



中华人民共和国国家标准

GB/T 46071—2025

数据安全技术 数据安全和个人信息 保护社会责任指南

Data security technology—Guidance on social responsibility of data security and
personal information protection

2025-08-29 发布

2026-03-01 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 总则 2

6 组织治理 2

7 合规性、创新性和价值体现..... 5

8 公平运行、竞争和合作..... 7

9 用户权益保护..... 10

10 公益参与和社会发展 12

11 社会责任履行情况披露 14

附录 A（资料性） 数据安全和个人信息保护社会责任绩效评价方法 16

附录 B（资料性） 数据安全和个人信息保护社会责任实践案例 29

附录 C（资料性） 数据安全和个人信息保护社会责任报告模板 34

参考文献 36



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：北京赛西科技发展有限公司、中国科学院信息工程研究所、中国电子技术标准化研究院、中国网络安全审查认证和市场监管大数据中心、北京百度网讯科技有限公司、北京快手科技有限公司、蚂蚁科技集团股份有限公司、国家信息技术安全研究中心、公安部第三研究所、深圳赛西信息技术有限公司、贝壳找房(北京)科技有限公司、上海合合信息科技股份有限公司、南方电网数字电网集团信息通信科技有限公司、天翼云科技有限公司、荣耀终端股份有限公司、北京零一万物科技有限公司、旗天科技集团股份有限公司、北京抖音信息服务有限公司、阿里巴巴(北京)软件服务有限公司、广州竞远安全技术股份有限公司、北京腾云天下科技有限公司、上海杉涌律师事务所、西北工业大学、深圳市网安计算机安全检测技术有限公司、深圳国家金融科技测评中心有限公司、广州虎牙科技有限公司、上海飞书深诺数字科技集团股份有限公司、清华大学、北京企报产经在线文化传媒有限公司、广州赛西标准检测研究院有限公司、国浩律师(北京)事务所、北京天融信网络安全技术有限公司、华能信息技术有限公司。

本文件主要起草人：何延哲、高能、李敏、樊华、朱雪峰、范科峰、落红卫、许玉娜、李琳、杨韬、孟亚平、白晓媛、郭建领、张朝、黎水林、赵冉冉、宣琦、王海棠、王福彪、宋宏宇、李映婧、何刚、陈彬、吴月升、陆冰、彭晋、王昕、薛颖、邹秋阳、刘艾婧、徐欢、谢蜜、王平、龙军、程彦昊、吴佳美、陈深梓、王传银、张有义、廖超豪、葛梦莹、王震、黄蓉、罗丰、徐京、黄榴勇、杜浩文、高超、盛夏、张丁爽、王明彦、张明英、赵晓娜、陈心怡、梁哲琛、黄胜华、李政葳、张辉、晋钢、苏旂旒、韩硕、胡静、邱建中、苏力。

数据安全技术 数据安全和个人信息 保护社会责任指南

1 范围

本文件提供了组织实施数据安全和个人信息保护社会责任的组织治理、合规性、创新性和价值体现、公平运行、竞争和合作、用户权益保护、公益参与和社会发展,以及社会责任履行情况披露的指南。

本文件适用于组织开展数据安全和个人信息保护社会责任相关活动,也适用于第三方机构评价组织履行数据安全和个人信息保护社会责任的情况。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

社会责任 social responsibility

组织通过透明和合乎道德的行为为其决策和活动对社会和环境的影响而担当的责任。这些行为:

- 致力于可持续发展,包括社会成员的健康和社会的福祉;
- 考虑了利益相关方的期望;
- 符合适用的法律,并与国际行为规范相一致;
- 被融入整个组织并在组织关系中实施。

注 1: 活动包括产品、服务和过程。

注 2: 组织关系是指组织在其影响范围内的活动。

[来源:GB/T 36000—2015,3.16]

3.2

利益相关方 stakeholders

其利益可能会受到组织决策或活动影响的个人或团体。

[来源:GB/T 36000—2015,3.13]

3.3

消费者 consumer

出于私人目的而购买或使用财产、产品或服务的个人。

[来源:GB/T 36000—2015,3.19]

3.4

员工 employee

与组织通过劳动合同建立起劳动关系或存在事实劳动关系的个人。

[来源:GB/T 36000—2015,3.20]

3.5

弱势群体 vulnerable group

因具有一个或多个共同特点而易遭受歧视或处于不利的社会、经济、文化、政治或健康状况,乃至缺乏手段以实现其权利或享有平等机会的个体所组成的群体。

[来源:GB/T 36000—2015,3.15]

3.6

身体机能差异人群 people with physical disabilities

由于身体的某些机能丧失或弱化,因而在获取和使用信息方面存在困难的人群,其中包括残障人群、老年人群、身体机能未发育成熟的幼年人群等。

3.7

大型网络平台 large scale network platform

注册用户 5 000 万以上或者月活跃用户 1 000 万以上,业务类型复杂,网络数据处理活动对国家安全、经济运行和国计民生等具有重要影响的网络平台。

4 缩略语

下列缩略语适用于本文件。

APP:应用程序(Application)

5 总则

数据安全和个人信息保护社会责任是《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》等法律法规中提出的组织应尽义务,履行数据安全和个人信息保护社会责任是指组织在遵守数据安全和个人信息保护法律法规以及基本道德规范的基础上,最大限度地致力于促进基于数据要素经济活动可持续发展,提升数字社会的公众福祉,弥补数字鸿沟和推进社会进步。

组织在其数据处理活动履行适用法律法规义务的基础上,宜按担责、透明、合乎道德的行为、尊重利益相关方的利益、尊重法治、尊重国际行为规范和尊重人权等原则,从组织治理,合规性、创新性和价值体现,公平运行、竞争和合作,用户权益保护,公益参与和社会发展五方面主题,以及主题所包含的议题,履行数据安全和个人信息保护社会责任。

第 6 章~第 10 章中的主题和议题并不完全适用于所有组织,组织可结合所在地区的经济、社会和环境发展水平、自身行业特征、规模、性质、发展阶段和利益相关方期望,识别确定每项数据安全和个人信息保护社会责任主题和议题中适用的具体内容。

组织或第三方机构可通过开展数据安全和个人保护社会责任绩效评价的方式识别社会责任履行的薄弱环节,不断提升履行数据安全和个人信息保护社会责任的成熟度,评价方法见附录 A。其中,评价得到的绩效等级并非代表社会责任工作是否到位,不同规模、发展阶段和行业特征的组织将可能分布在不同的绩效等级,参与评价可为同等规模和同样发展阶段的同业组织提升履行社会责任水平提供参考,帮助其制定数据安全和个人信息保护社会责任工作的方针、目标和工作计划。

组织在数据安全和个人信息保护社会责任方面的实践案例见附录 B。

6 组织治理

6.1 发展理念和承诺声明

6.1.1 议题描述

发展理念是组织基于长久秉持的基本价值取向,明确组织进行决策和活动的核心指导原则,以及所

担负的愿景或使命、所追求的创立宗旨和所秉承的发展哲学等,从发展理念层面强调数据安全和个人信息保护的重要性对全面履行相关社会责任至关重要。组织通常通过管理层的承诺声明形式表明对发展理念的态度,管理层承诺声明有利于推动管理层对数据安全和个人信息保护社会责任相关工作予以重视。

6.1.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面:

- a) 组织在已成文并广泛推广的发展理念中阐述关于数据安全和个人信息保护相关的价值观、愿景、使命或宗旨等;

注:例如,在产品或服务的设计理念中体现数据安全和个人信息保护为最优先考虑的要素。

- b) 组织的管理层在正式和公开的场合阐述组织数据安全和个人信息保护的组织战略和发展理念等,并以承诺声明等形式予以强调;
- c) 组织的管理层在内部宣贯和培训等场合向员工阐述组织数据安全和个人信息保护的组织战略和发展理念等,以促进相关价值理念和价值观等得以贯彻;
- d) 设置对数据安全和个人信息保护社会责任发展理念和管理层承诺声明的跟踪机制,允许内部和外部人员对其进行评价和监督。

6.2 工作实施和资源支持

6.2.1 议题描述

组织中具体负责数据安全和个人信息保护社会责任工作的部门或人员,按照社会责任相关的工作方针和目标,制定工作计划并推动相关工作落实。同时,组织为推动数据安全和个人信息保护社会责任工作提供人力、财务和环境等资源。实施主体、工作计划和资源支持是数据安全和个人信息保护社会责任相关工作有效落实的前提,是数据安全和个人信息保护社会责任机制长期稳定运行的重要基础。

6.2.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面:

- a) 将数据安全和个人信息保护等方面的内容纳入组织的社会责任工作方针和目标中,并形成纲领性文件,在组织内向有关部门和人员进行下发,使其能充分地沟通和理解,并在日常工作中得以贯彻执行;
- b) 指定高层管理人员担任或兼任实施数据安全和个人信息保护社会责任工作的负责人并明确其职责,如任命高层管理人员担任个人信息保护合规官(PIPO)、首席隐私官(CPO)或个人信息保护负责人等职位,并由其负责履行相关社会责任的组织管理工作;

注 1: 作为负责人的高层管理人员职务、姓名和联系方式至少在组织层面予以公开。

- c) 指定负责数据安全和个人信息保护社会责任工作的部门或人员,明确其履行社会责任的工作职责和工作计划;

注 2: 选择指定部门还是人员取决于组织的经营规模、处理数据的量级和人员配备等情况。

- d) 为履行数据安全和个人信息保护社会责任提供相应的财务预算;
- e) 在相关部门或人员的工作职责中明确定期向社会披露社会责任履行情况,如定期发布包含数据安全和个人信息保护相关内容的社会责任报告;
- f) 建立有效的内审或评估机制,保障数据安全和个人信息保护社会责任的工作计划得以有效实施,并保持实施的质量和可持续性;
- g) 为获取数据安全和个人信息保护相关的社会反馈信息提供技术支持,以便相关部门或人员全面了解利益相关方在数据安全和个人信息保护社会责任方面的期望和诉求,并积极沟通回应。

注 3：获取社会反馈的信息渠道包括：新闻媒体报道、互联网社交或信息发布平台等的热议话题、投诉和举报渠道等。

6.3 制度宣贯和人员培训

6.3.1 议题描述

组织通过开展宣贯法律法规、政策和制度等的各类活动，使组织内部员工深刻理解并付诸实践。组织通过各种方式或手段督促员工在知识、技能和态度等方面有所改进，以达到预期目标。宣贯和培训将推动数据安全和个人信息保护社会责任相关工作在内部有广泛的认可度，并提高员工对相关工作的配合意识。

6.3.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面：

- a) 在管理制度中明确贯彻落实数据安全和个人信息保护社会责任的相关内容，并将制度文件下发至相应部门和人员；

注 1：管理制度包括负责落实社会责任的组织架构体系、相关部门和人员职责、工作方针和目标等，具体见 6.2。

- b) 定期开展数据安全和个人信息保护社会责任理念、制度、知识和案例等的宣贯和培训工作；
- c) 鼓励员工积极学习数据安全和个人信息保护相关的知识和技能，为其提供数据安全和个人信息保护相关知识技能培训，并鼓励员工参与外部专业培训并获取职业技能证书；
- d) 聘请数据安全和个人信息保护专家，对负责落实数据安全和个人信息保护社会责任相关工作的关键岗位人员（如个人信息保护负责人、相关部门责任人和社会责任报告编制人等）进行重点培训。

注 2：数据安全和个人信息保护专家具备在履行相关社会责任方面的经验，参与过丰富的数据安全和个人信息保护社会公益活动，并优先选择受到权威组织表彰和社会广泛认可的专家。

