ICS 35.240.99
CCS L67

团 体 标 准

T/ISC 0066—2024

个人信息保护社会责任报告编写指南

Guidelines for Compiling Social Responsibility Reports on Personal Information Protection

（发布稿）

2024－11－26 发布 2024－12－25 实施

中 国 互 联 网 协 会 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。

本文件由中国互联网协会提出并归口。

本文件起草单位：中国信息通信研究院、中国互联网协会互联网行业社会责任建设工作委员会、恺英网络股份有限公司、厦门吉比特网络技术股份有限公司、 北京蜜莱坞网络科技有限公司、武汉斗鱼鱼乐网络科技有限公司 、唯品会（中国）有限公司、北京搜狐新媒体信息技术有限公司

本文件主要起草人：赵雯越、常琳、沈军、付丽娜、高岩、林慧琴、夏晓晖、浦洋、杜森、王阳、张亮、孙骞、郭洪文

引　言

随着法律法规及监管要求的逐步明确，个人信息保护对公开性和透明度的要求不断提升，个人信息处理者与公众及消费者信息公开及信息沟通的要求越来越具象。

为了更有效地落实《个人信息保护法》第五十八条“提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务：（四）定期发布个人信息保护社会责任报告，接受社会监督”，本文件基于法律法规要求以及个人信息处理者相关实践，提出了具有可操作性的指南，以指导个人信息处理者编写及发布个人信息保护社会责任报告。

鉴于当前个人信息处理者实践，个人信息保护社会责任报告可以社会责任报告、可持续发展报告、ESG报告（环境、社会、管治报告或环境、社会和治理报告）、社会影响力报告、企业公民报告等形式或其组成部分出现。

个人信息处理者对所发布个人信息保护社会责任报告的真实性、准确性和完整性负责，并接受政府、社会公众、新闻媒体及其他第三方监督。

个人信息保护社会责任报告编写指南

1 范围

本文件提供了个人信息保护社会责任报告编写指南，包括基本原则、报告内容、编制及发布流程。

本文件适用于指导提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者编写个人信息保护社会责任报告。非上述提及的个人信息处理者也可参考本文件编写个人信息保护社会责任报告。

个人信息处理者可根据自身合规要求、业务范围、经营状况及市场环境，对标准所提及的具体内容做适当调整及删减。

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 36001-2015 社会责任报告编写指南

GB/T 19000-2016 质量管理体系基础和术语

GB/T 35770-2022 合规管理体系　要求及使用指南

3 术语和定义

GB/T 36001-2015 界定的以及下列术语和定义适用于本文件。

3.1 个人信息保护社会责任报告　social responsibility report on personal information protection

基于与利益相关方进行个人信息保护社会责任沟通的需要，个人信息处理者定期或不定期对外公开发布的一种特定报告或特定章节，用于展示其个人信息保护社会责任理念和认识，并系统披露其社会责任活动及绩效信息的特定报告或特定章节。

[来源：GB/T 36001-2015，3.1，有修改]

3.2

绩效　performance

可度量的结果。

注：绩效可能与定量或定性的发现有关。绩效可能与活动、过程、产品（包括服务）、体系或企业的管理有关。

[来源：GB/T 19000-2016，3.7.8]

3.3

合规　compliance

履行个人信息处理者的全部强制性必须遵守的要求，以及其自愿选择遵守的要求。

[修订：GB/T 35770-2022，3.26，有修改]

4 缩略语

下列缩略语适用于本文件。

ESG 环境、社会和治理（Environmental, Social, Governance）

5 基本原则

5.1 合规性

个人信息保护社会责任报告需要遵守相关法律法规要求，法律法规要求披露的信息可按要求在报告中体现，报告不披露现法律法规禁止披露的信息，并保护信息所涉及利益相关方受法律法规保护的隐私和权益。

