ICS 35.030
CCS L 80

T/CCIA

中 国 网 络 安 全 产 业 联 盟 技 术 规 范

T/CCIA 002—2022

数据安全和个人信息保护社会责任指南

Guidance on social responsibility of data security and personl information protection

2022－12－30 发布　　2023－02－01 实施

中国网络安全产业联盟　　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》给出的规则起草。

本文件由中国网络安全产业联盟提出。

本文件由中国网络安全产业联盟归口。

本文件起草单位：中国电子技术标准化研究院、中国科学院信息工程研究所、北京百度网讯科技有限公司、北京快手科技有限公司、中国网络安全审查技术与认证中心、蚂蚁科技集团股份有限公司、北京市环球律师事务所、腾讯科技（深圳）有限公司、贝壳找房（北京）科技有限公司、北京数安行科技有限公司、北京华品博睿网络技术有限公司、旗天科技股份有限公司、完美世界（北京）软件科技发展有限公司、深圳赛西信息技术有限公司、启明星辰信息技术集团股份有限公司、广州竞远安全技术股份有限公司、上海冰鉴信息科技有限公司、南京尚网网络科技有限公司、成都卫士通信息产业股份有限公司、北京腾云天下科技有限公司、北京汉华飞天信安科技有限公司、北京亿赛通科技发展有限责任公司等。

本文件主要起草人：何延哲、高能、李敏、落红卫、郭建领、白晓媛、樊华、孟洁、张朝、武杨、王海棠、薛颖、刘玉红、严孝馨、王昕、李海英、黄蓉、王福彪、刘金利、周瑞群、李超然、张雪、徐荣荣、张栌文、成嘉轩、张艺伟、邵冰、彭晋、徐晶晶、胡娴、葛梦莹、彭根、孙硕、毕思文、曾希雯、伍贤锋、李楷等。

数据安全和个人信息保护社会责任指南

1 范围

本文件为组织理解数据安全和个人信息保护社会责任以及实施相关活动提供指南。

本文件适用于处理数据的组织，还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水平。

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 35273—2020 信息安全技术 个人信息安全规范

GB/T 36000—2015 社会责任指南

GB/T 41479—2022 信息安全技术 网络数据处理安全要求

3 术语和定义

GB/T 36000—2015界定的以及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。

[GB/T 36000—2015，定义 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。

[GB/T 36000—2015，定义 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。

[GB/T 36000—2015，定义 3.19]

3.4

员工 employee

与组织(3.22)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。

[GB/T 36000—2015，定义 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。

[GB/T 36000—2015，定义 3.15]

4 概述

本文件旨在帮助组织在遵守法律法规和基本道德规范的基础上实现更高的社会价值，最大限度地致力于可持续发展。

组织在其数据处理活动满足适用的法律法规要求的基础上，参照GB/T 36000—2015提出的原则，根据本文件第5章至第9章中的主题和议题（共5大主题，24个议题），确定具体的数据安全和个人信息保护社会责任范围及优先事项。本文件第5章至第9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、发展阶段及利益相关方期望，识别确定每项社会责任主题和议题中适用的具体内容。

组织或第三方机构宜根据附录A给出的评价方法，识别社会责任履行的薄弱环节并持续改进，不断提升履行数据安全和个人信息保护社会责任的管理成熟度和绩效等级。

附录B给出了组织在数据安全和个人信息保护社会责任实践案例。

5 组织治理和内部管理

5.1 核心价值观及发展理念

5.1.1 议题描述

核心价值观，是指存在于组织内部并为组织全体员工认同且长久秉持的基本价值取向，是引领组织进行决策和活动的核心指导原则。发展理念，是指组织所担负的使命、所秉持的基本信念、所追求的创立宗旨、所遵循的发展哲学。从核心价值观和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。

5.1.2 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。

——组织在已成文并广泛推广的核心价值观、发展理念中阐述关于数据安全及个人信息保护相关的愿景、目标。

注：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。

5.2 管理层承诺或声明

5.2.1 议题描述

管理层承诺或声明，是指对组织负有管理责任的人员作出的公开表态或说明。公开的承诺和声明有

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。

5.2.2 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。

——组织的管理层在正式、公开的场合阐述组织数据安全和个人信息保护的核心价值观、发展理念等，并以承诺、声明等形式予以强调。

——组织的管理层在内部培训场合向员工阐述组织数据安全和个人信息保护的核心价值观、发展理念等，以促进相关价值观、理念等得以贯彻。

5.3 社会责任战略及工作目标

5.3.1 议题描述

社会责任战略，是指用于统领和指导本组织中长期社会责任实践的谋略、方案和对策，通常包括社会责任方针、目标、方案和措施等。工作目标，是指组织根据实际情况需要所拟订的具体行动目标。

5.3.2 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。

——组织将数据安全、个人信息保护以及数字包容等方面的内容纳入组织的社会责任战略和工作目标中。

——组织将社会责任战略、工作目标形成具体的纲领性文件，在组织内向有关部门及人员进行下发，使其能充分的沟通和理解，并在日常工作中得以贯彻执行。

5.4 实施主体及资源支持

5.4.1 议题描述

实施主体，是指组织中具体实施数据安全和个人信息保护社会责任工作的部门或人员。资源支持，是指组织为推动数据安全和个人信息保护社会责任工作提供财务、人力、环境等资源。实施主体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实施的前提条件。

5.4.2 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。

——指定具体的高管担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，如任命高管担任数据保护官（DPO）或首席隐私官（CPO）等职位，并由其负责履行相关的社会责任。

注 1：担任负责人的高管职务、姓名、联系方式至少在组织层面予以公开。

——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目标、工作职责和工作方案。

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情况。

——在相关部门或人员的工作职责中明确需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。

——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，以便于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、信息发布等平台的热议话题、投诉、举报渠道等。

——为履行数据安全和个人信息保护社会责任提供专门、充足的财务预算。

5.5 内部宣贯和培训

5.5.1 议题描述

内部宣贯，是指组织通过宣传法律法规、政策、方案等使组织内部深刻理解并付诸于实践。内部培训，是指组织通过各种方式、手段督促员工在知识、技能、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更广泛的认可度，并促进内部员工对相关工作的配合意识。

5.5.2 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。

——组织在内部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。

注 1：内部管理制度中可包含落实社会责任的组织架构体系、相关职责、目标、方案等，具体可参考 5.3、5.4。

——在组织内部定期（每年至少一次）开展数据安全和个人信息保护社会责任理念、制度、知识、案例等的宣传、培训工作。

——聘请外部数据安全和个人信息保护专家，对负责落实社会责任要求的关键岗位人员（如负责人、相关部门责任人、社会责任报告编制人等）进行重点培训。

注 2：外部专家宜具备在履行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的社会公益活动，并优先选择受到权威组织表彰和社会广泛认可的专家。