6.4 内部监督和员工激励

6.4.1 议题描述

组织对社会责任战略的实施、相关主体职责的履行和各方面资源保障等情况进行监督检查，评价组织内部管理的有效性，发现组织管理缺陷并及时改进。组织通过有效的手段，激发员工的动力，充分挖掘潜力，以达到预期目标。监督和激励措施有助于提升数据安全和个人信息保护社会责任相关工作的内部执行力。

6.4.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面：

- a) 建立内部监督机制，包括便捷的内部投诉或举报或通道，由数据安全和个人信息保护社会责任工作相关的部门或人员接收内部人员反馈的监督意见，推动相关意见得到处理并注意保障内部意见反馈人员的相关权益；
- b) 将数据安全和个人信息保护社会责任履行情况纳入内部合规审计工作内容中；
- c) 鼓励员工通过参与数据安全和个人信息保护的社会公益活动或相关实践活动、社会培训和资格考试等方式提升能力水平；
- d) 将相关人员充分、积极和主动履行数据安全和个人信息保护社会责任职责和义务纳入到其绩效考核体系中，如相关工作取得积极社会反响在绩效考核时予以加分或给予奖励。

注：获得权威部门的感谢信、奖状或公开表彰通知等视为取得积极社会影响。

7 合规性、创新性和价值体现

7.1 产品或服务的合规性

7.1.1 议题描述

产品或服务在数据安全和个人信息保护方面的合规性,是指产品或服务在遵守法律法规、规章和强制性标准等的基础上,参照适用的标准等追求更高的合规水平。合规工作主要表现为组织开展制度、文档、策略和流程的建设,完成内审、自评估、第三方评估或第三方审计,以及获得认证等。

7.1.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面:

- a) 通过组织内自行发起或引入第三方机构对产品或服务相关法律法规、规章和标准的符合情况进行评估或审计,并形成评估或审计记录、结论和报告以指导产品或服务持续改进;

注 1: 评估或审计适用的标准化文件包括国家标准、国际标准、行业标准或团体标准等。

- b) 引入第三方机构评估,取得并维持产品或服务在数据安全和个人信息保护方面的合规认证(包括国内和国际);

注 2: 数据安全和个人信息保护认证的评估依据见 GB/T 35273 和 GB/T 41479。

- c) 发布数据安全和个人信息保护合规相关的说明(如白皮书、报告或声明等),向外界披露组织在数据安全和个人信息保护合规方面的履责情况,增进利益相关方对产品或服务所采取合规措施的理解;



- d) 在组织层面建立产品或服务的合规性的监督机制,采取发布前审核、不定期抽检和定期内审等手段,督促产品或服务持续保持合规水平;

- e) 建立数据安全和个人信息保护合规风险管理体系,基于法律法规、规章、标准和外部环境等的变化对合规实施动态管理,及时发现、预警和处置合规风险,不断提升合规能力水平。

7.2 技术的创新性和先进性

7.2.1 议题描述

组织推动数据安全和个人信息保护相关技术的不断创新,能更高效、低成本解决数据安全和个人信息保护方面的问题,或对提升相关生产力水平、推动经济发展和社会进步有促进作用。组织通常以研究成果转化等方式,实现产品或服务在数据安全和个人信息保护水平的突破性进展,为行业和社会创造经济效益和社会效益。

7.2.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面:

- a) 构建数据安全和个人信息保护创新性和先进性的评价标准和指导方针;
- b) 建立对数据安全和个人信息保护技术创新的长期激励机制,包括管理制度、绩效考核或资金奖励等;
- c) 参与申报并实施数据安全和个人信息保护相关的科研项目;
- d) 产品或服务数据安全和个人信息保护相关技术的创新性和先进性获得外部认可,包括获得专利、成为优秀案例和获得奖项等;
- e) 对具备数据安全和个人信息保护相关技术创新性和先进性且产业实践效果良好的产品或服务,通过参赛和试点应用等方式扩大其影响面和应用面;

- f) 将获得的数据安全和个人信息保护专利和获得的科技奖项等作为组织宣传的重要素材予以体现；
- g) 构建同行业交流机制或交流平台，交流分享创新性理念和方法，并为技术创新提供学术研究和国际交流等方面的有利条件；
- h) 整合系列具有自主知识产权且在创新性和先进性上具有显著优势的数据安全和个人信息保护相关技术，形成相关的产品或服务，并创立行业知名品牌，为提升行业整体水平和在国际上展现竞争力有显著作用。

7.3 产品或服务的使用价值

7.3.1 议题描述

产品或服务的使用价值包括对用户和社会方面的价值。当用户使用产品或服务时，组织通过充分履行数据安全和个人信息保护责任，推动数据得到充分利用并发挥其应有价值，可为用户提供普惠、便捷、智能和安全的服务；同时，数据安全和个人信息保护相关的产品和服务可为推动公众参与数据安全和个人信息保护社会共治提供条件，支撑有关部门开展有关系统性治理活动，营造全社会数据安全和个人信息保护良好氛围。

7.3.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面：

- a) 用户使用产品或服务的相应功能仅处理实现该功能所必要的数据；
注 1：在用户使用功能时不设置不合理的条件，如无关功能捆绑、设置过长的等待时间或增加操作步骤等。
- b) 产品或服务将数据安全和个人信息保护相关功能设置为基础功能的一部分；
注 2：基础功能中的数据安全和个人信息保护相关功能通常不向用户收取费用。
- c) 产品或服务所提供的推荐功能或选项主动引导用户加强数据安全和个人信息保护，以推动大范围用户强化数据安全和个人信息保护设置；
注 3：如拥有大量用户的产品或服务，通过默认设置等方式向用户提供数据安全和个人信息保护的功能。
- d) 通过不断优化数据处理的流程和步骤，以优化收集数据时机和场景，减少收集数据的种类和存储时间，在不影响使用的前提下不断拓宽数据脱敏、去标识化和匿名化处理技术的应用面；
- e) 在不影响用户权益并取得合法授权的前提下，通过使用算法或模型处理数据和个人信息进行自动化决策等方式挖掘数据价值，包括提升服务质量、提高响应效率和强化安全保障等；
- f) 产品或服务可支撑有关主管监管部门、社会或行业组织等开展的数据安全和个人信息保护相关的治理等活动。

7.4 数字包容和特殊保护

7.4.1 议题描述

组织通过为多元化群体，尤其是身体机能差异人群（如未成年人、残障人士或高龄老人等）提供更人性化和安全的数据服务，更好地贯彻个人信息优先保护和默认保护等增强保护的理念，保障多元化群体在网络空间和数字社会中的各类权益，使得多元化群体公平、自由和安全地获取和享受技术变革和产业

7.4.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面：

- a) 产品或服务设置无障碍功能，为多元化群体提供平等的数字产品或服务的同时，重视并保护多

元化群体的数据和个人信息,为多元化群体提供符合其应用场景和自身特性的数据安全和个人信息保护机制;

- b) 收集身体机能差异人群的个人信息前,充分评估处理个人信息对其权益的影响,评估时在通用评估方法的基础上考虑身体机能差异人群权益侵害后危害可能加重的因素,以促使采取更为严格的安全保护措施降低风险;

注:评估依据见 GB/T 39335。

- c) 在面向身体机能差异人群提供符合其使用习惯的产品或服务时,为其提供个人信息的增强保护机制,如监护人同意、辅助操作和便捷行使权利的模式,对其个人信息使用场景进行严格限制等;
- d) 制定身体机能差异人群个人信息处理规则,并为身体机能差异人群提供专门的服务页面和服务渠道,使其感知和获取个人信息处理规则等方面的信息;
- e) 参与身体机能差异人群数据安全和个人信息保护相关标准制定,加入相关倡议或计划等活动,以促进行业协同;
- f) 投入资源主动推广身体机能差异人群使用的产品或服务(或相关功能模式),并通过公益宣传活动为其科普数据安全和个人信息保护知识,引导身体机能差异人群关注使用产品或服务时保护自身个人信息;
- g) 对数字包容和身体机能差异人群保护方面的涉及数据安全和个人信息保护的技术能力和技术资源进行开放,为行业提供参考和支撑。

8 公平运行、竞争和合作

8.1 数据处理规则的透明性

8.1.1 议题描述

组织以适当方式公开其数据处理的具体规则,明示处理的目的、方式和范围等,使利益相关方能够了解数据处理活动,从而增进利益相关方的信任,便于利益相关方进行监督和审计。

8.1.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面:

- a) 涉及个人信息处理时,在遵守相关法律法规的基础上,按公开透明原则,向个人完整、真实和准确披露个人信息处理的规则;

注:规则制定和披露相关内容见 GB/T 35273 和 GB/T 44588。

- b) 建立与利益相关方沟通的机制,就数据处理的目的、方式和范围等规则进行及时沟通后进行审核并确认。必要时向利益相关方提供专门的数据处理规则问询或答疑的渠道,针对复杂、疑难或关注度高的数据处理规则(如利用算法自动化决策相关的数据处理规则),可通过解释说明的方式以增进理解;
- c) 数据处理规则可能影响到利益相关方重大权益时,采取书面或口头告知等方式重点说明情况,无法取得联系方式的可采取公开发布的方式,便于利益相关方理解后做出决定;
- d) 数据处理规则影响范围广泛(如大型网络平台服务提供者的产品或服务的隐私政策)的组织,可通过向独立监督机构、第三方机构或业界专家征询意见等方式完善规则内容。

8.2 公平竞争和成果保护

8.2.1 议题描述

构建公平竞争环境,营造优胜劣汰的市场氛围,激励组织和生态内中小企业更加有效率地投资和创新,为以更优质的产品或服务满足消费需求和促进经济发展创造条件。通过保护组织创新的成果,如数据安全和个人信息保护的知识产权、商业秘密和其他财产性权益等,激励相关先进知识成果的共享和技术的迭代创新。

8.2.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面:

- a) 在数据处理相关的生产经营活动和参与市场竞争中,按自愿、平等、公平和诚信的原则,遵守竞争和知识产权保护相关的法律法规和商业道德,将公平竞争和知识产权保护作为组织治理、生产经营和商业活动的行为准则;
- b) 不以数据安全和个人信息保护为由进行自我优待,干扰其他组织产品或服务正常运行,干涉用户自主判断的行为;
- c) 制定并实施组织内部反腐败反舞弊制度,对管理层和员工在数据安全和个人信息保护方面的腐败和舞弊行为均采取零容忍态度;

注:腐败行为包括:通过利用权限删除或更改用户操作记录进行牟利,在业务合作中收受商业贿赂造成数据被超范围使用或共享等后果。

- d) 对所获得或使用的数据安全和个人信息保护相关知识成果共享支付合理的费用;
- e) 在行使并保护自身的数据安全和个人信息保护知识成果相关权利时,考虑社会期望和行业需求,尽可能创造更大价值;
- f) 通过内部培训和考试等方式,提高员工对数据安全和个人信息保护相关的反不正当竞争和知识产权保护等方面的意识和知识;
- g) 拥护政府部门构建平台经济公平竞争环境的政策和行动,积极配合监管部门对涉及数据安全和个人信息保护的反不正当竞争和知识产权保护调查和执法行动。

8.3 平台规则和供应商管理

8.3.1 议题描述

平台型组织是指通过连接不同的用户、供给方和需求方,以创造和提供价值的商业组织,平台型组织制定有效的数据安全和个人信息保护的策略、方针、制度、细则和程序等规则能促使参与方(如商户和合作伙伴等)切实履行相关责任和义务。组织建立供应商管理机制,实现平等交易和互利互惠的供应商关系,可促进供应商数据安全和个人信息保护水平的整体提升。

8.3.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面:

- a) 平台型组织所制定的平台规则,宜在遵守数据安全和个人信息保护相关法律法规、规章和标准等的基础上,关注行业最佳实践,引导参与方更好地执行保护数据安全和个人信息保护的策略和采取更有效的安全措施;
- b) 将数据安全和个人信息保护相关平台规则执行效果纳入审计等监督环节中,以推动平台规则切实有效执行;
- c) 定期开展平台规则整体执行效果评估,并根据评估结果对平台规则进行优化;可引入第三方机

