

**E.2.2 合规评估机制**

 在满足 GB/T 35273—2020中第11.4条要求的基础上，还建议遵守以下要求：

1. 宜建立个人信息安全影响评估制度，评估并处置个人信息处理活动存在的安全风险。
2. 组织在以下情形应事前进行个人信息保护影响评估，并对处理情况进行记录：
	1. 处理敏感个人信息；
	2. 利用个人信息进行自动化决策；
	3. 委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；
	4. 向境外提供个人信息；
	5. 法律法规有新的要求；
	6. 产品服务有重大变更；
	7. 新产品、服务、业务功能计划实施；
	8. 发生重大个人信息安全事件；
	9. 其他对个人权益有重大影响的个人信息处理活动。
3. 个人信息保护影响评估应包括下列内容:
	1. 个人信息的处理目的、处理方式等是否合法、正当、必要；
	2. 对个人权益的影响及安全风险；
	3. 所采取的保护措施是否合法、有效并与风险程度相适应。
4. 个人信息保护影响评估报告和处理情况记录应当至少保存三年。

**E.2.3 安全保障机制**

 组织宜采取以下措施防止用户个人信息泄露、毁损、篡改或者丢失：

1. 确定各部门、岗位和分支机构的用户个人信息安全管理责任。
2. 建议建立用户个人信息收集、使用及其相关活动的工作流程和安全管理制度。
3. 建议对工作人员及代理人实行权限管理，对批量导出、复制、销毁信息实行审查，并采取防泄密措施。
4. 妥善保管记录用户个人信息的纸介质、光介质、电磁介质等载体，并采取相应的安全储存措施。
5. 建议对储存用户个人信息的信息系统实行接入审查，并采取防入侵、防病毒等措施。
6. 建议记录对用户个人信息进行操作的人员、时间、地点、事项等信息。
7. 建议按照电信管理机构的规定开展通信网络安全防护工作。
8. 建立常态保障和应急保障机制：
	1. 常态保障应建立数据分类分级制度，利用数据加密、数据脱敏、匿名化等安全技术保障用户个人信息安全。加强前端和后端安全防护。主动监测发现个人信息泄露、窃取、篡改、毁损、丢失、非法使用等风险威胁，及时响应处置要求。
	2. 应急保障应建立及时有效的应急响应机制，以应对组织个人信息安全事件的处理。
9. 安全保障应覆盖用户个人信息全生命周期，完善内部岗位权限分工，从数据的生成、传输、存储、使用、共享、备份、销毁的全生命周期来保障数据安全。
10. 应当对用户个人信息保护情况每年至少进行一次自查，记录自查情况，及时消除自查中发现的安全隐患。
11. 组织保管的用户个人信息发生或者可能发生泄露、毁损、丢失的，应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人，通知应包括下列事项：
	1. 发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；
	2. 个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；
	3. 个人信息处理者的联系方式。

**E.2.4 安全保障机制**

组织应遵守以下要求：

建立内部审计机制：

1. 在需求阶段，对需求的合规性以及需求所涉及的数据进行审计，规避用户信息风险。
2. 在设计阶段，对需求设计中涉及的用户个人信息收集、处理进行审计，保障设计的合规性。
3. 在开发阶段，对需求开发所涉及的插件、开源库、API、SDK的合规性进行内审，避免第三方违规收集。
4. 开发完成后，对产品或服务整体进行合规性审核，无合规问题后方可进行发布上线。
5. 产品或服务上线运营后，定期对其进行合规性审计，对运行中出现的合规问题进行优化解决。
6. 产品或服务下线停服后，对个人信息进行删除和匿名化处理，并对处理的情况进行审核。

**E.2.5 安全保障机制**

组织应建立外部审计机制：

1. 定期与监管机构汇报合规性工作，听取相关意见进行优化。
2. 定期邀请第三方技术检测机构进行合规性检测，及时发现问题并解决。

**E.2.6 安全保障机制**

 组织应安全培训机制：

1. 应当对其工作人员进行用户个人信息保护相关知识、技能和安全责任培训。
2. 定期邀请业内专业人士解读最新政策并给予指导；
3. 定期组织个人信息安全事件演练。

# 参考文献

[1] GB/T 25069—2022 信息安全技术 术语

[2] GB/T 42460—2023 信息安全技术 个人信息去标识化效果评估指南

[3] 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

[4] GB/T 35273—2020 信息安全技术 个人信息安全规范

[5] GB/T 37964—2019 信息安全技术 个人信息去标识化指南

[6] 中华人民共和国个人信息保护法（2021年8月20日，十三届全国人大常委会第三十次会议表决通过）

[7] App违法违规收集使用个人信息行为认定方法（2019年12月30日国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局发布）

[8] 工业和信息化部关于开展纵深推进 App侵害用户权益专项整治行动的通知(工信部信管函

〔2020〕164号）