5.6 内部监督和员工激励

5.6.1 议题描述

内部监督，是指组织对内部管理制度的建立与实施情况进行监督检查，评价组织内部管理的有效性，发现组织管理缺陷，并及时加以改进。员工激励，是指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更加显著的执行力。

5.6.2 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。

——建立内部监督机制，由数据安全和个人信息保护社会责任工作的部门或人员接收内部人员反馈的监督意见，并推动相关意见得到处理。

——鼓励相关人员积极学习数据安全和个人信息保护相关的知识和技能，并通过考取证书、获取证明等方式提升自身能力水平。

——将相关人员充分、积极、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，如取得积极社会反响在绩效考核时予以加分。

注：由权威部门授予感谢信、奖状等方式可视为取得积极社会影响。

6 合规性、创新性和价值体现

6.1 产品或服务的合规性

6.1.1 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，是指产品或服务符合法律法规、规章、规范性文件、相关标准等的要求，以降低合规性风险。合规工作主要表现形式为组织开展制度、文档、策略、流程的建设，完成内审、自评估、第三方评价、第三方审计，获得权威机构认证等。

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。

——通过组织内自行发起或引入独立第三方对产品或服务遵循法律法规、规章、强制性标准的情况进行评估或审计，并形成评估或审计记录、结论或报告以指导产品或服务持续改进。

注 1：评估或审计的依据可参考推荐性的国家标准、行业标准、团体标准，以及业界广泛认可的技术规范等。

注 2：常用的评估依据有：GB/T 35273-2020、GB/T 41479-2022 等。

——引入独立第三方评价后，取得产品或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。

——通过对组织层面数据安全和个人信息保护方面的管理体系、技术能力的认证与监督，使得产品或服务能够持续保持符合性。

——发布数据安全和个人信息保护相关的合规说明（或白皮书、报告、说明等），向外界展示数据安全和个人信息保护方面的履责情况，增进用户对产品或服务所采取合规措施的理解。

——及时发现并响应对数据安全和个人信息保护相关的安全事件，建立与利益相关方、监管部门的沟通渠道及程序，不断提升数据安全和个人信息保护能力水平。

6.2 技术的创新性和先进性

6.2.1 议题描述

技术的创新性和先进性，是指基于当前技术发展水平，能更高效、低成本解决数据安全和个人信息保护相关特定问题，或能提升相关生产力水平，或对经济发展、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、社会创造经济效益、社会效益。创新性和先进性主要表现形式有专利、权威机构认证、国家或行业奖项、试点示范等。

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。

——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。

——建立对技术创新的长期激励机制，包括管理制度、绩效考核、资金奖励等。

——参与申报、实施数据安全和个人信息保护相关的科研项目。

——搭建同行业交流机制或平台，推动创新标杆组织进行内部分享或培训，交流分享创新性理念、方法，并为技术创新提供学术研究、国际交流等方面的有利条件。

——参与产品或服务数据安全和个人信息保护相关技术的创新及先进性评比、奖项申报等活动，并取得优异的成绩。

——采取必要的机制尊重和保护产品或服务的数据安全和个人信息保护相关技术的创新性和先进性证明成果（如申报专利、知识产权保护措施、试点证明等），防范成果被窃取、盗用。

——对具备数据安全和个人信息保护相关技术创新性、先进性且产业实践效果良好的产品或服务，通过获得权威机构认证等方式扩大其影响面、应用面。

——将数据安全和个人信息保护专利申请及授权量、获取的科技奖项作为组织宣传的重要素材予以体现。

——整合系列具有自主知识产权、在创新性和先进性上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，并创立行业知名的品牌，为提升行业整体水平、在全球范围内展现竞争力有显著作用。

6.3 用户使用的价值体现

6.3.1 议题描述

用户使用的价值体现，是指根据数据处理的目的，向用户提供其所需的产品或服务，并充分履行数据安全和个人信息保护责任，为用户提供保障其数据和个人信息权益的机制。

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。

——用户提供必要的数据即可使用与所处理数据相关的功能。

注 1：在用户使用功能时不能设置不合理的条件，如捆绑其他功能、增加收集数据的种类、设置过长的等待时间、增加无关的操作步骤等。

——将数据安全和个人信息保护的功能设置为基础功能的一部分。

注 2：基础服务通常不向用户额外收取费用。

——通过不断优化数据处理的流程、步骤，以优化收集数据时机、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增加对数据的脱敏、去标识化、匿名化处理。

——在不影响用户权益的前提下，通过优化算法等方式进一步挖掘数据价值，提升服务质量、提高响应效率、强化安全保障等。

——提供必要的措施以保障用户对其数据的控制权，并优化用户行使权利的路径，包括对数据进行查询、复制、更正、删除、转移等。

注 3：境外的组织面向境内用户提供的行使权利的路径时，充分考虑了境内用户的语言、操作等习惯。

——对数据处理活动进行审计，以支持用户在合理范围内对组织是否超出约定处理数据进行查验、核实等。

——及时处置用户对于数据安全和个人信息保护相关的投诉、举报，定期评估投诉、举报的数量、处理率、处理评价情况，以提升产品或服务的功能和投诉、举报的处理机制。

6.4 社会治理的价值体现

6.4.1 议题描述

社会治理的价值体现，是指组织为保障用户数据安全及个人信息保护，所制定的具有社会功能的治理策略，以支撑有关部门开展社会治理活动，降低社会安全风险；促进社会组织、企业开展行业自律，履行社会责任；引导用户自我管理、自我教育、自我服务、自我监督，发挥用户参与的积极作用。

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。

——产品或服务可支撑有关主管监管部门、社会组织等开展的数据安全和个人信息保护相关的评议、治理、监管、执法等活动，或对相关活动提供技术支撑、资源保障。

注 1：支撑有关主管监管部门、社会组织活动期间，涉及到受委托处理数据的，需充分履行数据安全和个人信息保护义务。

——为社会公众提供参与预防、举报、惩治数据安全和个人信息保护相关侵权行为的制度、渠道，完善用户参与社会治理的机制。

——向社会公众发布数据安全和个人信息保护相关的常见问题、突发事件预警、优秀经验案例等有参考价值的信息、内容。

——产品或服务所提供的功能等能主动引导用户加强数据安全和个人信息保护，大范围提升数据安全和个人信息保护的水平。

注 2：如拥有大量用户的产品或服务，通过免费、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。

——通过构建技术平台、行业合作框架等方式，对频繁发生、影响恶劣的危害用户数据安全和个人

信息保护相关权益的行为、信息等能快速识别、响应，并及时处置。

——通过多组织协作、与监管部门联动等形式及时响应数据安全和个人信息保护相关的事件应急处置等活动。

6.5 数字包容与特殊保护

6.5.1 议题描述

数字包容与特殊保护，是指组织为保障多元人群的数据安全及个人信息保护所开展的活动，使得多元人群能公平、自由、安全地获取和享受技术变革和产业发展提供的便利，能无差别的体验数字化生活。数字包容与特殊保护主要表现形式有为多元人群提供更便利的数据安全服务、更有效的个人信息保护措施、为多元人群提供更全面的和公平的社会环境。

