ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 44588—2024

数据安全技术　互联网平台及产品服务个人信息处理规则

Data security technology—Personal information processing rules of internet platforms, products and services

2024-09-29 发布　　2025-04-01 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 …… 2
5　概述 …… 2
6　个人信息处理规则的基本要求 …… 3
7　个人信息处理规则的编制程序 …… 3
8　个人信息处理规则的内容 …… 3
9　个人信息处理规则的发布 …… 6
10　个人信息处理规则的修订 …… 7
11　个人信息处理规则的争议纠纷解决 …… 7
参考文献 …… 8

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。

本文件由全国网络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：北京理工大学、国家计算机网络应急技术处理协调中心、中国电子技术标准化研究院、中国信息通信研究院、中国网络空间研究院、完美世界(北京)软件科技发展有限公司、上海携程商务有限责任公司、北京抖音信息服务有限公司、贝壳找房(北京)科技有限公司、北京微播视界科技有限公司、长城汽车股份有限公司、北京百度网讯科技有限公司、北京三快科技有限公司、OPPO广东移动通信有限公司、维沃移动通信有限公司、北京腾云天下科技有限公司、掌阅科技股份有限公司、上海商汤智能科技有限公司、北京尚隐科技有限公司、北京转转精神科技有限责任公司、北京市竞天公诚律师事务所上海分所、奇安信科技集团股份有限公司、华为技术有限公司、荣耀终端有限公司、北京三星通信技术研究有限公司、北京小桔科技有限公司、中国电信股份有限公司江西分公司、北京同元法律咨询有限公司、中国石油天然气股份有限公司长庆油田分公司、广州视源电子科技股份有限公司、杭州小影创新科技股份有限公司。

本文件主要起草人：洪延青、任彦、朱雪峰、薛颖、薛晨、吴梦漪、葛梦莹、何延哲、杨钦、葛鑫、胡影、田申、窦禹、陈湉、何云云、李妍洁、高超、刘笑岑、李昳婧、林星辰、张朝、吴迪、薛晶、徐全全、李杭敏、余方、袁立志、杨丹、王一宇、易立、王敬周、李阳春、宋子奕、王海棠、黄蓉、刘榕、程艳、高斯平、田林川、毛欣怡、付艳艳、赵鹏阳、衣强、赵晓娜、孙淑娴、陈舒、成瑾、陆萌、吴庚、王兴、宋小艾、李世红、周杨、朱垒、王丹辉、解伯延、张成、马可、张博文、杨昕雨、贾科、张玮、安锦程、连禧宇、吴越、张娜、田明仁、郭立、苏莹、宋养齐、焦琼辉、廖汉兴。

数据安全技术　互联网平台及产品服务个人信息处理规则

1　范围

本文件规定了互联网平台及产品服务个人信息处理规则的基本要求、编制程序、规则内容、发布形式，以及个人信息处理规则争议纠纷解决等方面的要求。

本文件适用于规范互联网平台及产品服务的运营者制定、发布个人信息处理规则的过程，也适用于对个人信息处理规则进行监督、管理和评估。

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 25069—2022　信息安全技术　术语

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 25069—2022 和 GB/T 35273—2020 界定的以及下列术语和定义适用于本文件。

3.1

互联网平台及产品服务　internet platforms, products and services

通过互联网直接向个人信息主体提供所需业务功能的平台、产品或服务。

3.2

移动互联网应用程序　mobile internet application

运行在移动智能终端上的应用程序。

注：包括智能终端预装、下载安装的应用软件，以及基于应用软件开发平台接口开发的、用户无需安装即可使用的小程序、快应用等，简称 App。

[来源：GB/T 41391—2022，3.1，有修改]

3.3

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识别的自然人有关的各种信息，不包括匿名化处理后的信息。

[来源：GB/T 35273—2020，3.1，有修改]

3.4

敏感个人信息　sensitive personal information

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。

注：敏感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，以及不满十四周岁未成年人的个人信息。

[来源：GB/T 35273—2020，3.2，有修改]

3.5

个人信息主体　personal information subject

个人信息所标识或者关联的自然人。

[来源：GB/T 35273—2020，3.3]