构保障评估结果的客观性；

- d) 鼓励将数据安全和个人信息保护相关平台规则执行效果面向社会公开,如定期发布包含相关执行效果的报告等；
- e) 建立供应商管理制度,并在供应商筛选阶段公开相关制度,明确供应商遵守的数据安全和个人信息相关安全基线和淘汰指标等；
- f) 设立必要的监督机制维护供应商的公平竞争,不宜通过设定过于复杂或特殊的数据安全和个人信息保护能力入选条件,限制供应商的入选；
- g) 以合同或协议等方式与供应商约定数据的使用目的、使用范围、保密约定和安全责任等内容；
- h) 涉及与供应商使用数据接口等方式进行数据交换时,采取必要的技术手段对数据交换日志进行记录,如供应商不具备技术能力,酌情向其共享相关日志信息以增进透明性；
- i) 建立与供应商联动的应急响应机制,对合作过程中发现的数据安全风险和发生的数据安全事件及时响应,向供应商同步相关信息,并为供应商提供必要的技术和人员等资源支持；
- j) 注重与供应商的长期合作,协助供应商解决数据安全和个人信息保护方面面临的困难和问题,建立互信共赢的合作关系。

8.4 行业共治和知识共享

8.4.1 议题描述

组织通过加入行业组织和联合相关领域组织、开展行业自律行动、参与标准编制、分享知识成果和促进先进技术落地应用等,与行业组织和同业伙伴共同推动在数据安全和个人信息保护方面得到发展和取得更大效益。

8.4.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面内容。

- a) 积极加入数据安全和个人信息保护相关行业组织,响应行业组织发起的自律活动,如加入数据安全和个人信息保护相关的自律倡议书、工作计划或国际协定等。
- b) 积极参与数据安全和个人信息保护相关标准的研制和试点验证等工作。
- c) 自行或与其他组织合作,以多种方式参与数据安全和个人信息保护相关知识共享,包括:
 - 1) 发布相关的白皮书,分享优秀经验和案例；
 - 2) 与高校或培训机构等联合开发相关课程；
 - 3) 鼓励员工发表技术文章、参与专刊或专著撰写等；
 - 4) 发表数据安全和个人信息保护相关科研论文；
 - 5) 获得授权后向开源社区等分享相关源代码；
 - 6) 向具有法定职能的组织共享数据安全威胁事件情报。
- d) 自行组织或主动参与推动数据安全和个人信息保护产业发展和技术创新等方面的活动,并关注活动的专业性和公正性,常见的活动有:
 - 1) 数据安全和个人信息保护主题的会议和沙龙等；
 - 2) 数据安全和个人信息保护相关的比赛和评比等；
 - 3) 数据安全和个人信息保护相关的展览等。
- e) 在所涉行业、领域或自身业务范围内促进数据安全和个人信息保护先进技术的推广和应用,如区块链、数据沙箱和隐私保护计算等新兴技术。

9 用户权益保护

9.1 人身财产利益保护

9.1.1 议题描述

组织提供的产品或服务不会因未尽数据安全和个人信息保护义务而给用户(主要为消费者)带来严重的人身和财产(包括虚拟财产)损害风险,并通过多种识别风险的机制,防范损害用户人身和财产利益的行为发生。

9.1.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面内容。

- a) 在产品或服务的设计和开发过程中,通过以下方法最大程度地降低用户人身和财产损害的风险:
 - 1) 分析产品或服务在所有使用场景、阶段和条件下,可能对用户人身和财产产生损害的功能组件或服务场景,评估损害风险并明确防止损害的具体措施;
 - 2) 充分考虑用户的需求差异、能力差异或局限性(尤其是了解信息所需时间的差异或局限性),优化产品或服务的设计方案,防止因其导致用户利益受损;
 - 3) 按以下优先级顺序降低对用户利益的风险:首先,考虑采用完全消除风险的安全设计;其次,考虑增设保护性机制降低风险;最后,考虑向用户提供警示信息。
- b) 如有充分证据表明,现已存在能显著提高数据安全和个人信息保护水平的解决方案,在综合考虑组织大小、特性和经济状况等因素后,及时积极采取并落实该等解决方案。
- c) 在产品或服务的使用过程中,建立识别用户风险行为的特征库和识别机制。
注 1: 如对用户发布信息中涉及隐私的内容进行自动判别。
- d) 建立识别损害用户人身和财产利益违法违规行为的特征库,并持续监测和防范违法行为,识别用户存在风险行为时,通过显著方式向用户警示可能出现的风险,同时视具体情况采取复合措施核验用户身份。
注 2: 基于用户风险行为级别不同,逐步增加身份验证的手段,以准确识别用户身份,同时保护身份验证信息的安全。
注 3: 除使用文字信息外,尽可能使用符号、图片或语音等方式向用户告知重要警示信息。
- e) 在用户使用产品或服务前,组织宜:
 - 1) 指导用户安全和正确使用产品或服务;
 - 2) 结合产品或服务的具体情况,说明与使用有关的风险和预防措施;
 - 3) 告知用户遭受或可能遭受人身和财产损害时的反馈渠道和处置方式。
- f) 当用户遭受或可能遭受人身和财产损害时,为用户提供便捷的反馈渠道并及时处置。
- g) 采取紧急措施以避免用户人身和财产利益继续受损,紧急措施涉及处理用户个人信息时严格限定处理范围并尽可能同步向用户告知相关情况。
- h) 在产品或服务的使用过程中,如出现重大安全漏洞或包含有误导或错误的信息,可中止提供服务以防止用户利益受损,并通知受影响的用户以采取补救措施。

9.2 用户权利行使保障

9.2.1 议题描述

组织在提供产品或服务时,受理用户关于数据安全和个人信息保护方面权利诉求和问题反馈,以保

障用户权利的行使和接受用户监督。组织还可通过用户的请求、投诉和建议等完善内部数据安全和个人信息保护的机制,不断优化用户行使数据安全和个人信息保护相关权利的方式。

9.2.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面:

- a) 以清晰和显著的方式披露数据安全和个人信息保护相关权利行使请求和投诉渠道、处理方式和反馈时限,并不断优化用户行使权利的路径和步骤;

注 1: 境外的组织面向境内用户提供行使权利的路径时,充分考虑境内用户的语言和操作等习惯。

- b) 公示的渠道稳定且易用,如涉及渠道的变更或转换,尽可能通过内部协调实现,不对用户带来不必要的困扰或打扰;

- c) 提供一定比例人工客服支持的投诉反馈渠道;

注 2: 比例可根据用户对投诉处理机制满意度的评价情况予以设定。

- d) 建立投诉处理流程,并持续完善操作规范,明确反馈时间,形成从投诉接收到投诉反馈的闭环,避免用户投诉无人处理、无人反馈和反馈超时等情况;

- e) 建立投诉分级处理制度,优先处理影响严重或影响面大的侵犯用户数据安全或者个人信息保护的投诉内容,对多次投诉未果或特殊投诉等复杂情形设立相关负责人受理的机制;

- f) 建立投诉处理满意度的反馈途径,便于用户通过该途径反馈意见或建议;

- g) 建立投诉处理库(不少于维保期,至少保留半年内投诉处理情况),记录投诉处理的时间、原因和处理情况等,并通过定期评估投诉和举报的数量、处理率和处理评价情况等,不断完善投诉处理机制;

- h) 处理用户权利行使相关投诉时不向用户收取费用,根据用户诉求处置相关事宜时涉及成本费用的除外;

- i) 定期公开用户权利行使和投诉汇总情况,如在社会责任报告等公开发布的文件中予以体现。

9.3 主动接受外部监督

9.3.1 议题描述

组织通过主动披露等方式使外部组织或个人了解组织在数据安全和个人信息保护方面的措施和成果,针对外部组织或个人提出的疑问和改进建议进行反馈和改进;此外,组织可通过成立主要由外部成员组成的独立监督机构对组织数据安全和个人信息保护情况进行指导和监督,以完善其数据安全和个人信息保护措施和制度体系。

9.3.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面:

- a) 向社会公开数据安全和个人信息保护相关的策略和规则,披露数据安全和个人信息保护社会责任履行情况,并公布联系方式主动接受社会监督;

- b) 面向社会征集数据安全和个人信息保护待改进问题和工作建议,视情况给予贡献者奖励;

- c) 大型网络平台服务提供者成立主要由外部成员组成的独立监督机构,对其个人信息保护情况进行监督;

注 1: 相关监督机构设立方法见 GB/T 45404。

注 2: 个人信息保护情况包括采取的个人信息处理规则、个人信息保护制度体系、个人信息保护影响评估、个人信息保护人员培训、个人信息保护合规审计、个人信息保护社会责任披露和个人信息保护安全事件应急处置等情况。

- d) 指定组织内负责数据安全和个人信息保护的具体人员,使其承担与外部组织或个人沟通和对

接的职责；

- e) 建立利益相关方和投资者沟通机制,对于其在数据安全和个人信息保护方面提出的意见和建议予以反馈；
- f) 向独立监督机构赋予对组织在数据安全和个人信息保护措施进行核实和质疑的权利,通过向独立监督机构如实提供数据安全和个人信息保护的相关管理和技术措施等方式接受其监督,如独立监督机构质疑得到证实,则予以纠正并采取措施防止同类问题发生。

9.4 自我保护素养提升

9.4.1 议题描述

组织通过开展宣传教育等活动,帮助用户(主要为消费者)在使用产品或服务的过程中,基于所得到的信息充分认识到数据安全和个人信息保护方面自身的权利、责任和义务,使其做出更有利于保护自身数据安全和个人信息和更加负责任的活动。

9.4.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面内容。

- a) 在产品或服务的显著页面、位置或步骤设置提升数据安全和个人信息保护方面用户进行自我保护的相关宣传活动。
- b) 在特定日期(如消费者保护日等)举办主题性和针对性强的宣传活动。
- c) 用户数据安全和个人信息保护教育和意识培养活动的内容包括:
 - 1) 数据安全和个人信息保护的适用法律法规、政策和制度等；
 - 2) 常用的投诉举报途径和消费者权益保护机构联系方式等；
 - 3) 数据安全和个人信息保护相关的知识和技能；
 - 4) 产品或服务相关的数据安全和个人信息保护功能；
 - 5) 与使用产品或服务有关的风险信息和所有必要的警示信息；
 - 6) 数据和个人信息泄露导致的风险和案例；
 - 7) 使用产品或服务过程中注重保护他人的数据和个人信息意识。
- d) 以提供奖励等方式鼓励用户积极参与教育和意识培养相关活动。

10 公益参与和社会发展

10.1 参与公益事业

10.1.1 议题描述

组织通过举办或参与公益活动,支持公共服务机构和社会团体等在数据安全和个人信息保护开展活动或扩大影响力,提升组织在数据安全和个人信息保护社会责任方面的绩效和社会认可度。

10.1.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面内容。

- a) 通过赞助或捐赠等方式,支持数据安全和个人信息保护相关公益事业。
- b) 调研运作良好的数据安全和个人信息保护的公益类项目和组织,根据组织拟定的社会责任战略和工作目标、自身业务的特点和参与人员的特长等确定参与公益活动的范围和工作计划,使得公益活动与组织核心业务和社会责任目标相一致,形成持续的社会影响力。
- c) 参与具体的公益活动,常见的有:

- 1) 筹建数据安全和个人信息保护研究机构、维权组织或科普中心等公益机构或向相关公益机构进行捐赠；
 - 2) 设立扶助基金或向相关基金捐赠，帮助弱势群体在数据安全和个人信息保护方面学习、深造和工作；
 - 3) 设立专门奖项或通过赞助方式，对全社会数据安全和个人信息保护优秀人才、团体和项目等进行奖励；
 - 4) 鼓励员工参加志愿者活动，帮助社会公众（尤其是缺乏自我保护意识的弱势群体）了解数据安全和个人信息保护知识和技能，提供公益法律援助和答疑咨询服务。
- d) 对于公益事业项目的效果进行评估，优化和调整工作的范围和方式等以提升社会责任履行效果。

