|  |  |
| --- | --- |
| ICS | 35.030 |
| CCS | L 80 |

中华人民共和国国家标准

GB/T XXXXX—XXXX



信息安全技术 互联网平台及产品服务隐私协议要求

Information security technology — Requirements of privacy policy of Internet platforms, products and services

(点击此处添加与国际标准一致性程度的标识)

2022-05-20

XXXX - XX - XX发布

XXXX - XX - XX实施

`

目次

前[言 III](#_Toc13412)

[1 范围 1](#_Toc23905)

[2 规范性引用文件 1](#_Toc10826)

[3 术语和定义 1](#_Toc18915)

[4 缩略语 2](#_Toc24446)

[5 概述 2](#_Toc9547)

[6 隐私协议的编制程序 3](#_Toc24230)

[7 隐私协议的内容 3](#_Toc20797)

[8 隐私协议的发布和可视化 6](#_Toc8370)

[9 隐私协议的修订 6](#_Toc29460)

[10 隐私协议的争议纠纷解决 7](#_Toc22111)

[参考文献 8](#_Toc1816)

1. 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：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、北京字节跳动科技有限公司、长城企业股份有限公司、北京百度网讯科技有限公司、深圳市腾讯计算机系统有限公司、OPPO广东移动通信有限公司、维沃移动通信有限公司、掌阅科技股份有限公司、上海商汤智能科技有限公司、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、奇安信科技集团股份有限公司、普信恒业科技发展（北京）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。

本文件主要起草人：洪延青、窦禹、薛颖、何延哲、杨钦、葛鑫、胡影、田申、薛晨、陈湉、何云云、李维扬、黄晓林、李妍洁、高超、刘笑岑、李昳婧、林星辰、吴迪、李杭敏、余方、伍莎莎、袁立志、杨丹、王一宇、易立、李阳春、宋子奕、程艳、高斯平、刘明、田林川、毛欣怡、付艳艳、孙淑娴、陈舒、成瑾、吴庚、王兴、宋小艾、周杨、武杨、朱垒、王丹辉、解伯延、张成、马可、贾科、张玮、安锦程、连禧宇、吴越、张娜、田明仁。

信息安全技术　互联网平台及产品服务隐私协议要求

* 1. 范围

本文件规定了互联网平台及产品服务隐私协议编制程序、具体内容、发布形式，增加隐私协议的可读性、透明性，以及处理隐私协议相关的争议纠纷等方面的要求。

本文件适用于规范个人信息处理者制定、发布隐私协议的过程，也适用于主管监管部门、第三方评估机构等对隐私协议进行监督、管理和评估。

* 1. 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

* 1. 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。

* + 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]

* + 1. 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]

* + 1. 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]

* + 1. 个人信息处理者　personal information handler

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。

[来源：GB/T 35273—2020，3.4，有修改]

* + 1. 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。

[来源：GB/T 35273—2020，3.7，有修改]

* + 1. 明示同意　explicit consent

个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主作出肯定性动作，对其个人信息进行处理作出明确授权的行为。

注：肯定性动作包括个人信息主体主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

[来源：GB/T 35273—2020，定义3.6]

* + 1. 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。

* + 1. 业务功能　business function

满足用户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。

[来源：GB/T 35273—2020,3.17,有修改]

* 1. 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）

* 1. 概述

制定、发布隐私协议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。

隐私协议应清晰、准确、完整地描述个人信息处理者的个人信息处理行为，并以便于用户阅读、理解的视角，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。

* 1. 隐私协议的编制程序

个人信息处理者在编制隐私协议时，应遵循以下程序：

1. 建立完善的个人信息安全管理体系，明确参与隐私协议编制的责任部门或责任人，以及人员职责分工，个人信息处理者的负责人应为体系建设和隐私协议编制提供足够的资源保障；
2. 针对产品或服务收集使用的个人信息进行分析，明确实现各服务类型所需收集的必要信息的范围，以及非必要信息之外的所打算收集使用的个人信息的范围，确保满足合法、正当、必要的要求；

注1：此步骤应参考《常见类型移动互联网应用程序（App）必要个人信息范围》

1. 涉及到可能对个人信息主体权益产生重大影响的行为，事先进行个人信息安全影响评估，进一步明确对收集使用个人信息的目的、方式、范围以及权利保障措施，使其不会对个人信息主体权益产生高风险影响；

注2：以下事项可认为对个人信息主体权益产生重大影响：处理敏感个人信息、利用个人信息进行自动化决策、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、向境外提供个人信息等。

1. 针对不同的服务类型，分别建立和维护个人信息处理情况描述表。描述表包括处理的个人信息类型、保存位置、流转需求、所涉及系统和责任主体等情况；
2. 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、更正、删除个人信息，及撤回同意和注销账号的渠道；
3. 基于a）-e）的工作内容，梳理有关信息，作为编制隐私协议的基础，根据本标准第7章内容进行编制隐私协议内容；
4. 编制隐私协议，应采用清晰易懂，符合通用的语言习惯，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；
5. 个人信息收集使用规则发生变化时，如涉及新服务类型上线，使用目的变化等，及时更新隐私协议，并向个人信息主体主动展示，并同时向个人信息主体说明更新的理由，保证历史版本可查。
   1. 隐私协议的内容