5.2 全面性

个人信息保护社会责任报告需要完整、客观、并尽可能全面体现个人信息保护方面的正面和负面表现，以及相关绩效信息，以便于利益相关方全面认知个人信息保护方面情况。

5.3 可及性

个人信息保护社会责任报告可采用纸质文件、电子文件等多种载体进行发布。个人信息处理者至少在一种渠道对外发布该报告，以确保所披露的信息易于被利益相关方获取和理解。

6 编制内容

6.1 总则

个人信息处理者考虑自身活动及与其活动有紧密联系的其他实体或个人的行动所导致的针对个人信息保护方面的潜在和实际影响，充分了解如下情况：

a） 自身的经营环境；

b） 所处的内外部环境；

c） 法律法规及监管要求；

d） 主要社会责任标准；

e） 行业内的个人保护保护相关事件及热点议题；

f） 与个人信息处理者发展密切相关的利益相关方的需求和期待。

注：了解方式包括：访谈、问卷、座谈、研讨、调研等。

个人信息处理者可根据所了解到的上述情况，结合自身合规要求、业务范围、经营状况及市场环境，对本章内容补充或删减，策划并撰写个人信息保护社会责任报告具体内容。

6.2 报告基本情况

报告所涉及的个人信息处理者基本情况信息，包括：企业概况、主要业务、价值观与发展理念、主要利益相关方等。

报告所涉及的时间范围和业务范围。

6.3 组织治理

6.3.1 使命理念

个人信息处理者所制定的、用于指导个人信息保护工作相关的战略、规划、方针、愿景、使命、理念等。

6.3.2 履责声明/承诺

个人信息处理者及其高级管理层所宣称的个人信息保护声明、承诺、工作方针等，以体现其对个人信息保护的重视和关注。

6.3.3 管理职责及组织架构

个人信息处理者所建立的涵盖董事会（适用时）、管理层、执行层、独立监督机构等个人信息保护相关的组织架构、管理职责、岗位分工以及具体的相关履职情况。

6.4 组织管理

6.4.1 个人信息管理情况

6.4.1.1 总则

针对个人信息保护，个人信息处理者所建立的全流程管理制度以及具体实施效果，若相关内容已在其他公开报告中涉及，可做适当引用。

6.4.1.2 收集阶段

针对个人信息保护，个人信息处理者在合法合规性的基础上，所建立的信息收集方面的管理制度，以及具体实施效果，例如：最小必要原则、个人信息主体自主意愿、明示告知、获取个人信息主体授权同意等。

6.4.1.3 存储阶段

针对个人信息保护，个人信息处理者所建立的信息数据存储、数据备份、数据恢复等方面的管理制度，以及具体实施效果，例如：最小化存储时间原则、去标识化、敏感个人信息加密存储等。

6.4.1.4 使用阶段

针对个人信息保护，个人信息处理者所建立的信息访问控制、信息使用/用户画像目的限制等使用方面的管理制度，以及具体实施效果。所披露的个人信息使用管理制度及实施效果宜涉及利益相关方关注的个人信息使用场景，例如：个性化展示、自动化决策等。

6.4.1.5 加工阶段

针对个人信息保护，个人信息处理者所建立的信息加工方面的管理制度，以及具体实施效果，例如：保证个人信息不被无关的相关方获知、加工过程系统持续稳定、如实告知个人信息主体对其个人信息的查询等。

6.4.1.6 传输、提供和公开阶段

针对个人信息保护，个人信息处理者所建立的信息传输、提供和公开方面的管理制度，以及具体实施效果，例如：个人信息影响评估、明示告知、传输前后对个人信息保护机制等。

6.4.1.7 删除阶段

针对个人信息保护，个人信息处理者所建立的信息删除及信息留存方面的管理制度，以及具体实施效果，例如个人信息留存时间、删除方式等。

6.4.2 合规要求识别及落实

针对个人信息保护，个人信息处理者所建立的、周期性的、持续性的跟进合规及监管要求机制。

个人信息处理者依据上述要求，不断完善内部制度与流程并积极整改问题（若涉及），确保合规要求的有效响应，并展示其落实情况和所取得的具体效果。

6.4.3 事件处置、应急响应及预警演练

针对个人信息保护，个人信息处理者所建立的信息数据泄露（丢失）、滥用、被篡改、数据被损毁、数据违规使用等安全事件的应急预案、应急处置等相关内容，以及应急演练实施效果。