10.2 科普宣传活动

10.2.1 议题描述

组织通过积极开展宣传科普活动，增强组织在数据安全或个人信息保护领域的透明性，提升行业和公众对相关前沿技术的了解，帮助公众提升数据安全和个人信息保护相关的知识和技能，扩大组织在社会层面的影响力和认可度。

10.2.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面内容。

- a) 为举办数据安全和个人信息保护相关的科普宣传活动提供必要的资源支持，包括人员、经费、场地、新闻媒体和传播渠道等。
- b) 自行组织或主动参与推动社会公众了解和掌握数据安全和个人信息保护知识和技能的科普活动，同时兼顾科普素材的趣味性和互动性，常见的活动有：
 - 1) 数据安全和个人信息保护主题的文章、漫画、海报和短视频等；
 - 2) 数据安全和个人信息保护相关的互动答题、游戏和体验等；
 - 3) 数据安全和个人信息保护相关的影视剧、专题片、专著和手册等发布物等。
- c) 通过邀请社会公众人物参与、与新闻媒体合作、与其他组织联动或在适当的时间段集中举办等方式扩大活动的影响面和宣传效果。

注：适当的时间段包括：国际、国家、地方或行业等层面发起的宣传活动举办期内，有关的纪念日和节假日等，如国家网络安全宣传周期间。

- d) 对于科普宣传活动的效果进行评估和总结，为后续活动的开展提供参考。

10.3 推动社会共治

10.3.1 议题描述

组织在数据安全和个人信息保护方面考虑产业生态和社会治理因素并开展相关工作，支撑有关部门和配合社会或行业组织开展社会共治活动，以推动防控科技伦理风险、增进用户素养和降低社会安全风险，提升社会层面重视数据安全或个人信息保护的氛围和治理水平。

10.3.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面：

- a) 参与有关主管监管部门、社会或行业组织等开展的数据安全和个人信息保护相关的法律法规政策宣贯和案例推广等活动；

- b) 积极加入包含数据安全和个人信息保护相关职责的社会或行业组织,参与其组织的各类活动;
- c) 从多角度出发与不同组织,如政府、企事业单位、高校和研究机构等,达成数据安全和个人信息保护社会共治相关的工作备忘录或合作协议等,以扩大工作的范围,提高工作的频率;
- d) 为有关主管监管部门、社会或行业组织等开展的数据安全和个人信息保护相关的法律法规政策宣贯、标准实践推广、安全事件应急响应、日常监督管理和打击违法犯罪等治理活动提供技术支撑和资源保障;

注:支撑有关主管监管部门、社会或行业组织活动期间,涉及受委托处理数据时,履行数据安全和个人信息保护义务。

- e) 通过构建技术平台和行业合作框架等方式促进信息共享和机制优化,为社会公众提供警示、预防或举报等防范数据安全和个人信息保护相关侵权行为的渠道或工具,以配合主管监管部门、社会或行业组织完善用户参与社会治理的机制;
- f) 组织为大型网络平台服务提供者时,可明确上述工作支撑部门或人员,并纳入到日常管理和考核中。

10.4 促进社会发展

10.4.1 议题描述

组织通过对数据安全和个人信息保护相关的产业链提供支持,包括人才培养、职业资格和上下游协同发展等,提升数据安全和个人信息保护方面的就业稳定性和创新积极性,促进数据在安全合规前提下流通利用,推动数据安全和个人信息保护相关产业快速发展。

10.4.2 相关行动和期望

组织宜采取的行动和达到的期望包括但不限于以下方面:

- a) 经济可行的前提下,选择最大程度创造就业机会的方式,设置数据安全和个人信息保护相关的工作岗位;
- b) 设立在职人才培养系统或运行人才培养计划,接纳学校或培训机构中数据安全和个人信息保护方向学生或学员的实习,如参与有偿合作项目,给予适当的劳动报酬;
- c) 关注数据安全和个人信息保护方面的优秀解决方案,并为其创造应用和实践的机会;
- d) 不影响服务质量的前提下,为新增的数据安全和个人信息保护方向的供应商,尤其是中小企业和初创企业供应商创造机会;
- e) 与高校或科研机构合作开展数据安全、个人信息保护和安全促进数据流通利用相关课题研究、项目申报和联合研发等活动;
- f) 关注数据安全和个人信息保护方向的中小企业和初创企业的发展,如满足投资条件,可向其提供资金方面的支持;
- g) 如组织具备一定能力、经验和资源等,可通过与政府、社会或行业组织等合作的方式,搭建产业孵化基地和创新实验平台等,吸引优秀人才创业发展;
- h) 积极参与数据流通交易基础设施和数据服务市场的投资和建设,研发数据安全和个人信息保护创新产品,丰富数据安全和个人信息保护专业服务供给,壮大数据安全和个人信息保护服务规模,繁荣数据安全和个人信息保护服务市场。

11 社会责任履行情况披露

11.1 披露原则

组织主动披露社会责任履行情况是组织接受社会监督的重要前提,同时也有助于增进用户对组织

保护数据安全和个人信息方面的了解,提升组织的形象和声誉。披露原则包括:

- a) 客观全面:披露信息准确、真实和具体,聚焦组织已实施的数据安全和个人信息保护社会责任相关活动,涉及绩效评价的无夸大成分;
- b) 易懂易得:披露信息尊重利益相关方语言习惯,易于利益相关方阅读和理解,采取多样化的披露形式便于利益相关方获取;
- c) 注重时效:披露信息反映社会责任履行的最新动态,披露信息发生变化时及时更新;
- d) 及时反馈:设置反馈渠道,及时回应外部组织或人员对披露信息内容的疑问。

11.2 披露内容

组织披露数据安全和个人信息保护社会责任履行情况时,披露信息宜关注以下内容:

- a) 披露信息包含社会责任履行整体说明,包括组织简介、总体履责情况和履责成效等;
- b) 披露信息包含社会责任履行具体情况,内容范围涵盖第 6 章~第 10 章中相关内容;
注 1: 与个人信息保护相关的社会责任相关的重点披露内容包括:个人信息保护组织架构和内部管理情况、个人信息保护能力建设情况、个人信息保护措施和成效、个人行使权利的受理情况、独立监督机构履职情况、重大个人信息安全事件处理情况、促进个人信息保护社会共治的科普宣传和公益活动情况等。
- c) 披露信息包含对组织数据安全和个人信息保护社会责任工作的反馈和建议渠道,如调研问卷、留言栏或反馈电子邮箱等;
- d) 根据组织开展业务、消费群体和利益相关方等特点,选择适当的语言种类、文本结构和披露方式以增加披露内容的可读性和传播效果;
注 2: 披露方式包括但不限于:详细版、简化版、海报版或视频版等。
- e) 必要时,可邀请第三方机构或外部专家等参与披露内容的编制和审核,以提升披露内容的完备性和权威性;
- f) 对披露信息进行审查,防止披露涉及国家秘密、商业秘密、具体个人信息或其他特殊原因不宜进行披露的信息。

11.3 披露方式

组织披露数据安全和个人信息保护社会责任的方式等宜考虑以下要素。

- a) 组织定期披露其数据安全和个人信息保护社会责任履行情况,大型网络平台服务提供者定期(如每年)发布数据安全和个人信息保护相关的社会责任报告(或包含数据安全和个人信息保护社会责任履行相关的白皮书等发布物)。数据安全和个人信息保护社会责任报告模板见附录 C。
- b) 组织采取用户、社会或行业组织以及监管部门等容易触达的渠道进行发布,具体可选择一种或多种,包括但不限于:印刷品、网站、APP 和新闻媒体渠道等;鼓励组织以电子版文件等形式披露,以促进低碳环保。
- c) 鼓励组织在路演活动、会议论坛、工作总结和投资者汇报等重要节点介绍其数据安全和个人信息保护社会责任履行情况,扩大相关工作的影响力以获得资源支持。
- d) 组织为上市公司时,积极响应证券监督管理部门和证券交易所对可持续发展报告提出的数据安全和个人信息保护相关议题,结合所处行业特点、行业发展阶段、自身商业模式和所处价值链等情况,将数据安全和个人信息保护社会责任履行情况纳入披露的可持续发展报告中。

附录 A

(资料性)

数据安全和个人信息保护社会责任绩效评价方法

A.1 评价指标和评价等级确定

通过指标评价方式,可促进组织确定数据安全和个人信息保护社会责任管理的优先事项,对社会责任绩效等级进行评价,有助于组织策划和实施提升数据安全和个人信息保护社会责任绩效的相关工作。

数据安全和个人信息保护社会责任评价指标和绩效评价等级见表 A.1。结合第 6 章~第 10 章内容,将社会责任评价指标设计为 5 项一级指标,一级指标下设 20 项二级指标。针对每项二级指标,分为四个评价等级(一星级、二星级、三星级和四星级),每项二级指标分值区间为 2 分~3 分,即:一星级:1 分~2 分,二星级:3 分~5 分,三星级:6 分~8 分,四星级:9 分~10 分(建议以 1 分为梯级评分),不符合指标描述事项不得分,根据指标描述事项的落实情况在分值区间中进行评价。根据每项二级指标得分情况,对组织数据安全和个人信息保护社会责任绩效等级进行综合评价,评价方法如下。

一星级(基础级):组织履行了相关法律法规中数据安全和个人信息保护社会责任的基本义务。所有二级指标总分大于或等于 20 分(总分换算为百分制)。

二星级(计划级):组织在达到一星级的基础上,将数据安全和个人信息保护社会责任相关工作纳入了年度工作计划,并进行了考核。其中 20 项指标(存在不适用指标时,从评价指标总数中扣除)中 70% 以上达标,即 70% 以上的二级指标项至少得 3 分。

三星级(系统级):组织在达到二星级的基础上,建立良好的数据安全和个人信息保护社会责任管理体系,推动持续开展数据安全和个人信息保护社会责任相关工作,并取得更高的社会责任绩效。其中 20 项指标(存在不适用指标时,从评价指标总数中扣除)中 70% 以上达标,即 70% 以上的二级指标项至少得 6 分。其中标星项[包括“★”和“☆(组织为大型网络平台服务提供者时)"]为必选指标(不适用的情况除外),且标星项至少得 6 分;

四星级(成熟级):组织在达到了三星级的基础上,持续改进数据安全和个人信息保护社会责任管理绩效,主动承担更多社会责任并推动行业进步,在多项指标上不断实现更高的社会责任绩效。其中 20 项指标(存在不适用指标时,从评价指标总数中扣除)70% 以上达标,即 70% 以上的二级指标项至少得 9 分。

数据安全和个人信息保护社会责任绩效总分的计算方式见公式(A.1)。

$$S = [\sum I_n / (N \times 10)] \times 100 \quad \dots\dots\dots (A.1)$$

式中:

S —— 社会责任绩效总分;

I_n —— 适用评价指标得分;

N —— 适用评价指标数量。

注:总分通过四舍五入方式取小数点后一位。

如因组织规模、业务领域或发展阶段等因素,20 项二级指标中适用指标数量不足 60%(12 个)时,考虑到评价本身的全面性和公正性等要素,不宜进行绩效评级。如存在不适用指标,则充分说明不适用的理由。

示例 1:如企业当前业务的服务对象不涉及个人用户的(业务领域原因),可认为二级指标中的“14 用户权利行使保障”为不适用。

示例 2:如企业没有以任何形式参与数据安全和个人信息保护活动或科普宣传工作(与组织规模、业务领域和发展阶段等无关),不宜认为二级指标中的“18 科普宣传活动”为不适用。