3.6

个人信息处理者　personal information handler

个人信息控制者

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、个人。

注：与 GB/T 35273—2020 中的“个人信息控制者”所指一致。

3.7

同意　consent

个人信息主体对其个人信息进行处理自愿、明确作出授权的行为。

注：包括通过积极的行为作出授权（即明示同意），或者通过个人信息主体的行为而推定其作出授权，如个人信息主体在被告知个人信息收集行为后仍选择进入信息采集区域。

[来源：GB/T 35273—2020，3.7，有修改]

3.8

服务类型　service type

移动互联网应用程序提供的业务功能分类。

注：常见服务类型如地图导航、网络约车、即时通信、网上购物、网络支付等。

3.9

业务功能　business function

满足个人信息主体具体使用目的的功能。

注：一种服务类型通常包括多个业务功能，如网上购物服务类型包括注册、登录、推荐、文字搜索、语音搜索、图片搜索、浏览、收藏、添加购物车、下单、支付、添加收货地址、退货、商家聊天、评论、分享商品等多个业务功能。

[来源：GB/T 35273—2020，3.17，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）

SDK：软件开发工具包（Software Development Kit）

5　概述

制定、发布个人信息处理规则是个人信息处理者遵循公开透明原则的重要体现，是保证个人信息主体知情权的重要手段，也是约束自身行为和配合监督管理的重要机制。

6 个人信息处理规则的基本要求

个人信息处理规则应清晰、准确、完整地描述个人信息处理者的个人信息处理行为和处理规则，并以便于个人信息主体阅读和理解的视角，突出向个人信息主体展现可能会对个人权益产生影响的重点内容。

7 个人信息处理规则的编制程序

个人信息处理者在编制个人信息处理规则时，应遵循以下程序。

a) 建立完善的个人信息安全管理体系，明确参与个人信息处理规则编制的责任部门或责任人、人员职责分工，并为个人信息处理规则的编制工作提供足够的资源保障。

b) 针对不同的业务功能，描述个人信息处理情况（如建立分别的个人信息处理情况描述表）。描述表内容包括：处理的个人信息种类、目的或必要性、方式（如用户填写、系统权限调用、第三方获取等）、保存方式（如本地保存、后台保存、使用云服务等）、保存期限、流转需求、所涉及系统和部门（或人员）、适配的安全措施等情况。

c) 针对个人信息处理情况描述表进行分析，明确实现特定业务功能所需收集的必要信息的范围，以及特定业务功能可能收集的非必要个人信息的范围。

d) 针对个人信息处理情况描述表进行分析，识别可能对个人信息主体权益产生重大影响的信息处理行为，包括处理敏感个人信息、利用个人信息进行自动化决策、向其他个人信息处理者提供个人信息、公开个人信息、向境外提供个人信息等。

e) 对个人信息主体权益可能产生重大影响的信息处理行为，相应地开展个人信息安全影响评估，进一步明确对处理个人信息的目的、方式、范围、个人权益保障措施，确保处理行为对个人权益的影响处于可接受的水平。

f) 建立个人信息主体权利响应机制，确保向个人信息主体提供查询、复制、更正、补充、删除个人信息，及撤回同意和注销账号的渠道，并在法律法规规定的时限内予以响应。

g) 基于a)～e)的工作内容，梳理有关信息，作为编制个人信息处理规则的基础，根据第8章内容进行编制个人信息处理规则内容。

h) 采用清晰易懂，符合通用的语言习惯编制个人信息处理规则，并使用标准化的数字、图示等，避免使用有歧义、晦涩难懂、模棱两可的语言，避免过于冗长影响用户阅读。

8 个人信息处理规则的内容

8.1 个人信息处理规则的内容构成

个人信息处理规则的内容应至少包括：个人信息处理者和个人信息处理规则适用范围、摘要、个人信息的处理规则、个人信息的安全保护规则、个人信息的跨境流动规则、个人信息主体的权利保障规则、个人信息处理规则的更新规则、个人信息处理规则的反馈、投诉和争议解决规则等。

8.2 个人信息处理者和个人信息处理规则适用范围

个人信息处理规则的主体和适用范围应包括：个人信息处理者的名称（组织）或姓名（个人）和地址、个人信息保护负责人联系方式、个人信息处理规则所适用的产品或服务范围、所适用的个人信息主体类型、生效及更新时间等。