个人信息处理者处理重大个人信息安全事件的情况及效果（若涉及）。

6.4.4 内审/自评估及第三方评估/认证/审计

针对个人信息保护，个人信息处理者对相关管理制度、实施效果、场景等进行的个人信息保护相关内审/审计及第三方评估/认证/审计工作的相关制度及具体情况。

6.4.5 内部意识提升及教育培训

针对个人信息保护，个人信息处理者面向全体员工、有权查看和处理个人信息的员工、相关业务人员、新入职员工等，所开展的、多层次、多维度的意识提升、教育培训、岗位考试、案例分享等多样活动的具体情况，宜披露具体绩效数据，例如：覆盖人次、累计时长、课程数量等。

6.5 消费者权益保护及服务提升

6.5.1 用户个人信息保护

针对个人信息保护，个人信息处理者所遵循的处置原则、功能设置、实施情况及效果，例如：保障用户对其个人信息控制权（如查询、复制、更正、删除、转移等）的具体方式等。

针对个人信息保护，个人信息处理者对特定群体（如：未成年人用户、老年用户、残障用户等）及多元用户（如：身处不同地区、处于不同知识水平、处于不同语言环境等相关用户）权益保护相关的特定管理规定、功能设置、实施情况及效果。

针对个人信息保护，个人信息处理者积极扩展相关技术及潜能，保障用户信息方面的良好实践，例如：用户号码隐私保护、“双清单”展示、匿名化数据处理、安全多方计算/差分隐私/区块链/人工智能等技术应用等。

6.5.2 用户沟通交流管理

针对个人信息保护方面，个人信息处理者所建立的体验评价、申诉投诉、政策查询、意见征集等用户沟通交流渠道，以及对所沟通交流事项的收集、统计、分析、处置等过程所对应的管理规定、实施情况及效果，宜披露具体绩效数据，例如：沟通交流的频次及数量、办结率/处置率等。

6.5.3 信息披露及提升公众意识

针对个人信息保护方面，个人信息处理者在官方网站、应用程序、行业组织会议等渠道，通过规则/算法展示、科普文章或视频、社会责任报告、会议发言等，面向公众所开展的信息披露、知识普及、意识宣传、警示案例教育等。

6.6 生态圈及供应链发展

6.6.1 生态圈及供应商筛选

个人信息处理者进行生态伙伴/供应商筛选时，考虑个人信息保护相关的基线要求；在不影响合法合规和服务质量的前提下，优先考虑个人信息保护表现优良、尤其是具有代表性和多元化的生态伙伴/供应商。

6.6.2 向第三方提供用户个人信息的管理规定

个人信息处理者与生态伙伴/供应商约定个人信息及数据的使用目的、使用范围、保密约定、安全责任等内容，约定方式可通过合同、协议等形式。

个人信息处理者向第三方提供个人信息的管理规定，例如：用户知情同意并获取授权,匿名及去标识化,配合司法机关/行政机关等调证、提供用户个人信息等。

6.6.3 生态圈及供应商监督管理措施

根据生态伙伴/供应商个人信息保护的实际情况，基于责任共担、生态共建、互信共赢的理念，个人信息处理者所制定的生态圈及供应链监督管理措施，例如：普查抽查、评级定级、罚款限流、下架等，宜披露具体绩效数据和实践案例，例如：监督措施实施的次数、对象、效果、典型案例等。

6.6.4 生态圈及供应商履责支持措施

根据生态伙伴/供应商个人信息保护的实际情况，基于责任共担、生态共建、互信共赢的理念，个人信息处理者所制定的生态圈及供应链履责支持及鼓励措施，例如：投入技术/人力/资金支持、提供培训/指导/咨询/流量支持/项目扶持、总结表彰良好实践等，宜披露具体绩效数据和实践案例，例如：支持鼓励措施的提供次数、措施覆盖率、生态伙伴/供应商参与情况、生态伙伴/供应商履责效果等。

6.7 促进产业提升

6.7.1 技术研发及应用

针对个人信息保护方面，个人信息处理者所建立的支持鼓励前沿技术积累、研发创新、技术应用、知识产权保护、成果转化方面的相关管理办法、激励政策及实施效果，例如：软件著作权、发明专利、国家或行业奖项、试点示范、第三方认证等。