表 A.1 评价指标和评价等级

一级指标	二级指标	一星级(基础级)	二星级(计划级)	三星级(系统级)	四星级(成熟级)
一	1	★ ^a 发展理念和承诺声明 组织的发展理念符合法律法规和个人信息安全相关的理念	组织在成文的发展理念中强调了数据安全和个人信息保护的重要性及相关的价值观、愿景、使命或宗旨等。 组织的管理层在正式和公开的场合阐述过组织数据战略和个人信息保护的组织和理念	组织通过发布公告、制度文件或白皮书等形式对数据安全和个人信息保护做出管理层的承诺声明。 组织配置相应的资源,促使业务发展持续满足发展理念,推广其中数据安全和个人信息保护相关的愿景和目标,并通过内部培训场合同全体员工传达等	组织的发展理念包含了带动并引领与自身经营有实质性关联的领域在数据安全和个人信息保护方面工作的内容,并对同业伙伴、供应链上下游、被投资方和客户等产生了实际的积极影响。 组织设置对数据安全和个人信息信息保护社会责任发展理念和管理层承诺声明的跟踪机制,允许内部和外部人员对其进行评价和监督
	2	☆ ^b 工作实施和资源支持 组织在业务开展过程中,投入过人力和财务等资源践行部分数据安全和个人信息保护社会责任议题	组织制定的工作方针、目标和工作计划等包含了数据安全和个人信息保护社会责任相关主题和议题。 组织为数据安全和个人信息保护社会责任相关工作指定了负责人员并明确其职责。 组织为其履行数据安全和个人信息保护社会责任提供必要的人力和财务支持	组织将社会责任工作方针和目标等形成的纲领性文件和内部制度规范,通过向有关部门和人员下发或定期培训等方式,使其充分地沟通和理解,并在日常工作中得以贯彻执行。 组织指定了具体的高层管理人员担任数据安全和个人信息保护社会责任工作实施的负责人并明确其职责,提供了充足的预算支持,并配备了相应的责任部门或人员。 组织明确了定期向社会披露数据安全和个人信息保护社会责任履行情况的计划	组织持续改进社会责任工作方针和目标中有关数据安全和个人信息保护相关内容,并结合组织的发展更新社会责任事项。 组织建立了不断了解利益相关方在数据安全和个人信息保护社会责任的期望和诉求的机制;通过增加预算和人力等方式不断充实社会责任工作实施的力量;与利益相关方协同,合并多方资源,扩大社会责任工作的影响力和影响面

表 A.1 评价指标和评价等级(第 2 页/共 10 页)

一级指标	二级指标	一星级(基础级)	二星级(计划级)	三星级(系统级)	四星级(成熟级)
组织治理	3 制度宣贯和人员培训	组织的内部制度中有体现履行数据安全和个人信息社会责任的相关内容,在内部宣贯和培训工作中涉及了数据安全和个人信息保护相关的内容	组织在内部管理制度中明确了数据安全和个人信息保护社会责任的相关内容,并将制度文件下发至相应部门和人员。 组织定期开展数据安全和个人信息保护相关培训,其中包括了对开展数据安全和个人信息保护社会责任理念、制度、知识和案例等内容	组织内部每年至少一次开展数据安全和个人信息保护社会责任相关宣贯和培训工作。 组织设立相应系统或部门对实施数据安全和个人信息保护相关宣贯和培训的组织活动进行管理,不断提升宣贯的效果,扩大培训的专业度和覆盖面。 组织制定数据安全和个人信息保护相关员工培训计划,为员工参与外部专业培训并获取职业技能证书提供支持	组织建立了数据安全和个人信息保护社会责任知识和技能的培训和相关人员培养体系,并对该体系持续改进。 组织为同业伙伴、供应链、被投资方和客户等与自身经营有实质性关联的领域提供数据安全和个人信息保护法律法规、规章和标准等的宣贯,知识和技能培训的协助
	4 内部监督和员工激励	组织允许内部人员对数据安全和个人信息保护方面提出反馈意见并予以处理	组织建立了内部监督机制,包括相关的投诉或举报渠道,指定相应部门或人员接收内部人员反馈关于数据安全和个人信息保护社会责任方面的监督意见,并及时处理意见	组织将数据安全和个人信息保护社会责任履行情况纳入内部合规审计工作范围中。 组织建立了可考核的内部监督机制,明确监督意见的处理部门和流程措施。 组织通过绩效考核等方式推动员工积极履行数据安全和个人信息保护社会责任和义务	组织持续优化和改进内部监督机制,以提高监督机制的效率和效果。 组织持续优化和改进员工激励机制,对取得积极社会反响的社会责任相关活动予以奖励,充分调动员工在数据安全和个人信息保护方面的积极性

表 A.1 评价指标和评价等级(第 3 页/共 10 页)

一级指标	二级指标	一星级(基础级)	二星级(计划级)	三星级(系统级)	四星级(成熟级)
二	5 ★ 产品或服务 的合规性	组织有数据安全和 个人信息保护方面的法 律法规、规章和强制性标 准等的知识和人员储 备,并按照其开展业务 活动	组织已通过对其产品或服务在数据安全和个人信息保护方面的合规性进行评估,并接受持续监督。 组织定期发布数据安全和个人信息保护合规相关的白皮书等发布物,向外界披露数据安全和个人信息保护合规方面的履责情况。 组织建立了产品或服务合规性的监督机制,采取发布前审核、不定期抽检和定期内审等手段,督促产品或服务持续保持合规性	组织引入了第三方机构进行评估,已取得产品服务在数据安全和个人信息保护方面的合规认证,并接受持续监督。 组织定期发布数据安全和个人信息保护合规相关的白皮书等发布物,向外界披露数据安全和个人信息保护合规方面的履责情况。 组织建立了产品或服务合规性的监督机制,采取发布前审核、不定期抽检和定期内审等手段,督促产品或服务持续保持合规性	组织为率先取得数据安全和个人信息保护相关合规认证(国内和国际)提供人力、财务和环境等资源保障。 组织建立了数据安全和个人信息保护合规风险管理体系,基于法律法规、规章、标准和外部环境等的变化对合规实施动态管理,及时发现、预警和处置合规风险,不断提升合规能力水平。 组织主动参与同行业针对产品或服务合规性相关的建设和合作,为同业伙伴、供应链、被投资方和客户的网络安全和个人信息保护合规能力提供帮助
	6 技术的创新性和先进性	组织在数据安全和 个人信息保护方面所使 用的技术有一定的创新 性和先进性。 组织积极参加同行 业内关于数据安全和个 人信息保护创新性和先 进性技术的研讨和交流	组织定期通过同行业交流机制或交流平台,分享数据安全和个人信息保护创新理念和 方法,以参赛和参与试点等方式扩大了影响力和应用面。 组织的产品或服务使用的 数据安全和个人信息保护技术的 创新性和先进性以获得专利、 专业机构认证、成为优秀案例或 获得奖项等方式得到认可	组织已构建并积极实施数据安全和个人信息保护创新性和先进性评价标准和指导方针,已建立技术创新的长期激励机制。 组织参与或承担过省部级数据安全和个人信息保护科研项目。 组织参与数据安全和个人信息保护相关技术的创新性和先进性的评比和奖项申报等活动,并取得了优异的成绩,如省部级科技奖项等	组织搭建了同行业交流机制或交流平台,为技术创新提供学术研究和国际交流等方面的有利条件。 组织参与或承担过国家级数据安全和 个人信息保护科研项目。 组织在数据安全和个人信息保护技术的 创新方面有突出成就,获得了国家级科 学技术奖项或发表的论文取得国际范围 的广泛认可或开源成果被同业高度赞赏并 广泛应用等。 组织已具有自主知识产权或在创新性 和先进性上有显著优势的技术,已创立行 业知名的品牌,在提升行业整体水平和 提高产业国际竞争力上有显著贡献

表 A.1 评价指标和评价等级(第 4 页/共 10 页)

一级指标	二级指标	一星级(基础级)	二星级(计划级)	三星级(系统级)	四星级(成熟级)
合规性、创新性和价值体现	7 产品或服务的使用价值	组织的产品或服务仅处理实现功能所必要的数据。 组织的产品或服务将数据安全和个人信息保护相关功能设置为基础功能的一部分	组织的产品或服务提供的功能主动引导用户加强数据安全和个人信息保护。 组织的产品或服务为数据安全和个人信息保护相关的治理活动提供支撑	组织的产品或服务所提供的功能引导大范围用户强化了数据安全和个人信息保护设置。 组织通过不断优化数据处理的流程和步骤,以优化产品或服务收集数据时机和场景,减少收集数据的种类和存储时间,在不影响使用的前提下不断拓宽数据脱敏、去标识化和匿名化处理技术的应用面。 组织的产品或服务支撑了有关主管部门、社会或行业组织等开展的数据安全和个人信息保护相关的治理等活动	组织在不影响用户权益的前提下,通过使用算法或模型处理数据和个人信息,进行自动化决策等方式挖掘数据价值。 组织积极采取措施引导、推动同业伙伴、供应链、被投资方和客户等与自身经营有实质性关联的领域形成注重产品或服务使用价值的良好生态。 组织的产品或服务在有关主管部门、社会或行业组织等开展的数据安全和个人信息保护相关的治理活动中发挥了关键作用,使治理工作取得显著成效
	8 数字包容和特殊保护	组织有为多元化群体提供平等的数字产品或服务的案例。 组织的产品或服务在面向身体机能差异人群个人信息保护方面采取了相关措施	组织重视并保护多元化群体的数据和个人信息,为多元化群体提供符合其应用场景的数据安全和个人信息保护机制,如监护人同意或辅助操作等。 组织为身体机能差异人群提供的服务页面和服务渠道,使其能感知和获取个人信息保护方面的信息	组织收集身体机能差异人群的个人信 息前,充分评估了处理个人信 息对其权益的影响,采取了更为 严格的安全保护措施降低安全 风险。 组织的产品或服务对身体机能 差异人群个人信息保护采取优先和 默认保护的策略,限定个人信息的 使用范围并提供便捷的行使权利 渠道。 组织投入资源主动推广身体机 能差异人群使用的产品或服务(或 相关功能模式),并开展公益宣传活 动为其科普数据安全和个人信息保 护知识,引导身体机能差异人群关 注使用产品或服务时保护自身个 人信 息	组织参与了身体机能差异人群数据安 全和个人信息保护相关标准制定,加入相 关倡议或计划等活动,以促进行业协同。 组织对数字包容和特殊保护方面的涉 及数据安全和个人信息保护的能 力和技 术资源进行开放,为行业提供参考和支撑

表 A.1 评价指标和评价等级(第 5 页/共 10 页)