8.3 个人信息处理规则的摘要

个人信息处理规则的摘要应使个人信息主体快速了解个人信息处理规则的主要组成部分及其核心要旨，且置于完整个人信息处理规则开始的部分，或以单独文件、单独界面展示。该部分包括但不限于以下内容：

a) 所提供的业务功能和所收集的个人信息的种类。如所收集的个人信息种类较多，可在摘要中通过个人点击链接的形式跳转至个人信息处理规则特定章节；

b) 个人选择或关闭特定业务功能的权利和操作方式；

c) 个人选择或拒绝提供非必要个人信息的权利和操作方式。

8.4 个人信息的处理规则

8.4.1 个人信息的收集使用规则

收集使用个人信息的规则应包括：

a) 明确列举涉及处理个人信息的各个业务功能；

注 1：对基本业务功能的识别参考 GB/T 41391—2022 的附录 A。

b) 分别列出各业务功能所收集的必要个人信息种类和非必要个人信息种类、目的或必要性、方式（如用户填写、系统权限调用、第三方获取等），并以“个人信息收集清单”的形式统一集中展示；

注 2：描述实现特定业务功能所必需的必要个人信息种类时，参考 GB/T 41391—2022 的附录 A。

注 3：不使用概括性语言综述所收集个人信息，如“我们收集您的身份等相关信息”此类描述，明确写明个人信息种类的表述“我们收集您的姓名、电话号码、地址信息、设备信息、网络信息、应用信息、通讯录信息”。

c) 如涉及敏感个人信息，详细说明敏感个人信息种类、目的、处理敏感个人信息的必要性和规则，并说明对个人信息主体权益的影响；

d) 在“个人信息收集清单”中列明个人信息被处理的方式，以及拒绝对个人信息的处理可能对产品或服务使用的影响；

e) 统一集中展示产品或服务中所嵌入的各个第三方代码或插件（如 SDK）的名称，并列明各个第三方代码或插件在 App 中实际所对应收集的全部个人信息种类，以及所处理个人信息的目的、方式、频次或时机等；

注 4：如嵌入的第三方代码或插件较多，直接在个人信息处理规则展示篇幅太长，可以突出链接等方式将相关内容插入到个人信息处理规则中。

f) 说明个人信息存储的地域（通常为省级行政区域）；如个人信息存在跨境传输情况，应对个人信息境外存储的地域（通过为国家或地区）单独列出或重点标识；

g) 根据个人信息的使用情况，注明不同类型个人信息预计的保存时间或个人信息存储期限的确定方法（如：自收集日期开始 5 年内）以及删除或销毁的截止日期（如：2019 年 12 月 31 日或个人信息主体注销账户时）；

h) 确需改变个人信息收集和使用的目的、方式、种类的，在以同意为个人信息处理的合法性基础的情况下，明确会重新征得个人信息主体的同意；

i) 说明是否需要对外提供（例如共享或转让）个人信息，并详细描述需要对外提供的个人信息种类和原因、个人信息的接收方身份、接收方使用个人信息的目的、个人信息对外提供过程中的安全措施，以及对外提供个人信息是否对个人信息主体带来风险，并将以上内容形成“个人信息对外提供清单”；

j) 说明是否需要公开披露个人信息，并详细描述需要公开披露的个人信息种类、原因、是否对个人信息主体带来风险；

k) 说明何种情况下个人信息处理者会不经过个人信息主体同意，对外提供和公开披露个人信

息，如响应执法机关和政府机构的要求、保护个人信息主体的生命安全和重大财产利益；

l） 收集不满十四周岁未成年人个人信息的，单独描述个人信息处理规则。

8.4.2 个人信息的安全保护规则

保障数据安全的规则包括：

a） 应说明个人信息处理者对个人信息进行安全保护的措施，包括但不限于：个人信息完整性保护措施，个人信息传输、存储和备份过程的加密措施，个人信息访问、使用的授权和审计机制，个人信息的保留和删除机制等；

b） 宜举例说明目前遵循的个人信息安全规程和取得的相关认证，例如个人信息处理者目前主动遵循的国际或国内的个人信息安全法律、法规、标准、协议等，以及个人信息处理者目前已取得的个人信息安全相关的权威独立机构认证；

c） 应描述个人信息主体提供个人信息后可能存在的安全风险；

d） 应表明在发生个人信息安全事件后，个人信息处理者将依法及时告知个人信息主体。

8.4.3 个人信息的跨境流动规则

如因业务需要或司法、执法要求，存在向境外提供个人信息的，个人信息处理规则应详细说明向境外提供的目的、提供方式、境外接收方的身份、向境外提供的个人信息种类、向境外提供时所遵守的安全保护标准，以及个人信息主体所拥有的权利、行使权利的方式或路径等。