6.7.2 产业发展

针对个人信息保护方面，个人信息处理者利用技术优势及业务积累，积极参与的相关产业政策、法律法规、标准编制、公共事务管理、行业自律及治理活动、技术生态建设、产业人才培养、产业孵化基地等方面的相关工作及成果。

7 编制及发布流程

7.1 总则

个人信息处理者编制及发布个人信息保护社会责任报告的流程通常包括如下步骤：

a） 组建报告编制小组；

b） 策划报告内容；

c） 报告信息采集、筛选及审核；

d） 撰写报告并设计排版；

e） 报告批准；

f） 报告发布；

g） 报告影响评估的跟踪及反馈。

7.2 组建报告编制小组

个人信息处理者根据个人信息保护相关的管治架构，联合内部相关部门，宜组建个人信息保护社会责任报告编制小组，小组负责人宜由高级管理层人员担任，例如：首席数据官等。

个人信息处理者可视情况，委托外部专业机构承担部分工作，或组建专家团队提供专业意见。

报告编制小组宜制定工作计划，包括职责分工、工作进度、里程碑节点等。

7.3 策划报告及内容

7.3.1 报告的时间范围和发布频次

个人信息处理者宜充分考虑报告内容的连续性，自行选定个人信息保护社会责任报告所覆盖的时间范围和发布批次，例如：可每一年或两年发布报告，报告的时间范围可以自然年度，也可与企业财年保持一致。

若发生引起社会广泛关注的个人信息保护方面的重大事件或重大变化时，个人信息处理者可不定期发布相关报告。

7.3.2 报告范围

个人信息保护社会责任报告的内容应遵循相关法律法规要求，宜尽可能覆盖个人信息保护相关的个人信息处理者所涉及的运营业务，范围需要作为报告的具体内容之一而如实体现（参考本文件第6.2章）。

7.3.3 报告具体内容

个人信息处理者策划个人信息保护相关的具体内容（参考本标准第6章）。

7.4 报告信息采集、筛选及审核

7.4.1 报告信息采集

个人信息处理者根据所策划的报告内容，开展信息采集，信息来源包括但不限于：应用程序、业务系统、内部数据库、调研问卷、座谈访谈、客户及消费者反馈以及其他合法及公开的途径。

7.4.2 报告信息筛选及信息审核

个人信息处理者可建立机制，针对所采集的信息进行筛选及审核，筛选原则包括但不限于：

a） 法律法规等合规要求；

b） 该信息披露后对个人信息处理者的影响。

审核维度包括但不限于：

a） 信息的真实性；

b） 信息的有效期；

c） 信息的颗粒度；

d） 信息的全面性；

e） 信息统计方法及口径的适用性和一致性。

对于拟在报告中首次披露的信息，个人信息处理者宜严格按照个人信息处理者内部信息的筛选及审核程序实施相应流程，确保信息的适宜性；对于在报告中持续性披露的信息，个人信息处理者宜关注信息统计方法及口径的一致性，以确保持续性披露信息的连贯性和可比性。

7.5 撰写报告并设计排版

个人信息处理者根据审核通过的信息，对报告进行文字撰写。为增强报告的可读性，可综合实用性和美观性，对报告进行设计排版。

7.6 报告批准

报告内容经个人信息处理者的高级管理层正式批准。

7.7 报告发布

个人信息处理者可根据自身时间规划而发布报告，报告可引申为多种形式，例如：简化版、视频版、游戏互动版等，报告发布渠道可选择一种或多种，例如：官方网站、应用程序、公众号等。

个人信息处理者可在与利益相关方的交流座谈、商业谈判、营销服务等过程中，重复使用报告内容，扩大报告的辐射范围，增强影响力，最大化报告的应用价值。

7.8 报告影响评估跟踪及反馈

个人信息处理者可采取访谈、问卷、座谈、研讨、调研、业务系统推送等技术手段和工具，对个人信息保护社会责任报告的发布效果、利益相关方的反馈、传播数据等进行跟踪、挖掘和分析，评估报告的辐射范围和影响力等，以便为下一次报告编写及发布的策划和改进提供参考。