一级指标	二级指标	一星级(基础级)	二星级(计划级)	三星级(系统级)	四星级(成熟级)
公平运行、竞争和合作	★ 9 数据处理规则的透明性	组织依据法律法规、规章和标准等,完整、真实和准确地披露了数据处理的目的、方式和范围	组织建立和实施了数据治理规则披露的管理制度,提供与利益相关方问询或答疑等的渠道,便于沟通协商	组织建立了完备的数据处理规则披露机制,并对数据处理规则进行影响评估,针对可能影响到利益相关方重大权益的数据处理规则,采取多种方式进行重点说明,以增加利益相关方的理解。 组织数据治理规则影响范围广泛的(如大型网络平台服务提供者的产品或服务的隐私政策),通过向外部监督机构、第三方机构或业界专家征求意见等方式完善了规则内容	组织建立了与利益相关方对数据处理规则进行事前沟通协商的机制,其数据处理规则则在同业伙伴、供应链、被投资方和客户等与自身经营有实质性关联的领域产生积极影响,并推动多方数据治理规则同步更新,适应生态健康发展的需要
	10 公平竞争和成果保护	组织在数据处理相关的生产经营活动和参与市场竞争中,按自愿、平等、公平和诚信的原则,将公平竞争作为组织治理、生产经营和商业活动的行为准则。 组织尊重和承认数据安全和个人信息保护相关财产权益	组织建立了反不正当竞争的、反腐败和保护知识产权相关的、反腐败和保护知识产权的内部管理制度。 组织建立了成果保护的管理制度,对数据安全和个人信息保护相关成果实施了保护,或使用相关成果支付了合理费用	组织建立了完善的识别、监控、防止和报告不正当竞争的管理制度,并根据经营所在地法律法规和政策的变动及时更新相应的管理制度。 组织采取了严格的反腐败内部管理制度并定期落实具体举措,对情节严重的汇报至有关部门。 组织定期开展和参与公平竞争和成果保护的相关培训和活动	组织在同业伙伴、供应链、被投资方和客户等与自身经营有实质性关联的领域积极影响或合作,协助有关部门开展反不正当竞争和知识产权保护的行动调查和执法行动,在维护行业领域公平竞争中发挥显著作用。 组织在行使并保护自身的数据安全和个人信息保护知识产权等相关权利时,充分考虑社会期望和行业需求,选择适当的形式(如技术开源等)推动知识和技术成果在更大范围共享

表 A.1 评价指标和评价等级(第 6 页/共 10 页)

一级指标	二级指标	一星级(基础级)	二星级(计划级)	三星级(系统级)	四星级(成熟级)
公平运行、竞争和合作	☆ 平台规则和供应链管理	组织以合同或协议等方式与平台参与方和供应商约定数据安全和个人信息保护相关责任和义务	组织制定可促进数据安全和个人信息保护的运营规则和供应链管理制度。 组织明确供应商遵守的数据安全和个人信息安全基线淘汰指标并予以筛选	组织严格实施可促进数据安全和个人信息保护的运营规则,并建立和实施平台规则执行效果评估管理制度,将平台规则执行效果评估纳入审计等监督环节,以推动平台规则切实有效执行。 组织基于自身技术和人员等资源优势,为供应商提供必要的技术支持和应急协助	组织定期开展平台规则整体执行效果评估,并根据评估结果对平台规则进行优化,并将平台规则执行效果进行公开,接受利益相关方的监督和评议。 组织注重与供应商的长期合作与共赢,并为中小企业供应商提供机会,协助供应商提升数据安全和个人信息保护水平
	11 行业共治和知识共享	组织参与或支持过能推动数据安全和个人信息保护产业发展和技术创新等方面的各类活动	组织定期与相关领域内的组织,就数据安全和个人信息保护相关的前沿技术进行交流合作。 组织通过发布白皮书或发表专业文章等形式将数据安全和个人信息保护相关知识予以共享。 组织参与了数据安全和个人信息保护相关标准的研制和试点验证等工作	组织以主办方或承办方的身份开展过数据安全和个人信息保护产业发展和技术创新等方面的活动。 组织通过联合开发课程、撰写科研论文、发布专刊或专著等形式将数据安全和个人信息保护相关知识予以共享。 组织积极响应社会或行业组织发起的自律活动,如加入数据安全和个人信息保护相关的自律倡议书、工作计划或国际协定等	组织作为负责单位参与国家、行业数据安全和个人信息保护相关标准的研制和试点推广工作。 组织通过开源代码或威胁情报分享等形式将数据安全和个人信息保护相关知识予以共享。 组织开展了数据安全和个人信息保护先进技术的推广及应用并取得显著成效。 组织主动发起数据安全和个人信息保护相关的自律活动,并在国际和国内取得良好反响
12					

表 A.1 评价指标和评价等级(第 7 页/共 10 页)

一级指标	二级指标	一星级(基础级)	二星级(计划级)	三星级(系统级)	四星级(成熟级)
四 用 户 权 益 保 护	★ 13 人身财产 利益保护	组织在提供产品或服务过程中采取了降低用户人身和财产损害的措施	组织在使用户使用产品或服务前,采用生动、简明和准确的表述方式,指导用户安全正确使用产品或服务,并说明与使用有关的风险和预防措施,告知用户遭受或可能遭受人身和财产损害时的反馈渠道和处置方式	组织在处理与人身和财产安全密切相关的数据和个人信息前,系统性对处理活动进行风险和风险评估,并采取了与风险相适应的保护措施。 组织建立了用户权益保护的技术保障能力和具体工作机制,如识别用户风险行为的特征库、紧急告知和阻断机制以及快速反馈渠道等。同时,没有证据表明目前采取的数据安全和个人信息保护解决方案还有显著提升的空间	组织建立了行业共享和动态可更新的侵害用户权益的违法违规行为特征库,并持续监测和防范违法违规行为。 组织用户人身和财产保护方面的经验和机制得到广泛认可并通过形成标准或能力共享等方式,引导利益相关方共同强化用户人身和财产保护措施,为同业伙伴、供应链、被投资方和客户等与自身经营有实质性关联的领域提供相关的指导和帮助
	★ 14 用户权利行使保障	组织建立了有效的用户数据安全和个人信息保护相关权利行使投诉和争议处置机制,以清晰和显著的方式披露投诉渠道、处理方式和反馈时限	组织建立并提供了一定比例人工客服支持的投诉反馈渠道,并在法律法规、规章和标准规定的时间内对用户数据安全和个人信息保护相关权利行使相关投诉进行响应。 组织建立了投诉分级处理制度,优先处理影响严重或影响面大的侵犯用户数据安全或者个人信息保护的投诉内容	组织对多次投诉未果或特殊投诉等复杂情形设立相关负责人受理的机制。 组织建立了投诉处理满意度反馈途径,便于用户通过该途径反馈意见或建议。 组织定期公开用户权利行使和投诉汇总情况,如在社会责任报告和公开发布的文件中予以体现	组织建立了投诉处理数据库,记录投诉处理的时间、原因和处理情况等,并通过定期评估投诉和举报的数量、处理率和处理评价情况等,不断完善投诉处理机制。 组织主动关注合作方和供应商用户满意度相关情况,针对影响较大的投诉问题进行追踪并提供协助,并作为下步调整合作的重要考虑要素



表 A.1 评价指标和评价等级(第 8 页/共 10 页)

一级指标	二级指标	一星级(基础级)	二星级(计划级)	三星级(系统级)	四星级(成熟级)
四 用 户 权 益 保 护	☆ 15 主动接受外部监督	组织向社会公开了联系用户对产品或服务数据安全和个人信息保护方面的外部监督	组织向社会披露数据安全和个人信息保护相关策略和规则,以及数据安全和个人信息保护社会责任履行情况,主动接受社会监督。 组织在获得数据安全和个人信息保护的认证后,持续接受专业机构监督,且无因合规问题导致认证被撤销的情况	组织指定特定人员承担与外部组织或个人沟通对接的职责。 组织通过定期发布数据安全和个人信息保护社会责任报告等形式,披露数据安全和个人信息保护社会责任履行情况。 组织为大型网络平台时,成立主要由外部成员组成的独立监督机构,对其个人信息处理活动进行监督,并将监督机构履责情况在社会责任报告中披露	组织面向社会征集数据安全和个人信息保护改进问题和工作建议,并为贡献者提供奖励。 组织建立了利益相关方和投资者沟通机制,对于其在数据安全和个人信息保护方面提出的意见和建议予以反馈。 组织向监督机构赋予对组织在数据安全和个人信息信息保护进行核实和质疑的权利,通过向独立监督机构如实提供数据安全和个人信息保护的相关管理和技术措施等方式接受其监督,如果质疑得到证实及时予以纠正
	16 自我保护素养提升	组织开展或参与过用户数据安全和个人信息保护素养提升方面宣传培训活动	组织明确了用户数据安全和个人信息信息保护素养提升的目标和计划,通过自运营的产品或服务中设置页面等形式开展了相关宣传活动	组织定期开展用户数据安全和个人信息信息保护素养提升相关活动,并通过提供奖励或社群激励等方式鼓励用户积极参与相关活动	组织构建了用户数据安全和个人信息信息保护素养提升体系,对该体系进行定期评审和改善。 组织联合同业伙伴、社会或行业组织等,共同开展用户数据安全和个人信息信息保护素养提升相关活动,以推动行业和领域整体形成合力

表 A.1 评价指标和评价等级(第 9 页/共 10 页)

一级指标	二级指标	一星级(基础级)	二星级(计划级)	三星级(系统级)	四星级(成熟级)
公益参与和社会发展	17 参与公益事业	组织参与或举办过数据安全和个人信息保护相关公益活动	组织在年度工作目标和财务预算中列明参与数据安全和个人信息保护公益事业项目的计划。 组织举办或参与的相关公益活动发挥了实质性作用,受到各方认可	组织将数据安全和个人信息信息保护相关的公益事业作为组织长期文化建设和战略规划予以明确。 组织定期组织员工参加面向社会公众科普、援助和答疑等志愿者活动。 组织对社会面的数据安全和个人信息信息保护相关优秀人才、团体、项目设立奖项或对奖项进行赞助	组织定期向数据安全和个人信息信息研究的研究机构、维权组织和科普中心等公益机构进行捐赠。 组织设立扶助基金或通过捐赠,帮助弱势群体在数据安全和个人信息信息保护方面学习、深造和工作等。 组织对公益事业项目的效果进行了评估,优化和调整工作的范围和方式等以提升社会责任履行效果
	18 科普宣传活动	组织参与或支持过数据安全和个人信息保护相关科普活动	组织以主办方或承办方的身份开展过数据安全和个人信息保护相关科普活动	组织将定期举办数据安全和个人信息信息保护相关的宣传和科普活动纳入日常工作计划。 组织通过在适当的时间段举办活动、举办系列活动、与政府部门、社会或行业组织以及其他组织联动等方式,提升了数据安全和个人信息信息保护相关的宣传和科普活动的效果	组织通过邀请社会公众人物参与或与新闻媒体合作等方式显著扩大了数据安全和个人信息保护科普宣传活动的影响面和宣传效果,得到了社会的关注和肯定。 组织对数据安全和个人信息信息保护相关的宣传和科普活动进行总结并对活动效果进行评估,不断优化活动的举办形式,扩大活动影响范围

表 A.1 评价指标和评价等级(第 10 页/共 10 页)

一级指标	二级指标	一星级(基础级)	二星级(计划级)	三星级(系统级)	四星级(成熟级)
公益参与和社会发展	推动社会共治	19	组织参与了包含数据安全和个人信息保护相关职责的社会的各类活动。 组织作为承办方协助过相关社会或行业组织开展数据安全和个人信息保护相关工作或活动	组织为有关主管部门、社会或行业组织开展的安全事件应急响应、日常监督管理和打击违法犯罪等治理活动提供过技术支持或资源保障。 组织从多角度出发与不同组织,达成数据安全和个人信息保护社会共治相关的工作备忘录或合作协议等,以扩大工作的范围,提高工作的频率。 组织为大型网络平台时,明确参与标准和参与社会共治活动等管理考核中	组织通过构建技术平台和行业合作框架等方式促进信息共享和机制优化,为社会公众提供警示、预防或举报等防范数据安全和个人信息保护相关侵权行为的渠道或工具。 组织在社会或行业组织中担任相关负责人角色,引导行业伙伴参与社会共治,共同维护数据安全和个人信息保护良好生态环境
			组织自身设置完善的数据安全和个人信息保护相关工作岗位,并为数据安全和个人信息保护相关学生或学员提供实习机会。 组织为数据安全和个人信息保护提供信息保护产品和服务供应用和实践的机会。 组织为数据安全和个人信息保护提供了数据安全和个人信息保护新产品和专业服务	组织持续提供数据安全和个人信息保护相关工作岗位。 组织建立和运行数据安全和个人信息保护相关的人才培养计划或培训系统。 组织为数据安全和个人信息保护方向的供应商,尤其是中小企业和初创企业供应商创造产品和服务应用和实现的机会。 组织参与了数据流通交易基础设施和数据服务市场的投资和建设,通过创新产品和服务壮大了数据安全和个人信息保护服务规模	组织的数据安全和个人信息保护相关岗位需求和人才培养机制呈现规模化特点。 组织积极为数据安全和个人信息保护方面具备优秀能力或潜力的人才与企业提供创业机遇、投资和合作机会,与政府、社会或行业组织等共同推进产业创新发展。 组织主导了数据流通交易基础设施和数据服务市场建设中的数据安全和个人信息保护相关工作,带动同领域其他组织共同繁荣数据安全和个人信息保护服务市场
	促进社会发展	20	组织在力所能及的情况下,设置数据安全和个人信息信息保护相关的工作岗位		
		<div>★ 三星级评价必选指标。</div> <div>☆ 组织为大型网络平台服务提供者时,三星级评价必选指标。</div>			