8.5 个人信息主体的权利保障规则

保障个人信息主体权利的规则应包括如下内容。

a） 说明个人信息主体对其个人信息拥有何种权利及行权途径，内容包括但不限于：

1） 对个人信息收集、使用、对外提供、公开披露等的选择权和拒绝权；

2） 个人信息主体所具备的查阅、复制、更正、补充、删除等权利；

3） 个人信息主体在自动化决策方面的可选项，如可以选择的广告偏好、是否同意进行个性化推荐、是否允许进行跨平台的广告推荐等；

4） 个人信息主体不再使用服务后撤回同意和注销账户的渠道；

5） 个人信息主体进行投诉举报、维权的有效渠道等；

6） 个人信息主体在接受通知方面的可选项，如是否接受短信、电话通知和推销等。

b） 如果需要个人信息主体自行配置或操作（如对所使用的软件、浏览器、移动终端等进行配置和操作）以行使 a）中权利的，对配置和操作的过程进行详细说明；说明方式应易于个人信息主体理解，必要时提供技术支持的渠道（客服电话、在线客服等）。

c） 如果为个人信息主体提供隐私偏好设置的，说明具体的设置方法。

d） 如果个人信息主体行使权利的过程将产生费用的，明确说明收费的原因和依据；

e） 如果个人信息主体提出行使权利的需求后需要较长时间才能响应的，明确说明响应的时间节点，以及无法短时间内响应的原因。

f） 如果个人信息主体行使权利的过程需要再次验证身份的，明确说明验证身份的原因、依据和方式，并采取适当的控制措施，避免验证身份过程中造成的个人信息泄露。

g） 如果个人信息处理者拒绝个人信息主体行使权利的，明确说明拒绝的原因和依据。

h） 明确联系渠道，包括：

1） 明确列出个人信息处理者接收涉及个人信息处理相关反馈和投诉的渠道，例如个人信息安全责任部门的联系方式、地址、电子邮件地址、个人信息主体反馈问题的表单等；

2） 明确个人信息主体在提供反馈或发起投诉后收到回应的时间；

3） 明确外部争议解决机构及其联络方式，以应对与个人信息主体出现无法协商解决的争议和纠纷。

8.6 个人信息处理规则的更新

个人信息处理规则的更新规则应包括：

a） 明确在个人信息处理行为的变更对个人信息主体权益发生重大影响的，承诺及时更新个人信息处理规则；

b） 通知个人信息主体关于个人信息处理规则更新的方式或途径。

注：通常情况下，通知个人信息主体的方式包括：在个人信息主体登录信息系统时或在更新信息系统版本后个人信息主体登录使用信息系统时弹出窗口，个人信息主体使用信息系统时直接向个人信息主体推送通知，或向个人信息主体发送邮件、短信等。

8.7 个人信息处理规则的反馈、投诉和争议解决规则

个人信息处理规则的反馈、投诉和争议解决规则应：

a） 明确列出个人信息处理者接收涉及个人信息处理相关反馈和投诉的渠道，例如个人信息安全责任部门的联系方式、地址、电子邮件地址、个人信息主体反馈问题的表单等；

b） 明确个人信息主体在提供反馈或发起投诉后收到回应的时间；

c） 明确外部争议解决机构及其联络方式，以应对与个人信息主体出现无法协商解决的争议和纠纷。

注：外部争议解决机构通常为：个人信息处理者所在管辖区的法院、认证个人信息处理者个人信息处理规则的独立机构、行业自律协会或政府相关管理机构等。

9 个人信息处理规则的发布

发布个人信息处理规则的要求包括：

a） 在收集个人信息前，个人信息处理者应主动提示个人信息主体阅读个人信息处理规则，在个人信息主体首次开启产品或服务时，通过弹窗等形式提示阅读个人信息处理规则，相关内容应仅涉及 App 最主要业务功能收集个人信息情况，便于个人信息主体就常用的 App 最主要业务功能进行最小化便捷授权；其他业务功能所涉及的个人信息处理规则应在个人信息主体首次使用该项具体业务功能时，通过弹窗等形式提示阅读该业务功能相关的个人信息处理规则内容，并进行个人信息授权；