6.5.2 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。

——开发无障碍产品/方案，为多元用户（例如不同地区、知识水平、语言环境、青少年、残障人士、老年人等）提供平等的数字产品或服务，消除数字鸿沟，重视并保护多元人群的数据和个人信息，为多元人群提供符合其应用场景的数据安全和个人信息保护机制。

——在面向特殊人群（如青少年、残障人士、老年人等）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、协助、行权的模式，为其个人信息使用场景进行严格限制等。

——制定特殊人群（如青少年、残障人士、老年人等）个人信息保护方面的处理规则，并为特殊人群提供专门的服务界面、服务渠道，以确保其能感知、获取个人信息保护方面的信息。

——参与特殊人群（如青少年、残障人士、老年人等）数据安全和个人信息保护相关标准制定，加入相关倡议、计划等活动，以促进行业协同。

——投入资源主动推广特殊人群（如青少年、残障人士、老年人等）使用的产品或服务（或相关模式），并引导特殊人群关注使用产品或服务时保护个人信息。

——对数字包容和特殊人群保护方面的涉及数据安全和个人信息保护的能力、技术资源进行开放，为行业提供参考、支撑。

7 公平运行、竞争与合作

7.1 数据处理规则的透明性

7.1.1 议题描述

数据处理规则的透明性，是指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，从而确保数据处理活动对利益相关方是清晰透明、容易获取的，从而增进利益相关方信任，便于利益相关方进行监督、审计。

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。

——涉及个人信息处理的，根据相关法律法规要求，遵循公开、透明原则，向个人完整、真实、准确披露个人信息处理的规则，具体的方式参照 GB/T 35273—2020 第 5 章。

——建立与利益相关方沟通的机制，就数据处理的目的、方式、范围等规则进行及时沟通、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、答疑的渠道，针对复杂、难懂、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），可通过进一步解释说

明的方式以增进理解。

——数据处理规则可能影响到利益相关方重大权益的，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，确保利益相关方能够理解后做出决定。

——数据处理规则影响范围广泛（如超过 1000 万用户的互联网平台的产品及服务的个人信息保护政策），可通过公开征求意见等方式进一步确认具体条款内容的合理性；有关法律法规、规章制度等有规定的从其规定。

7.2 知识和技术成果保护与共享

7.2.1 议题描述

知识和技术成果主要表现形式为知识产权、商业秘密及其他财产性权益。承认数据安全和个人信息保护的财产性权益既可促进投资、经济和有形财产的安全，也可激励知识和技术成果的共享与技术迭代创新。

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。

——实施能够推动尊重数据安全和个人信息保护知识和技术成果的政策、做法和管理程序。开展恰当的调查，以确保享有相关知识和技术成果的使用权或处置权。

——坚决抵制侵犯数据安全和个人信息保护相关知识和技术成果及阻碍相关知识和技术成果合法共享的活动，包括滥用支配地位进行垄断、假冒和盗版等不正当竞争行为。

——对所获得或使用的数据安全和个人信息保护相关知识和技术成果共享支付合理的对价。

——在行使并保护自身的数据安全和个人信息保护相关知识和技术成果相关权利时，考虑社会期望、个人需求。

——鼓励开展数据安全和个人信息保护相关知识和技术成果的价值链创新，进一步提升知识和技术成果共享效益。

——推动形成数据安全和个人信息保护相关知识和技术成果的交易及价值创造机制，以价值共享的形式推动知识和技术成果共享。

——可自行或与其他组织合作，推动探索多种数据安全和个人信息保护相关知识和技术成果共享方式，包括：

- 发布数据安全和个人信息保护相关的白皮书，分享优秀经验、案例；
- 与高校、培训机构等联合开发课程；
- 鼓励员工发表技术文章、参与专著撰写等；
- 向开源社区等分享源代码；
- 向具有法定职能的组织共享威胁、事件情报。

——促进数据安全和个人信息保护先进技术的推广及应用，如区块链、联邦学习、隐私计算等新兴技术。

7.3 构建有效的平台规则

7.3.1 议题描述

平台规则的有效性关系到平台运营者所制定数据安全和个人信息保护的策略、方针、制度、细则、程序等能否促使平台参与方（如商户、合作伙伴等）切实履行相关责任和义务。定期评估平台规则的有效性，可明晰当前规则落地现状，为策略、方针、制度、细则、程序等优化提供支持。定期对外公布平台规则的执行效果可提升平台的信誉、影响力，以引导平台参与方不断强化数据安全和个人信息保护意识。

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。

——组织所制定的平台规则，需关注数据安全和个人信息保护相关法律法规要求以及行业最佳实践，引导平台参与方更好地执行保护数据安全和个人信息保护的策略、采取更有效的安全措施。

——将数据安全和个人信息保护相关平台规则执行效果纳入到审计等监督环节中，以推动平台规则能切实有效执行。

——形成可以衡量数据安全和个人信息保护相关平台规则执行效果的评价指标、标准，通过计算方式评价平台规则的执行效果以认定工作成效。

——定期（至少每年一次）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。为保证执行效果评价客观性，可引入第三方或权威机构，保证评估结果的客观性。

——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，如定期发布相关的执行效果的报告等。

7.4 供应商规则共建及协助

7.4.1 议题描述

供应商规则共建及协助，是指建立供应商的管理机制，实现平等交易、互利互惠、和谐共赢的供应商关系，促进相关供应商的数据安全和个人信息保护水平整体提升。

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。

——建立供应商管理制度，并在供应商筛选阶段公开，明确供应商应符合的数据安全和个人信息相关安全基线、淘汰指标等。

——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、特殊的数据安全和个人信息保护要求，以定向促成相关供应商的入选。

——以合同、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、安全责任等内容。

——对合作过程中接触数据的人员权限进行限定、审批、登记及管理，并要求签署保密协议，定期对相关人员行为进行审核。

——涉及与供应商使用接口等方式进行数据交互的，采取必要的技术手段对数据交互日志进行记录，如供应商不具备技术能力的，可向其共享相关日志信息以增进透明性。

——通过对供应商数据处理活动的安全风险和供应商数据安全管理能力进行评估等方式，推动供应商保持数据安全能力水平。评估发现重大安全风险的，可执行供应商退出、替换机制等，避免为利益相关方带来损失。

——建立供应商应急响应机制，对合作过程中的数据安全事件及时响应，并为供应商提供必要的技术、人员等资源支持。

——注重与供应商的长期合作，协助供应商业解决数据安全和个人信息保护方面面临的困难和难题，建立互信共赢的合作关系。

7.5 公平竞争环境构建

7.5.1 议题描述

构建公平竞争环境，营造优胜劣汰的市场氛围，能够激励组织更加有效率地投资和创新，激励组织以更优质的产品或服务吸引消费者，对促进经济发展和人民生活水平至关重要。但如果组织利用在数据、流量等方面积累的优势地位，破坏公平竞争环境，将可能阻碍中小企业的发展和新业态的创新。