7.1 概述

隐私协议应至少包括适用范围、摘要、收集使用个人信息规则、保障个人信息安全的规则、保障个人信息主体权利的规则、个人信息跨境流动的规则、隐私协议更新的规则等，并提供个人信息处理者的联系方式。

7.2 隐私协议的发布主体和适用范围

隐私协议的该部分应包含个人信息处理者的身份和地址、个人信息保护负责人联系方式、隐私协议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。

7.3 隐私协议的摘要

该部分为隐私协议的重点说明，是隐私协议的一个要点摘录。目的是使个人信息主体快速了解隐私协议的主要组成部分、个人信息处理者所做声明的核心要旨。隐私协议的摘要可以至于完整隐私协议开始的部分，或以单独文件展示，隐私协议的摘要通常包括：

* 1. 个人信息主体常用业务功能收集的个人信息种类；
  2. 向第三方提供个人信息的主要场景；
  3. 个人信息主体行使权利的主要途径；
  4. 个人信息主体投诉举报的主要渠道；
  5. 其他需要个人信息主体关注的事项。

7.4 收集使用个人信息的规则

隐私协议的该部分内容包括：

* 1. 详细列举收集和使用个人信息的服务类型及具体的业务功能，不应使用概括性语言；

注：此步骤应参考《常见类型移动互联网应用程序（App）必要个人信息范围》中对服务类型的划分。

* 1. 根据不同服务类型，分别列出各业务功能所收集的必要个人信息类型和非必要个人信息类型，并以“个人信息收集清单”的形式统一集中展示；
  2. 描述实现特定业务功能所必需的必要个人信息类型时，应参考《常见类型移动互联网应用程序（App）必要个人信息范围》；
  3. 不应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，而应明确写明“我们收集您的姓名、电话号码、地址信息”；
  4. 收集身份证、护照、驾驶证等法定证件信息和个人生物识别信息时，应专门提醒个人信息主体此次收集活动涉及的信息，并说明处理目的、处理规则；
  5. 在“个人信息清单”中还应列明每类型个人信息被处理的方式、频次、时机，以及拒绝对该类型个人信息的处理可能对个人的影响；
  6. 统一集中展示服务或产品中所嵌入的各第三方代码或插件（如SDK）的名称，各第三方代码或插件所收集的全部个人信息类型，以及所处理个人信息的目的、方式、种类、频次、时机等处理个人信息的规则；
  7. 说明个人信息在使用过程中涉及的地理区域，如个人信息存储和备份的地域，个人信息传输过程中涉及的地域范围；如果个人信息存在跨境传输情况，需单独列出或重点标识；
  8. 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）以及需要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）；
  9. 确需改变信息收集和使用的目的，应当说明会征得个人信息主体的同意；
  10. 个人信息处理者说明是否需要共享、转让个人信息，并详细描述需要共享、转让的个人信息类型和原因、个人信息的接收方、对接收方的约束和管理准则、接收方使用个人信息的目的、个人信息共享、转让过程中的安全措施，及共享、转让个人信息是否对个人信息主体带来高危风险，并将以上内容形成“个人信息对外提供清单”；
  11. 个人信息处理者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类型、原因、是否对个人信息主体带来高危风险；
  12. 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，共享、转让和公开披露数据，如响应执法机关和政府机构的要求、进行个人信息安全审计、保护个人信息主体避免遭受欺诈和严重人身伤害等。

7.5 保障个人信息安全的规则

隐私协议的该部分内容包括：

1. 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；
2. 目前遵循的个人信息安全规程和此方面取得的认证。包含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；
3. 应描述提供个人信息后可能存在的安全风险；
4. 应表明在发生个人信息安全事件后，个人信息处理者将承担法律责任；
5. 应表明在发生个人信息安全事件后，将及时告知个人信息主体。

7.6 保障个人信息主体权利的规则

隐私协议的该部分内容包括：

1. 说明个人信息主体对其个人信息拥有何种权利，内容包括但不限于：个人信息收集、使用和公开披露时允许个人信息主体选择的个人信息范围，个人信息主体所具备的查阅、复制、更正、补充、删除等控制权限，个人信息主体可以选择的通信和广告偏好，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、个人信息主体进行投诉举报、维权的有效渠道等；
2. 对于需要自行配置或操作（如对所使用的软件、浏览器、移动终端等进行配置和操作）以达到查阅、复制、更正、补充、删除、撤回同意等目的，个人信息处理者应对配置和操作的过程进行详细说明，说明方式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）；
3. 如果为个人信息主体提供隐私偏好设置的，需说明具体的设置方法；
4. 如果个人信息主体行使权利的过程产生费用，需明确说明收费的原因和依据；
5. 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，需明确说明响应的时间节点，以及无法短时间内响应的原因；
6. 如果个人信息主体行使权利的过程需要再次验证身份，需明确说明验证身份的原因，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；
7. 如果个人信息处理者拒绝个人信息主体对个人信息进行查阅、复制、更正、补充、删除、撤回同意等的要求，需明确说明拒绝的原因和依据。