b） 个人信息处理规则应长期置于个人信息主体可便捷访问的页面，不应通过置于多级目录、缩减字号、淡化颜色、不提供简体中文版等方式干扰个人信息主体阅读；

c） 个人信息处理规则应提供机器可读的格式或链接（如可拷贝或下载的文本），以便于个人信息主体获取；

d） 应在 App 的设置首页提供个人信息处理规则的一键访问功能，便于个人信息主体查阅和保存，内容应包括 App 所有业务功能收集使用个人信息情况；

e） 产品或服务涉及多个业务功能时，个人信息处理者应明确个人信息处理规则仅用于向个人信息主体告知产品或服务个人信息处理总况，不应通过要求个人信息主体同意个人信息处理规则的形式一次性获得个人信息主体对多个业务功能的同意；

注 1：业务功能的区分参考 GB/T 35273—2020 的附录 C 和 GB/T 41391—2022 的附录 A。

注 2：如在个人信息主体仅使用一项业务功能时，确保其他未开启的服务类型不收集个人信息。

f） 个人信息主体逐步开启不同业务功能时，如涉及敏感个人信息的收集和使用的，个人信息处理

者应再次主动提示个人信息主体阅读相关的个人信息处理规则，如专门的处理规则或个人信息处理规则的相关部分内容；

g） 宜通过交互式选择界面体现个人信息处理规则的摘要内容，提升个人信息处理规则的可视化程度并保障个人信息主体自主选择的权利。

10 个人信息处理规则的修订

修订个人信息处理规则的要求包括：

a） 个人信息处理规则发生变化时，如涉及新服务类型上线，处理目的变化等，应及时更新个人信息处理规则，并以显著方式向个人信息主体主动展示更新的内容、更新的理由；

b） 个人信息处理者应在个人信息处理规则中提供链接，以使个人信息主体能够查阅过去 24 个月内曾正式发布的个人信息处理规则的历史版本；

c） 个人信息处理者不应以更新个人信息处理规则的方式强制要求个人信息主体同意收集超过必要个人信息范围之外的个人信息，或强迫个人信息主体同意对其各项权利的减损；

d） 对不涉及对个人信息主体权益重大影响的个人信息处理规则内容的修订，个人信息处理者应及时更新个人信息处理规则，并通知个人信息主体；

e） 对涉及对个人信息主体权益重大影响的个人信息处理规则内容的修订，以及处理个人信息数量较大的个人信息处理者制定或修订个人信息处理规则，个人信息处理者宜广泛征求用户代表、行业协会、专家学者的意见或建议，并充分吸收，主动接受社会监督。

11 个人信息处理规则的争议纠纷解决

个人信息处理者在收到个人信息主体关于个人信息处理规则的反馈、投诉时，应遵循以下规则：

a） 在十五个工作日内向个人信息主体给予清晰、明确的解释说明，并在个人信息主体要求时提供外部争议解决方式；

b） 在配合外部争议解决机构处置个人信息处理规则相关争议问题时，必要时应提供个人信息处理规则编制过程中形成的工作记录。

参 考 文 献

[1] GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南

[2] 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

[3] ISO/IEC 29100:2011 Information technology—Security techniques—Privacy framework

[4] ISO/IEC 29184:2020 Information technology—Online privacy notices and consent

[5] 中华人民共和国个人信息保护法(2021 年 8 月 20 日第十三届全国人民代表大会常务委员会第三十次会议通过).

[6] 中华人民共和国电子商务法(2018 年 8 月 31 日第十三届全国人民代表大会常务委员会第五次会议通过).

[7] 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).

[8] 常见类型移动互联网应用程序必要个人信息范围规定(2021 年 3 月 22 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).

[9] 电信和互联网用户个人信息保护规定(2013 年 7 月 16 日中华人民共和国工业和信息化部令第 24 号公布).

[10] 全国人大常委会关于加强网络信息保护的决定(2012 年 12 月 28 日第十一届全国人民代表大会常务委员会第三十次会议通过).

[11] CWA 16113:2012 Personal data protection good practices.

[12] APEC Privacy Framework, APEC, 2005.

[13] EU General Data Protection Regulation, 2016.

[14] The OECD Privacy Framework, OECD, 2013.