7.5.2 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。

——在数据处理相关的生产经营活动和参与市场竞争中，遵循自愿、平等、公平、诚信的原则，遵守竞争、知识产权保护相关的法律法规和商业道德，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。

——杜绝任何形式利用数据的不正当竞争及垄断行为，如：

- 通过数据、算法、平台规则等方式达成垄断协议；
- 利用数据、算法、技术等方面的优势实施滥用市场支配地位的垄断行为；
- 通过非法或不正当手段获取其他平台数据（包括互联网平台用户的个人信息）；
- 利用数据和用户个人信息建立的竞争优势，形成数据孤岛，阻碍竞争对手进入市场，损害用户的自主选择权；
- 利用垄断地位阻止其他组织向监管部门投诉、举报；
- 其他不正当竞争行为。

——制定并实施组织内部反腐败制度，对管理层和员工在数据安全和个人信息保护方面的腐败行为均采取零容忍态度。

注：腐败行为包括：利用权限删除、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、共享等。

——通过内部培训、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垄断、反不正当竞争、知识产权保护等方面的知识和意识；

——拥护政府部门构建平台经济公平竞争环境的政策和行动，遵守数据安全、个人信息保护等相关的法律法规，积极配合监管部门对反垄断、反不正当竞争相关的调查和执法行动。

8 消费者权益保护

8.1 个人人身、财产利益保护

8.1.1 议题描述

消费者个人人身、财产（包括虚拟财产）利益保护，是指组织提供的产品或服务不会为消费者带来严重的人身、财产损害风险，并能够通过一系列识别风险的机制，防范损害消费者人身、财产利益的行为发生。

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。

——若有充分证据表明，现已存在能够显著提高数据安全和个人信息保护水平的解决方案，组织不宜保持较低的数据安全和个人信息保护水平。

——在产品或服务的设计、开发过程中，通过下列方法最大程度的降低消费者人身、财产损害的风险：

- 分析产品或服务在所有使用场景、阶段和条件下，可能对消费者人身、财产产生损害的功能组件、服务场景等，评估损害风险并明确防止损害的具体措施；
- 充分考虑消费者的需求差异、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，防止因其导致消费者利益受损；
- 遵循以下优先级顺序降低对消费者利益的风险：首先，考虑采用完全消除风险的安全设计；其次，考虑增设保护性装置降低风险；最后，考虑向消费者提供警示信息。

——在产品或服务的使用过程中，建立能够识别消费者风险行为的特征库。

——识别消费者存在风险行为的，视具体情况采取以下措施：

- 通过复合措施核验消费者的身份；
- 通过显著方式向消费者警示可能出现的风险，并经消费者确认。

注：除使用文字信息外，还宜尽可能使用符号、图片、语音等方式向消费者传递告知重要信息。

——当消费者遭受或可能遭受人身、财产损害时，为消费者提供简捷、迅速的反馈渠道，并及时处置。

——在消费者使用产品或服务前，组织宜：

- 指导消费者安全、正确使用产品或服务；
- 结合产品或服务的具体情况，说明与使用有关的风险及预防措施；
- 告知消费者遭受或可能遭受人身、财产损害时的反馈渠道及处置方式。

——采取紧急措施以避免消费者人身、财产利益继续受损，紧急措施涉及消费者个人信息处理的应当满足相关法律法规要求，并尽可能同步向消费者告知相关情况。

——在产品或服务的使用过程中，如出现重大漏洞、或包含有误导或错误的信息，可立即中止提供服务以防止消费者利益受损，并及时通知受影响的消费者以采取补救措施。

——建立能够识别损害消费者人身、财产利益违法违规行为的特征库，并持续监测、打击违法行为。

8.2 消费者投诉及争议处理

8.2.1 议题描述

消费者投诉及争议处理，是组织在提供产品或服务时，接受消费者关于数据安全和个人信息保护方面问题反馈、监督的关键手段。组织可通过消费者的投诉、建议等完善内部数据安全和个人信息保护的机制，不断提升数据安全和个人信息保护水平。

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。

——以清晰、显著的方式公示数据安全和个人信息保护相关投诉渠道、处理方式及反馈时限。

——公示的投诉渠道稳定、易用，如涉及投诉渠道的变更、转换，尽可能通过内部协调实现，不对消费者带来过多困扰、打扰。

——提供一定比例人工客服支持的投诉反馈渠道。

注：比例可根据消费者对投诉处理机制满意度的评价情况予以设定。

——建立投诉处理流程，并完善有效的操作规范，形成从投诉到反馈的闭环，避免消费者投诉无人处理、无人反馈等情况。

——建立投诉处理库（至少保留半年内投诉处理情况），记录投诉处理的时间、原因、处理情况等，便于组织定期评审并改进。

——建立投诉处理满意度的反馈途径，便于消费者通过该途径反馈意见或建议。

——处理投诉时原则上不向消费者收取费用，根据消费者要求处置相关事宜时涉及成本费用的除外。

——定期公开发布投诉处理汇总情况，如在社会责任报告等可公开发布的文件中予以体现。

8.3 接受中立机构监督

8.3.1 议题描述

接受中立机构监督，是指通过主动披露等方式使中立机构相关的社会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，针对中立机构提出的疑问和改进建议进行及时反馈和改进。

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。

——向社会公开数据安全和个人信息保护相关的规则，定期发布数据安全和个人信息保护社会责任报告，主动接受社会监督。

注：数据安全和个人信息保护社会责任报告模板见附录C。

——提供重要互联网平台服务、用户数量巨大、业务类型复杂的组织，可成立主要由外部成员组成的独立中立机构，对其数据和个人信息处理活动进行监督。

——指定组织内负责数据安全和个人信息保护的具体人员，使其承担与中立机构沟通、对接的职责。

——通过获得国际和国内的数据安全和个人信息保护的认证等方式接受认证机构监督。

——可向中立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，通过向中立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，组织应及时予以纠正。

8.4 消费者教育和意识培养

8.4.1 议题描述

消费者教育和意识培养是指通过一系列活动宣传等，促使消费者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，做出更有利于保护自身权益以及更加负责任的活动。

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。

——在运营的产品或服务的显著界面、位置、步骤设置消费者教育和意识培养相关的宣传活动。

——在特定日期（如消费者保护日等）设置消费者教育和意识培养相关的宣传活动。

——消费者教育和意识培养活动的内容包括：

- 数据安全和个人信息保护的适用法律法规、政策制度等；
- 常用的投诉举报途径、消费者保护机构联系方式等；
- 常见的数据安全和个人信息保护知识和技能；
- 产品或服务相关的数据安全和个人信息保护功能；
- 与使用产品或服务有关的风险信息以及所有必要的警示信息；
- 数据和个人信息泄露导致的风险和案例；
- 使用产品或服务过程中注重保护他人的数据、个人信息的意识。