7.7 个人信息跨境流动的规则

如果因业务需求、政府和司法监管要求存在跨境信息传输情况，需详细说明需要进行跨境传输的数据类型，以及跨境传输遵守的标准、协议和法律机制（合同等）。

7.8 隐私协议更新的规则

隐私协议的该部分内容包括：

1. 涉及用户权益重大影响的隐私协议更新情形；
2. 涉及用户权益重大影响的隐私协议更新程序，包括对更新内容公开征求意见的平台、时限、对公众意见采纳情况的发布等；
3. 说明使用何种方式及时通知个人信息主体。

注：通常情况下采取的通知方式如：个人信息主体登录信息系统时、更新信息系统版本并在个人信息主体使用时弹出窗口、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、向个人信息主体发送邮件、短信等。

7.9 提供联系方式

隐私协议的该部分内容包括：

1. 个人信息处理者需要明确给出处理个人信息安全问题相关反馈、投诉的渠道，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，并明确个人信息主体可以收到回应的时间；
2. 个人信息处理者需给出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。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隐私协议的独立机构、行业自律协会或政府相关管理机构等。
   1. 隐私协议的发布和可视化

个人信息处理者在发布隐私协议时，应遵循以下规则：

1. 在收集个人信息前，主动提示个人信息主体阅读隐私协议，如在个人信息主体首次开启产品或服务，或首次注册账户时通过弹窗的形式提示阅读；
2. 隐私协议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获取。个人信息主体为查阅个人信息保护政策所做的点击操作，不应超过4次；
3. 产品或服务涉及多种服务类型时，仅将隐私协议用于向个人信息主体告知产品或服务个人信息处理总况的目的，不应通过要求个人信息主体同意隐私协议的形式一次性获得个人信息主体对多种服务类型的同意。

注：如在个人信息主体仅使用一项服务类型时，其他未开启的服务类型不应收集个人信息。

1. 个人信息主体逐步开启不同服务类型时，应再次主动提示个人信息主体阅读隐私协议的相关部分内容；
2. 不应以更新隐私协议的方式强制要求个人信息主体同意收集更多的个人信息，或削减个人信息主体的各项权利；
3. 宜通过交互式选择界面体现隐私协议的摘要内容，提升隐私协议的可视化程度并保障个人信息主体自主选择的权利。
   1. 隐私协议的修订

个人信息处理者在修订隐私协议，应遵循以下规则：

1. 对不涉及对用户权益重大影响的隐私协议内容修订，个人信息处理者应及时更新隐私协议，并及时通知个人信息主体。
2. 对涉及对用户权益重大影响的隐私协议内容修订，个人信息处理者应：
   1. 在其官方网站、个人信息保护相关行业协会互联网平台面向社会公开征求意见，征求意见时长不得少于三十个工作日，确保用户能够便捷充分表达意见；
   2. 充分采纳公众意见，修改完善平台规则、隐私政策，并以易于用户访问的方式公布意见采纳情况，说明未采纳的理由，接受社会监督；
   3. 大型互联网平台应就隐私协议的修订内容应征求主要由外部成员组成的独立机构的意见和建议。

注：大型互联网平台运营者是指用户超过五千万、处理大量个人信息和重要数据、具有强大社会动员能力和市场支配地位的互联网平台运营者。

1. 日活用户超过一亿的大型互联网平台运营者平台规则、隐私政策制定或者对用户权益有重大影响的修订的，应当经国家网信部门认定的第三方机构评估，并报省级及以上网信部门和电信主管部门同意。

注：如有关部门就隐私协议的修订作出其他规定的，从其规定。

* 1. 隐私协议的争议纠纷解决

个人信息处理者在收到个人信息主体关于隐私协议的反馈、投诉时，应遵循以下规则：

1. 在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；
2. 向外部争议解决机构主动提供隐私协议编制过程中形成的工作记录。

参考文献

1. ISO/IEC 29100：2011　Information technology—Security techniques—Privacy framework
2. ISO/IEC DIS 29184　Information technology—Online privacy notices and consent
3. APEC Privacy Framework，APEC，2005
4. Consumer Privacy Bill of Rights Act of 2015 (Administration Discussion Draft)，　White House，2015
5. CWA 16113：2012　Personal data protection good practices
6. EU General Data Protection Regulation，2016
7. EU-U.S Privacy Shield，2016
8. The OECD Privacy Framework，OECD，2013