A.2 重点关注事项

本文件将数据安全和个人信息保护社会责任主题和议题中可能存在较高风险的事项确定为重点关注事项,见表 A.2。

如组织在重点关注事项中出现疑似行为或不道德事件,例如被新闻媒体或其他公开渠道曝光或被用户举报等,则在原本所拥有评级的基础上降低一个等级,如原等级为一星级,则撤销评级结论,并停止评价活动。

注 1: 经证明或确认疑似行为不存在或事件情况不属实,如未对利益相关方和用户权益产生实质性影响,可恢复原有评价等级。

如组织在重点关注事项中出现严重违法事件,例如受到主管监管部门行政处罚,造成恶劣社会影响,则撤销评级结论,并停止评价活动。一年内不再对该组织进行评价。

注 2: 如评价活动发起方认定为需停止评价活动,注明原因并对其事实与被评价组织进行核实确认。

表 A.2 重点关注事项

序号	相关主题	重点关注事项
1	合规性、创新性和价值体现	a) 产品或服务数据安全和个人信息保护方面不合规被监管部门通报或处罚; b) 发生网络安全事件导致数据泄露、篡改或毁损等
2	公平运行、竞争和合作	a) 侵犯数据安全和个人信息保护相关知识产权行为; b) 发生数据安全和个人信息保护相关不正当竞争行为; c) 存在腐败、贿赂或其他违法违规行为
3	用户权益保护	a) 损害用户个人信息权益; b) 泄露或滥用用户个人信息
4	公益参与和社会发展	妨碍社区的安全与稳定(如公共安全、网络安全或数据安全等方面)

A.3 社会责任最佳实践评价方法

“社会责任最佳实践”评价不同于 A.1 的社会责任绩效评价,不是对组织社会责任绩效等级的综合评价,而是在某个或某些指标上的专项评价。比如,无论组织是否达到 A.1 的绩效等级,只要表 A.1 的部分二级指标达到四星级,或一级指标中的一定比例二级指标均达到三星级或四星级,则可将指标对应的工作内容评价为最佳实践。“社会责任最佳实践”评价避免了中小企业在绩效评价环节不适用项过多或社会责任履行范围不广等不利因素,有助于鼓励中小型企业更好履行数据安全和个人信息保护社会责任。

“社会责任最佳实践”的具体评价依据和评价方法可根据评价需求设定。以下给出了某社会或行业组织进行“个人信息保护社会责任履行优秀案例”评价的方案示例,供参考。



示例：

<div><p style="text-align: center;">个人信息保护社会责任履行优秀案例评价方案</p><p>（一）评价依据</p><p>依据《中华人民共和国个人信息保护法》等法律法规要求,参考 GB/T 46071—2025《数据安全技术 数据安全和个人信息保护社会责任指南》开展“个人信息保护社会责任履行优秀案例”评价。</p><p>（二）评价方式</p><p>报名参与“个人信息保护社会责任履行优秀案例”评价的组织,根据评价工作小组提供的文件模板提交参评材料,由评价工作小组通过材料审查和专家评审组评审的方式进行评价。</p><p>（三）评价流程</p><ol style="list-style-type: none">1) 材料上报:××月××日前,组织根据报名要求,提交报名表和参评材料,以及评价所需的佐证材料,包括但不限于组织介绍材料、合规性证明、创新实践案例、用户反馈和社会责任报告等。2) 初步审查:评价工作小组对收集的材料进行初步审查,确认是否符合评价基本条件。3) 工作组评价:评价工作小组对收集的材料进行详细审查,组织提供的实践案例表示,涉及 GB/T 46071—2025《数据安全技术 数据安全和个人信息保护社会责任指南》20 个议题中,至少 1 个议题评价为四星级,或同一主题下至少 2 个议题评价为三星级,认为通过工作组优秀案例评价。4) 专家评审:组织行业专家组成“个人信息保护社会责任履行优秀案例”专家评审组(专家组成员不少于 10 人),对工作组评价后选择送的优秀案例进行专家评审,评审认为案例具有代表性、先进性和创新性,如专家投票同意的比例不低于 70%,进入优秀案例最终名单。5) 结果公示:××月××日前,对优秀案例最终名单进行公示。<p>（四）注意事项</p><p>组织在近一年内(××××年××月后),如存在 GB/T 46071—2025 中表 A.2 的重点关注事项,本次评价活动不予受理。评价期间,组织出现上述重点关注事项时,将立即停止评价活动,一年内不再对该组织进行评价。</p></div>

附 录 B

(资料性)

数据安全和个人信息保护社会责任实践案例

根据第 6 章～第 10 章内容,组织履行数据安全和个人信息保护社会责任主题和议题常见实践案例如表 B.1 所示。

表 B.1 社会责任履行实践案例

章	相关行动和期望	实践案例
6 组织治理	6.1 发展理念和承诺声明	<p>案例 1: 某公司在对内的公开信中提出公司的数据隐私保护理念、原则和核心要求。</p> <p>案例 2: 某公司在其公开发布的宣传册和官网主页面等渠道以显著方式披露其隐私保护的核心理念。</p> <p>案例 3: 某公司在社会责任报告的董事长致辞中阐明管理层对数据安全和个人信息保护社会责任的承诺或要求。</p> <p>案例 4: 在某一次行业生态大会上,某公司的首席执行官在主题演讲时专门对公司在个人信息保护方面的理念进行阐述</p>
	6.2 工作实施和资源支持	<p>案例 1: 某上市公司在制定的纲领性文件中,用专门的章条阐述了数据安全和个人信息保护的总体方针和安全策略。</p> <p>案例 2: 某科研机构参考有关部门发布的五年规划文件,制定了内部的五年规划,其中对数据安全相关的社会责任目标予以明确。</p> <p>案例 3: 某大型互联网公司建立了隐私保护委员会,负责决策公司数据管理重要事项,并由公司常务副总裁担任首席隐私官。</p> <p>案例 4: 某公司从现有的法务和安全团队中,指定 2 人从事数据安全和个人信息保护社会责任履行的工作内容,其中包括由其主笔撰写本年度社会责任报告。</p> <p>案例 5: 某公司在制定年度预算时,规划 100 万专门用于履行数据安全和个人信息保护社会责任的财务预算,其中 30 万将用于个人信息保护科普宣传的相关活动</p>
	6.3 制度宣贯和人员培训	<p>案例 1: 某公司根据数据安全相关法律法规要求,根据各业务线和职能部门分工不同,修订公司现有制度,明确各部门的数据安全具体职责和社会责任目标,并在全公司范围内集中宣贯。</p> <p>案例 2: 某互联网公司每年定期举办隐私保护安全月活动,活动包括了对法律法规的学习和合规实践的宣贯等,同时提供网络课程,全体员工学习时间不少于 2 个学时,部分重点岗位学习时间不少于 8 个学时,并通过统一的考试</p>
	6.4 内部监督和员工激励	<p>案例 1: 某公司制定发布了《数据安全管理制度》,制度中要求,一旦发生数据安全违规事件,会在公司内部进行全员电子邮件通报并对违背安全策略和规定的员工做出相应处罚,构成犯罪的,将向公安部门报案,依法追究刑事责任。</p> <p>案例 2: 某互联网公司针对不同的业务线,根据用户举报情况,定期公布数据安全和个人信息保护红黑榜,并将其与绩效考核挂钩</p>

表 B.1 社会责任履行实践案例（续）

章	相关行动和期望	实践案例
7 合规性、创新性和价值体现	7.1 产品或服务的合规性	<p>案例 1: 某互联网公司通过专业机构对公司业务开展了技术合规性评估,并在网站或 APP 中的显著页面向用户披露了本公司在数据安全和个人隐私保护方面的合规资质或证明。</p> <p>案例 2: 某互联网公司组建了数据安全和个人信息保护专职团队,每年依据国家标准对公司给用户提供的服务进行了合规性内审和自评估。对于存在差距的标准条款,在 3 个月内进行整改,并形成了整改报告。</p> <p>案例 3: 某数据安全公司按照法律法规、国家标准或行业标准等要求开发了数据安全风险监测的产品,客户根据使用产品的情况形成了应用报告,对产品能否满足合规性要求给出建议</p>
	7.2 技术的创新性和先进性	<p>案例 1: 某科研院所参与数据安全、个人信息保护相关的法律法规、政策文件的制定和研讨,提出了鼓励技术创新相关的多条建议,其中 5 条被采纳。</p> <p>案例 2: 某初创数据安全公司参与了由某行业组织举办的技术创新评比活动,该数据安全公司通过分享其产品和解决方案在数据安全方面的创新举措,获得评审委员会肯定,获得了某投资公司的青睐。</p> <p>案例 3: 某事业单位申报工业互联网数据安全课题,把本单位在工业互联网领域的创新实践应用到课题中,获得了省级创新大赛的奖项。</p> <p>案例 4: 某高校实验室对个人信息保护成立了科研小组,对相关技术开展研究,形成了 2 篇兼具可行性、创新性和先进性的核心期刊论文,获得了 1 项发明专利</p>
	7.3 产品或服务的使用价值	<p>案例 1: 某互联网平台通过 APP 为用户提供订餐服务,用户通过 APP 进行订餐时,APP 提供了收集个人喜好提供精准推荐的功能,用户拒绝该功能,APP 可继续提供基本的订餐服务。</p> <p>案例 2: 某互联网平台通过 APP 向小学生提供教学服务,但小学生的监护人发现一些教学功能显示小学生的完整联系方式。监护人在向互联网平台反馈后,该平台采取屏蔽部分字段方式优化了显示的内容,并在 3 天内完成 APP 升级。</p> <p>案例 3: 某数据安全公司的检查工具被某监管机构用于对辖区内的 10 家互联网公司开展数据安全检查,经工具扫描发现,有 5 家互联网公司存在数据泄露的风险,工具输出了相关的检查报告,并由数据安全公司的咨询专家给出了加固意见</p>
	7.4 数字包容和特殊保护	<p>案例 1: 某 APP 在收集个人信息时,提供了一键按钮,转换到长辈模式,在长辈模式下,文字字体更大,同时把需要特别注意的文字加粗,帮助高龄老人快速地了解收集个人信息的用途和范围。</p> <p>案例 2: 某 APP 在收集个人信息时,对个人信息处理的说明文字,提供了汉语、英语和法语等共 10 种语言文字说明,并且还提供了语音播放功能,帮助视觉障碍的用户通过声音获得信息。</p> <p>案例 3: 某用于网络教学的智能终端提供了家长守护的功能,家长可通过设置口令等方式将下载第三方 APP 的通道锁定,防止未成年人安装与学习无关的游戏和娱乐 APP</p>