——以提供奖励等方式鼓励消费者积极参与教育和意识培养相关活动。

9 公益参与和社会发展

9.1 慈善捐助和公益事业

9.1.1 议题描述

组织通过慈善捐助和参与公益活动，支持公共服务机构、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。

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。

——提供数据安全和个人信息保护相关慈善捐助、公益事业的财务预算。

——调研、了解运作良好的数据安全和个人信息保护的慈善、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、参与人员的特长等确定开展慈善捐助和公益参与

的范围和工作计划。

——参与具体慈善捐助和公益活动，常见的有：

- 筹建数据安全和个人信息保护研究的中立机构、维权平台、科普中心或向相关机构进行捐赠；
- 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、工作；
- 设立专门奖项，向数据安全和个人信息保护优秀人才、团体、项目等进行奖励；
- 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，提供免费的法律救助服务。

——对于慈善捐助和公益事业项目的效果进行评估，优化、调整工作的范围、方式等以提升社会责任履行效果。

9.2 活动举办和科普宣传

9.2.1 议题描述

组织通过积极举办或参与数据安全和个人信息保护相关的活动，以及开展科普宣传工作，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、公众对相关前沿技术的了解，帮助公众提升自我保护的知识和技能，扩大组织在社会层面的影响力和认可度。

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。

——为举办数据安全和个人信息保护相关的活动提供必要的资源支持，包括人员、经费、场地、媒体、渠道等。

——自行组织或主动参与能推动数据安全和个人信息保护产业发展、技术创新等方面的活动，同时保证活动的专业性、公正性，常见的活动有：

- 数据安全和个人信息保护主题的会议、沙龙等；
- 数据安全和个人信息保护相关的比赛、评比等；
- 数据安全和个人信息保护相关的展会等。

——自行组织或主动参与能推动社会公众了解、掌握数据安全和个人信息保护知识和技能的知识科普活动，同时保证科普素材的趣味性、互动性，常见的活动有：

- 数据安全和个人信息保护主题的文章、漫画、海报、短视频等；
- 数据安全和个人信息保护相关的互动答题、游戏、体验等；
- 数据安全和个人信息保护相关的影视剧、专题片、专著、手册等发布物等。

——通过邀请社会公众人物参与、与媒体合作、在适当的时间段集中举办等方式扩大活动的影响面、宣传效果。

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

——对于活动和科普宣传的效果进行评估、总结，为后续活动的开展提供参考。

9.3 行业自治和工作联动

9.3.1 议题描述

组织通过参与行业组织，并支持相关行业自律、治理行动，以及联合相关领域组织、配合主管监管部门工作等形式，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。

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。

——积极加入包含数据安全和个人信息保护相关职责的社会、行业组织，参与其组织的各类活动。

——积极响应社会、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、工作计划等。

——与相关领域内的组织，如政府、企事业单位、高校、研究机构等，达成数据安全和个人信息保护相关的工作备忘、合作协议等，以扩大工作的范围，提高工作的频率。

——协助主管监管部门开展数据安全和个人信息保护相关的法律法规宣贯、标准实践推广、日常监督管理、违法犯罪打击等工作。涉及大型平台、基础设施等的组织，可进一步明确工作支撑部门或人员，并纳入到日常管理和考核中。

9.4 就业创造和产业投资

9.4.1 议题描述

组织通过对数据安全和个人信息保护的产业链提供支持，包括人才培养、技能认证、上下游协同发展等，促进数据安全和个人信息保护方面的就业的稳定性、创新的积极性，推动相关产业快速发展。

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。

——经济可行的前提下，选择能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。

——设立在职人才培养平台，接纳学校、培训机构中数据安全和个人信息保护方向学生、学员的实习，参与有偿合作项目的，给予适当的劳动报酬。

——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、初创企业供应商创造机会。

——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。

——关注数据安全和个人信息保护方向的中小企业、初创企业的发展，满足投资条件的，可提供资金方面的支持。

——如组织具备一定能力、经验、资源等，可通过与政府、行业组织等合作的方式，搭建产业孵化基地、创新实验平台等，吸引优秀人才创业发展。

附 录 A
（规范性）
数据安全和个人信息保护社会责任评价方法

A.1 评价指标和评价等级确定

通过指标评价方式，可促进组织确定社会责任管理的优先事项，对社会责任绩效进行分级评价，有助于组织策划和实施提升社会责任的绩效。

表 A.1 给出了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。结合本文件第 5 章至第 9 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 24 项二级指标。针对每项二级指标，分为三个评价级别（一星级、二星级、三星级），每项二级指标分值区间为 3 分，即：一星级：1-3 分，二星级：4-6 分，三星级：7-9 分，不满足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，评价依据如下：

a) 一星级（基础级）：组织遵守法律法规要求，履行了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等于 30 分；

b) 二星级（系统级）：在达到一星级指标要求的基础上，建立良好的社会责任管理体系，并取得更高的社会责任绩效。要求 24 项指标（存在不适用指标的，从总数中扣除）中至少 60%以上达到指标要求，即 60%以上的二级指标项至少得 4 分。其中“★”项为必选指标（不适用的情况除外），该项至少得 4 分；

c) 三星级（成熟级）：在达到了二星级指标要求的基础上，持续改进社会责任管理绩效，主动承担更多社会责任，在多项指标上不断实现更高的社会责任绩效。要求 24 项指标（存在不适用指标的，从总数中扣除）至少 80%以上达到指标要求，即 80%以上的二级指标项至少得 7 分。

表 A.1 评价指标与评价等级

一级指标		二级指标		一星级(基础级)	二星级(系统级)	三星级(成熟级)
一	组织治理和内部管理	1	★核心价值观及发展理念	组织的核心价值观符合法律法规和政策中数据安全及个人信息相关的保护理念，在成文的核心价值观和发展理念中强调了数据安全和个人信息保护的重要性。	组织在已成文并广泛推广的核心价值观、发展理念中具体阐述关于数据安全及个人信息保护相关的愿景、目标。 组织配置相应的资源，以持续满足核心价值观和发展理念的管理要求并持续改进和更新。	组织的核心价值观及发展理念能在数据安全和个人信息保护方面对同业伙伴、供应链、投资、客户等与自身经营有实质性关联的领域产生积极影响。

表 A.1　评价指标与评价等级（续）

一级指标		二级指标		一星级(基础级)	二星级(系统级)	三星级(成熟级)
一	组织治理和内部管理	2	管理层承诺或声明	组织的管理层对数据安全和个人信息保护社会责任有关内容有做出过承诺或声明，承诺或声明内容符合相关法律法规、规章制度、标准等的要求。	组织的管理层通过多种形式对数据安全和个人信息保护社会责任有关内容做出承诺或声明，包括在正式、公开的场合公开声明；通过报告、制度文件等文字形式说明；通过内部培训场合向员工传达等。	组织设置对管理层承诺或声明的跟踪机制，允许内部、外部人员对其进行评价、监督，促进管理层能切实履行承诺并尽责。
		3	★社会责任战略及工作目标	组织的数据安全和个人信息保护相关的社会责任战略及工作目标符合相关法律法规、规章制度、标准等的要求，并已纳入到组织的社会责任战略和工作目标中。	组织将社会责任战略、工作目标形成的纲领性文件，通过向有关部门及人员下发、定期培训等方式，使其能充分的沟通和理解，并在日常工作中得以贯彻执行。	组织接受相关方的监督，以持续改进社会责任战略及工作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优先事项，逐步充实完善社会责任事项。
		4	★实施主体及资源支持	组织为数据安全和个人信息保护社会责任工作指定了负责人并明确其职责。 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财务、人力支持。	组织指定了具体的高管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；配备了相应的责任部门或人员予以支持。 组织明确了需定期向社会披露社会责任履行情况的职责；提供了专门的财务、人力、环境等资源支持。	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方面的期望和诉求的机制；通过增加预算、人力等方式不断充实社会责任履行的力量；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、影响面。
		5	★内部宣贯和培训	组织在内部管理制度中体现了贯彻落实数据安全和个人信息保护社会责任的要求，并将制度下发至相应部门、人员。	组织内部定期（每年至少一次）开展数据安全和个人信息保护社会责任理念、制度、知识、案例等的宣传、培训工作。 组织设立相应平台或人员对实施内部宣传和培训的组织活动进行管理，培训的专业度、覆盖面应当有所保证。	组织建立了数据安全与个人信息保护社会责任知识和技能的培养体系，并对该体系持续改进；同时还能为同业伙伴、供应链、投资、客户等与自身经营有实质性关联的领域提供协助。

表 A.1 评价指标与评价等级（续）

一级指标		二级指标		一星级(基础级)	二星级(系统级)	三星级(成熟级)
一	组织治理和内部管理	6	内部监督和员工激励	组织建立了内部监督机制，接收内部人员反馈的监督意见，并及时处理意见。为相关人员积极学习数据安全和个人信息保护相关的知识和技能提供便利条件。	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、流程措施；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职责和义务。 组织为相关人员考取数据安全和个人信息保护相关证书等提供资金、渠道、时间等方面的保障。	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、效果；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。
二	合规性、创新和价值体现	7	★产品或服务的合规性	组织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等形式，确保其满足法律法规、规章、相关产品或服务强制性标准等要求。	组织自评估时，参考了推荐性的国家标准、行业标准、团体标准等，以及业界广泛认可的技术规范。 组织引入了独立第三方进行评估，取得产品或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方面的合规白皮书。	组织建立了具体的数据安全和个人信息保护的合规计划，对组织层面数据安全和个人信息保护进行持续性的认证与监督，参与了同行业针对产品及服务合规性的相关领域建设及合作。 组织能及时发现、响应对数据安全和个人信息保护相关的安全事件，并建立与利益相关方、监管部门的沟通渠道及程序。
		8	技术的创新性和先进性	组织的产品或服务采取的技术有着创新性和先进性，并以专利、权威机构认证等方式得到认可。 组织积极参加同行业内关于创新性和先进性技术的研讨、交流，并分享了组织采取的创新性技术、理念、方法。	组织构建并积极实施了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，建立了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。 组织参与了数据安全和个人信息保护相关技术的创新及先进性的评比、奖项申报等活动，并取得优异的成绩，如省部级科技奖项等。 组织采取必要的机制尊重和保护技术的创新性和先进性证明成果。	组织搭建了同行业交流机制或平台，为技术创新提供学术研究、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。 组织整合了系列具有自主知识产权、在创新性和先进性上有显著优势的技术，创立行业知名的品牌，为提升行业整体水平、在全球范围内展现竞争力有显著作用。

表 A.1　评价指标与评价等级（续）

一级指标		二级指标		一星级(基础级)	二星级(系统级)	三星级(成熟级)
二	合规性、创新和价值体现	9	★用户使用的价值体现	当用户提供必要的数据时，组织即可向用户提供与所处理数据相关的功能。 组织的产品或服务将数据安全和个人信息保护的功能设置为基础功能的一部分。 组织提供必要的措施以保障用户对其数据的控制权。	组织不断优化用户行使权利的路径。 组织不断优化数据处理的流程、步骤，以减少收集数据的种类和保留时间。 组织对数据处理活动进行审计，以支持用户在合理范围内对组织是否超出约定处理数据进行查验、核实等。	组织通过优化算法等方式进一步挖掘数据价值，为用户提供更优质的服务。 组织通过定期评估投诉、举报的数量、处理率、处理评价情况，以提升产品或服务的功能和投诉、举报的处理机制。 组织积极采取措施引导、推动同业伙伴、供应链、投资、客户等与自身经营有实质性关联的领域能够形成注重用户使用价值的良好生态。
		10	社会治理的价值体现	组织参与、支撑了有关主管监管部门、社会组织等开展的加强数据安全和个人信息保护相关的活动。 组织向社会公众发布过数据安全和个人信息保护相关的常见问题、知识技能科普等相关的内容。	组织的产品或服务可支撑有关主管监管部门、社会组织等开展的数据安全和个人信息保护相关的评议、治理、监管、执法等活动，或对相关活动提供了技术支撑、资源保障。 组织向社会公众发布过数据安全和个人信息保护突发事件预警、优秀经验案例等有参考价值的信息、内容。 组织的产品或服务所提供的功能等能主动引导用户加强数据安全和个人信息保护，大范围提升数据安全和个人信息保护的水平。	组织为社会公众提供了参与预防、举报、惩治数据安全和个人信息保护相关侵权行为的制度、渠道，完善了用户参与社会治理的机制。 组织构建了技术平台、行业合作框架等，对频繁发生、影响恶劣的危害用户数据安全和个人信息保护相关权益的行为、信息等能快速识别、响应，并及时处置。 组织通过多组织协作、与监管部门联动等形式及时响应数据安全和个人信息保护相关的事件应急处置等活动。