表 B.1 社会责任履行实践案例（续）

章	相关行动和期望	实践案例
8 公平运行、竞争和合作	8.1 数据处理规则的透明性	<p>案例 1: 某社交软件公司,通过系统梳理业务所涉及的个人信息处理情况,在网站、APP 和小程序中用户便于查看的页面,详细披露了“个人信息收集清单”“第三方信息共享清单”“算法模型的运行原理”等处理规则。</p> <p>案例 2: 某科技公司,就向客户提供的信息技术服务中涉及的信息核验、差错处理、账单处理所收集数据的目的、种类、存储时间、销毁机制等,通过合同条款进行了明确约定</p>
	8.2 公平竞争和成果保护	<p>案例 1: 某研究机构,将数据安全和个人信息保护相关学术论文、学位论文、著作、专利、教材和讲义等内容建设成数字知识库,面向社会开放共享。</p> <p>案例 2: 某地方大数据产业园,对园区内开放自身数据,实现数据应用合作的企业,提供算力支持、市场资源支持和政府部门的专业指导,对所有入驻的企业和员工在数据安全、数据应用和数据技术等方面提供“终身免费公平竞争培训”。</p> <p>案例 3: 某投资公司,对投资企业和其高层管理人员,定期开展头脑风暴和反垄断培训,并聘请业界专家和律师等组成委员会,就数据的跨领域应用可行性、安全性和是否涉及垄断风险出具调研报告</p>
	8.3 平台规则和供应商管理	<p>案例 1: 某地方政府惠民服务平台,针对餐饮、教培和美容等行业中市民关心的个人信息保护问题,免费提供个人信息保护自查功能等。</p> <p>案例 2: 某银行,对供应商中涉及违规出售客户数据等行为,一经确认,马上除名且永不录用,并在银行官网公示。</p> <p>案例 3: 某集团性公司,由科技部门牵头,利用数据源审核、隐私计算等技术和措施打造“新数据中台”进行供应商的对接,并在供应商招标和管理考核中,加大数据安全和技术创新等指标的权重。</p> <p>案例 4: 某证券公司举办年度服务商峰会,评选优秀服务商的过程中将数据安全作为重要评分项,并邀请服务商分享案例经验,结合新年度的目标规划与服务商共议加强数据安全和个人信息保护的措施</p>
	8.4 行业共治和知识共享	<p>案例 1: 在某行业组织指导下,加入了个人信息保护相关的自律倡议书,并公布了相关工作计划。</p> <p>案例 2: 某文化创意设计产业博览会,将诸多知名艺术家和自由创作者的优秀作品,利用区块链等技术构建安全和可信的数字艺术品平台。</p> <p>案例 3: 某公司发布了年度个人信息保护白皮书,向业界披露其个人信息保护方面的优秀实践案例</p>



表 B.1 社会责任履行实践案例（续）

章	相关行动和期望	实践案例
9 用户权益保护	9.1 人身财产利益保护	<p>案例 1：设立“叫醒热线”，当识别到消费者财产利益等存在风险时，通过电话、发提醒和网络问答等形式提醒消费者。</p> <p>案例 2：在 APP 等客户端设立“消费者权益保护”频道，用户可查看和管理“服务协议”“隐私设置”“新消息通知”“免密支付/自动扣款”“服务管理”等，方便消费者一站式配置和获取与其权益相关的功能或服务。</p> <p>案例 3：在 APP 等客户端设立“一键报警按钮”，当消费者意识到人身或财产存在威胁时，可通过一键报警按钮与警方联系并通知紧急联系人</p>
	9.2 用户权利行使保障	<p>案例 1：某支付类 APP 实现 7×24 h 连续在线客服，承诺 3 min 内响应消费者咨询。对消费者投诉 48 h 内响应。</p> <p>案例 2：在 APP 等客户端设置“我的客服”频道，频道中对常见问题进行分类并答复，如隐私安全、账号安全和人工渠道等，方便消费者快速定位和解决问题。</p> <p>案例 3：配备充足的人工客服团队，人工客服热线接通率不低于 95%。细化人工客服分类并开展专项培训，如道具使用反馈组、隐私保护反馈组和账号安全反馈组等，使人工客服能准确和迅速地帮助消费者解决问题。</p> <p>案例 4：通过设置匿名投诉和个人信息脱敏显示等功能，保护投诉者的隐私，避免侵扰投诉者私人生活的安宁</p>
	9.3 主动接受外部监督	<p>案例 1：在 APP 等客户端设置“规则中心”，集中和统一披露平台规则情况、规则更新情况和规则解读等，便于外部机构或人员查阅和监督。</p> <p>案例 2：在 APP 等客户端设置“众裁厅”频道，邀请平台用户参与反馈纠纷处理和规则修改等方面的意见，根据用户的投票反馈结果进行处置。</p> <p>案例 3：某社交平台定期公示组织在提升数据安全和个人信息保护能力方面采取的措施和取得的成果。</p> <p>案例 4：某拥有上亿用户的互联网公司定期召开有外部专家参与的个人信息保护机制评审会，对其新发布的产品进行把关，形成决策建议</p>
	9.4 自我保护素养提升	<p>案例 1：在 APP 等客户端设置网络学习专区，提升消费者权益保护意识。用视频和漫画等形式，对消费者进行数据安全和个人信息保护相关科普教育和意识培养。</p> <p>案例 2：在 APP 等客户端设置“安全学院”聚合全国 30 多个省、直辖市和自治区公安机关发布的反诈防骗知识，增强消费者防范意识，避免因被恶意套取个人信息进而被诈骗。</p> <p>案例 3：在 APP 等客户端设置“全民个人信息保护意识小测验”，通过答题测试的方式对消费者进行意识教育，对于答题表现突出的奖励消费券</p>

表 B.1 社会责任履行实践案例（续）

章	相关行动和期望	实践案例
10 公益参与和社会发展	10.1 参与公益事业	<p>案例 1：某大型互联网企业设立扶助基金或向相关基金捐赠，帮助某西部地区弱势群体在数据安全和个人信息保护方面学习、深造和工作。</p> <p>案例 2：某网络安全上市公司设立专门奖项，对数据安全和个人信息保护优秀人才、团体和项目等进行奖励</p>
	10.2 科普宣传活动	<p>案例 1：某平台型互联网企业在本年度国家网络宣传周上，举办个人信息主题科普展，以有奖答题等方式向观众科普个人信息保护知识和技能。</p> <p>案例 2：某电商购物 APP 通过首页弹窗形式向用户宣传网上购物过程中个人信息保护的常用知识</p>
	10.3 推动社会共治	<p>案例 1：某互联网公司拥有上亿的用户覆盖面，公司通过配合监管部门，开发了用户举报个人信息侵权行为的渠道，并在其产品的显著页面予以发布，方便用户及时向监管部门反馈问题。</p> <p>案例 2：某网络安全企业发现了贩卖个人信息的线索，在向监管部门报告后，配合监管部门对侵害个人信息权益的黑色产业链进行打击</p>
	10.4 促进社会发展	<p>案例 1：某企业与某产业发展研究所合作开展了年度数据安全或个人信息保护研究课题。</p> <p>案例 2：某企业参与了某行业组织发起的网络安全优秀创业项目大赛，并就获奖项目进行投资承诺</p>

附 录 C
(资料性)

数据安全和个人信息保护社会责任报告模板

数据安全和个人信息保护社会责任报告可单独成报告,也可是组织整体社会责任报告的一个独立部分,报告的主体内容见第 6 章~第 10 章中的主题和议题(共 5 方面主题,20 个议题),以下是数据安全和个人信息保护社会责任报告模板示例。

示例:

<p>××××公司数据安全和个人信息保护社会责任报告</p> <p>一、关于本报告</p> <p>内容参考:企业对社会责任的理解决、企业社会责任实施的背景、企业社会责任报告的发布历程、企业社会责任报告的编制依据、该报告披露信息和数据的时间维度和更多信息及投诉建议渠道等。</p> <p>二、管理层致辞</p> <p>内容参考:以第一人称口吻阐述过去(如一年内),企业在社会中扮演的社会角色,描述自身数据安全和个人信息保护等方面的突出成果,以及企业是如何不断以创新驱动寻找新的社会责任价值,践行数据安全和个人信息保护社会责任的方向和途径。</p> <p>三、社会责任履行整体情况</p> <p>1. 企业简介</p> <p>内容参考:企业官方简介,以及采取何种组织架构和管理体系等履行企业社会责任。</p> <p>2. 关键绩效</p> <p>内容参考:基于第 6 章~第 10 章中的主题和议题(共 5 方面主题,20 个议题),归纳效果突出的社会责任相关活动,予以重点披露。</p> <p>3. 外部认可</p> <p>内容参考:数据安全和个人信息保护方面的科技成果、专利和各类奖项,以及社会活动中被高度肯定和被表彰等的案例。如果参与了数据安全和个人信息保护社会责任评价等活动,可说明评价背景、评价依据和评价结果等。</p> <p>四、社会责任履行详细情况</p> <p>内容参考:基于第 6 章~第 10 章中的主题和议题(共 5 方面主题,20 个议题)框架进行编排,也可根据自身企业文化、业务特点和用户类型等进行框架设计。该部分内容基于第 6 章~第 10 章中的内容予以归纳和总结,以图文结合的形式予以展现。同时,对于存在典型案例的议题,可详述典型案例,以丰富报告内容。</p>
--



示例（续）：

内容编排方式一：基于本文件中的主题和议题内容予以展开。

1. 组织治理

描述责任履行情况。

.....

5. 数字包容和特殊保护

描述责任履行情况。

【典型案例】

例如：介绍在数字包容和特殊保护方面产品的新功能，以及其采取默认保护个人信息的机制和用户使用的评价等。

.....

内容编排方式二：如仅撰写《个人信息保护社会责任报告》，可参照以下结构，同时结合本文件第 6 章～第 10 章中的主题和议题内容予以展开。

1. 个人信息保护组织架构和内部管理情况；
2. 个人信息保护能力建设情况；
3. 个人信息保护措施和成效；
4. 个人行使权利的受理情况；
5. 独立监督机构履职情况；
6. 重大个人信息安全事件处理情况；
7. 促进个人信息保护社会共治的科普宣传和公益活动情况；

.....

五、总结和展望

内容参考：总结数据安全和个人信息保护社会责任的履行经验和成效，描绘下一步（如下一年度）开展的工作、活动计划和目标等。

六、信息反馈

内容参考：向公众公开其在数据安全和个人信息保护社会责任方面工作的调研问卷、反馈和建议渠道。

七、附录（可选）

内容参考：披露识别和评价数据安全和个人信息保护社会责任活动的具体依据材料，如有关的出版物、发布成果、网站链接、新闻报道、活动纪实和证书证明等内容。



参 考 文 献

- [1] GB/T 35273 信息安全技术 个人信息安全规范
- [2] GB/T 36000—2015 社会责任指南
- [3] GB/T 36001—2015 社会责任报告编写指南
- [4] GB/T 36002—2015 社会责任绩效分类指引
- [5] GB/T 39335 信息安全技术 个人信息安全影响评估指南
- [6] GB/T 39604—2020 社会责任管理体系 要求及使用指南
- [7] GB/T 39626—2020 第三方电子商务交易平台社会责任实施指南
- [8] GB/T 41479 信息安全技术 网络数据处理安全要求
- [9] GB/T 44588 数据安全技术 互联网平台及产品服务个人信息处理规则
- [10] GB/T 45404 数据安全技术 大型互联网企业内设个人信息保护监督机构要求
- [11] RB/T 178—2015 合格评定 社会责任要求
- [12] RB/T 179—2018 合格评定 社会责任评价指南
- [13] SB/T 10963—2013 商业服务业企业社会责任评价准则
- [14] YD/T 3837—2021 信息通信行业企业社会责任评价体系
- [15] 中华人民共和国数据安全法(2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过)
- [16] 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)
- [17] 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)
- [18] 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)
- [19] 网络数据安全条例(2024年8月30日国务院第40次常务会议通过)