表 A.1 评价指标与评价等级（续）

一级指标		二级指标		一星级(基础级)	二星级(系统级)	三星级(成熟级)
二	合规性、创新性和价值体现	11	数字包容与特殊保护	组织有为多元用户提供平等的数字产品或服务的案例。 组织的产品或服务制定了面向特殊人群个人信息保护方面的处理规则。	组织重视并保护多元人群的数据和个人信息，为多元人群提供符合其应用场景的数据安全和个人信息保护机制。 组织在使用面向特殊人群的产品或服务时，其能提供个人信息的增强保护机制。 为特殊人群提供的服务界面、服务渠道，可确保其能感知、获取个人信息保护方面的信息。	组织参与了特殊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、计划等活动，以促进行业协同。 组织投入了资源开发、推广特殊人群使用的产品或服务（或相关模式），并引导其关注使用产品或服务时保护个人信息。 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、技术资源进行开放，为行业提供参考、支撑。
三	公平运行、竞争和合作	12	★数据处理规则的透明性	组织依据法律法规、规章制度、标准等的要求，完整、真实、准确地披露了数据处理的规则，明示信息处理的目的、方式和范围。	组织建立和实施了数据处理规则披露的管理制度，提供与利益相关方（组织、个人）问询、答疑等的渠道，便于进一步沟通协商。	组织建立了与利益相关方对数据处理规则进行事前沟通的机制（如征求意见等），使其数据处理规则在同业伙伴、供应链、投资、客户等与自身经营有实质性关联的领域产生积极影响。
		13	★知识和技术成果保护与共享	组织的知识和技术成果保护符合经营所在地法律法规和政策要求。 组织尊重、承认数据安全和个人信息保护相关财产性权益；参与过数据安全和个人信息保护相关知识和技术成果的分享活动。	组织建立和实施了知识和技术成果保护的管理制度；推行鼓励知识和技术成果共享的制度。 组织鼓励开展数据安全和个人信息保护相关知识和技术成果的价值链创新。	组织建立了知识和技术成果的交易及价值创造机制，以价值共享的形式推动知识和技术成果在更大范围共享。 组织定期主动发起多种形式的知识和技术成果共享活动，并纳入绩效考核机制。 组织以多种形式推动数据安全和个人信息保护先进技术的推广及应用。

表 A.1　评价指标与评价等级（续）

一级指标		二级指标		一星级(基础级)	二星级(系统级)	三星级(成熟级)
三	公平运行、竞争和合作	14	构建有效的平台规则	组织按照法律法规、规章制度、标准等的要求，制定可促进数据安全和个人信息保护的平台运营规则。	组织建立和实施了平台规则执行效果评估的管理制度，将效果评估纳入审计等监督环节，以推动平台规则能切实有效执行。 组织定期开展平台规则整体执行效果评估，并优化规则。	组织引入了第三方或权威机构对平台规则整体执行效果评估，吸纳其建议。 组织将平台规则执行效果进行公开，接受利益相关方的监督、评议。
		15	★供应商规则共建及协助	组织按照法律法规、规章制度、标准等的要求，制定了可促进数据安全和个人信息保护的供应商的管理制度。 组织以合同、协议等方式与供应商约定数据安全和个人信息保护相关责任、义务。	组织建立和实施了供应商的合作、监督机制，定期评估和审核供应商资格、供应过程规范性，推动供应商保持数据安全和个人信息保护能力水平。	组织基于自身技术、人员等资源优势，为供应商提供技术支持、应急协助。 组织注重与供应商的长期合作与共赢，协助供应商业提升数据安全和个人信息保护水平。
		16	★公平竞争环境构建	组织在数据处理相关的生产经营活动和参与市场竞争中，遵循自愿、平等、公平、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。	组织建立和实施了有关识别、监控、防止和报告不正当竞争的管理制度。 组织采取了严格的反腐败内部管理制度。 组织积极开展和参与公平竞争的相关培训与活动。	组织在同业伙伴、供应链、投资、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垄断、反不当竞争的行动，在维护行业领域公平竞争中发挥显著作用。
四	消费者权益保护	17	★个人人身、财产利益保护	组织根据法律法规、规章制度、标准等的要求，在产品或服务的设计、开发过程中，采取了降低消费者人身、财产损害的措施。 组织在处理与人身、财产安全密切相关的数据和个人信息前，对处理活动进行影响、风险等评估，并采取了与风险相适应的保护措施。	组织建立了消费者权益保护的技术保障能力和具体工作机制，如识别消费者风险行为的特征库、紧急告知和阻断机制、快速反馈渠道等。 组织在消费者使用产品或服务前，采用生动、简明、准确的表述方式，指导消费者安全、正确使用产品或服务，并说明与使用有关的风险及预防措施，告知消费者遭受或可能遭受人身、财产损害时的反馈渠道及处置方式。	组织建立了侵害消费者权益的违法违规行为特征库，并持续监测、管理违法违规行为。 组织通过消费者人身、财产保护相关的经验、机制进行共享等方式，引导利益相关方共同强化消费者人身、财产保护措施，为同业伙伴、供应链、投资、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。

表 A.1 评价指标与评价等级（续）

一级指标		二级指标		一星级(基础级)	二星级(系统级)	三星级(成熟级)
四	消费者权益保护	18	★消费者投诉及争议处理	组织根据法律法规、规章制度、标准等的要求，建立有效的投诉、争议处置机制，以清晰、显著的方式公示投诉及争议处理的渠道、处理方式及反馈时限。	组织建立并提供了充分和有效的人工客服支持。 组织建立了投诉处理流程，并完善有效的操作规范，形成从投诉到反馈的闭环，避免消费者投诉无人处理、无人反馈等情况。	组织建立和提供消费者处理投诉满意度的反馈途径，记录投诉处理的时间、原因、处理情况等，并定期公开发布投诉处理情况。 组织主动关注合作方、供应商消费者满意度相关情况，针对影响较大的投诉问题进行追踪，并作为下步调整合作的重要考虑要素。
		19	接受中立机构监督	组织依据法律法规、规章制度、标准等的要求，向社会公开数据安全和个人信息保护相关的规则，接受中立社会组织监督。	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，主动接受社会监督。 提供重要互联网平台服务、用户数量巨大、业务类型复杂的组织，成立主要由外部成员组成的独立中立机构，对其数据和个人信息处理活动进行监督。 组织在获得数据安全和个人信息保护的认证后，接受认证机构监督，且无认证被撤销的情况。	组织设立对接中立社会机构监督的岗位，并指定专人负责。 组织向特定中立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，通过向中立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。
		20	消费者教育和意识培养	组织举办、参与过消费者数据安全和个人信息保护知识教育和意识培养的活动。	组织明确了消费者教育及意识培养目标和计划，通过自运营的产品或服务中设置页面等形式开展活动。 组织以提供奖励等方式鼓励消费者积极参与教育和意识培养相关活动。	组织构建了消费者知识教育及意识培训体系，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，共同开展教育和意识培养活动，以推动行业、领域整体形成教育和意识培养合力。

表 A.1　评价指标与评价等级（续）

一级指标		二级指标		一星级(基础级)	二星级(系统级)	三星级(成熟级)
五	公益参与和社会发展	21	慈善捐助和公益事业	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慈善项目的计划。 组织参与过数据安全和个人信息保护公益慈善活动。	组织开展、参与了一系列公益慈善活动并发挥了实质性作用。 组织向数据安全和个人信息研究的中立机构、维权平台、科普中心等进行捐赠。 组织对数据安全和个人信息保护优秀人才、团体、项目设立专门奖项。 组织鼓励员工参加面向社会公众科普的志愿者活动。	组织将数据安全和个人信息保护相关的公益慈善事业作为组织长期文化建设和战略规划予以明确。 组织设立扶助基金或捐赠，帮助弱势群体在数据安全和个人信息保护方面学习、深造、工作等。组织对慈善捐助和公益事业项目的效果进行评估，优化、调整工作的范围、方式等以提升社会责任履行效果。
		22	★活动举办和科普宣传	组织参与、支持能推动数据安全和个人信息保护产业发展、技术创新等方面的活动。 组织参与、支持过数据安全和个人信息保护相关科普宣传活动。	组织以主办方或承办方的身份举办过数据安全和个人信息保护产业发展、技术创新等方面的活动。 组织以主办方或承办方的身份举办过数据安全和个人信息保护相关科普宣传活动。	组织将定期举办数据安全和个人信息保护相关的活动纳入日常工作计划。 组织通过邀请社会公众人物参与、与媒体合作等方式扩大影响面、宣传效果。 组织对数据安全和个人信息保护的相关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。
		23	★行业自治和工作联动	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、行业组织，并参加了其组织的各类活动。 组织积极跟踪国家、地方、行业发布的数据安全和个人信息保护相关政策性文件，了解相关部门组织的各类活动进展。	组织与相关领域内的组织，达成数据安全和个人信息保护相关的工作备忘、合作协议等。 组织积极参与、协助主管监管部门开展数据安全和个人信息保护相关的法律法规宣贯、标准制修订、实践推广、日常监督管理、违法犯罪打击等工作。	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制修订工作。 组织在社会、行业组织中担任相关负责人角色，引导同业伙伴自律自治，共同维护数据安全和个人信息保护良好生态环境。
		24	就业创造和产业投资	组织在力所能及的情况下，设置数据安全和个人信息保护相关的工作岗位。 组织为数据安全和个人信息保护相关学员提供实习机会。 组织为数据安全和个人信息保护相关产品、服务应用和实践的机会。	组织持续提供数据安全和个人信息保护相关岗位。 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平台。 组织在供应商筛选时，从制度、执行等方面有考虑为中小企业、初创企业供应商创造机会。	组织的数据安全和个人信息保护相关岗位需求、人才培养机制呈现规模化特点。 组织积极为具备优秀能力或潜力的人才与企业提供创业机遇或合作机会，与政府、行业组织等共同推进产业创新发展。

数据安全和个人信息保护社会责任绩效总分的计算方式为：

社会责任绩效总分=（所有适用项得分之和/（适用项数 * 9））*100。

注 1：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、发展阶段等因素，24 个二级指标中适用指标数量不足 60%（15 个）的，考虑到评价本身的全面性、公正性等要素，不宜进行评级。如存在不适用指标，则应当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消费者的（业务领域原因），可认为二级指标中的“18 消费者投诉及争议处理”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、发展阶段等无关），不宜认为二级指标中的“22 活动举办和科普宣传”为不适用。

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。

a) 若组织在重点关注项中出现疑似行为或不道德事件，如被媒体或其他公开渠道曝光、被消费者举报等，则在原本所拥有评级的基础上，降低一个等级，若原等级为一星级，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、事件情况不属实，未对利益相关方、消费者等权益产生实质性影响的，可恢复原有评价等级。

b) 若组织在重点关注项上出现严重违法事件，受到政府相应行政处罚，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级。

注 2：评价组织方认定为需停止评价活动的，应注明原因，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、处罚； b) 发生网络安全事件导致数据泄露、篡改、毁损等。
2	公平运行、竞争与合作	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、贿赂以及其他违法违规行为。
3	消费者权益保护	a) 损害消费者个人信息权益； b) 泄露消费者个人信息。
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、网络安全等方面）。

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 5 章至第 9 章内容，就组织履行数据安全和个人信息保护社会责任主题、议题，常见的实践案例如下表，供参考：

表B.1 社会责任履行实践案例

章节	相关行动和期望	示范案例
5 组织治理机制	5.1 核心价值观及发展理念	**示例 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。 **示例 2：**某公司在其公开发布的宣传册、官网主页面等渠道以显著方式展示其隐私保护的核心理念。
	5.2 管理层承诺或声明	**示例 1：**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。 **示例 2：**在某一次行业生态大会上，某公司的 CEO 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。
	5.3 社会责任战略及工作目标	**示例 1：**某上市公司在制定的纲领性文中，用专门的章节阐述了数据安全和个人信息保护的总体方针和安全策略。 **示例 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。
	5.4 实施主体及资源支持	**示例 1：**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。 **示例 2：**某公司从现有的法务、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。 **示例 3：**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。
	5.5 内部宣贯和培训	**示例 1：**某公司根据数据安全相关法律法规要求，根据各业务线及职能部门分工不同，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。 **示例 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、合规实践的宣贯等，同时提供在线课程，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。
	5.6 内部监督和员工激励	**示例 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。 **示例 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。

表B.1 社会责任履行实践案例（续）

章节	相关行动和期望	示范案例
6 合规性、创新性与价值体现	6.1 产品或服务的合规性	**示例 1**:某互联网公司通过第三方评价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展示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。 **示例 2**:某网络安全公司加入数据安全、个人信息保护相关的联盟，在联盟内发表促进数据安全、个人信息保护合规性方面的白皮书，供同行业参考。 **示例 3**: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。在每轮评估过程中针对标准条文逐一进行差距分析，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。 **示例 4**：某数据安全公司按照法律法规、国家标准、行业标准等要求开发了数据安全风险监测的产品，并完成了 2 个客户的部署和应用，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。该公司根据客户的反馈，对产品进行了优化改进。
	6.2 技术的创新性和先进性	**示例 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。 **示例 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。 **示例 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。 **示例 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、先进性的核心期刊论文，获得了 1 项发明专利。
	6.3 用户使用的价值体现	**示例 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。 **示例 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展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展示的内容，并在 3 天内完成 App 升级。 **示例 3**：某邮件服务供应商给用户提供邮箱服务，用户选择注销邮箱时，该供应商在反馈给用户的界面中询问用户是否保留邮箱名等信息以备后续重新使用，如果不保留可以彻底删除。用户确认彻底删除信息后，供应商对存储在库中的邮箱名进行了删除处理。
	6.4 社会治理的价值体现	**示例 1**：某监管机构决定对管辖区内的 10 家互联网公司开展数据安全检查，使用了某数据安全公司的检查工具，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。 **示例 2**： 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上线，方便用户及时向监管部门反馈问题。
	6.5 数字包容与特殊保护	**示例 1**：某 App 在收集个人信息时，提供了一键按钮，转换到老年人模式，在老年人模式下，文字字体更大，同时把需要特别注意的文字加粗，帮助老年人快速的理解收集个人信息的用途和范围。 **示例 2**：某 App 在收集个人信息时，对个人信息处理的说明文字，提供了中文、英文、法语等共 30 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。 **示例 3**：某用于在线教学的智能终端提供了家长守护的功能，家长可以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、娱乐 App。

表B.1 社会责任履行实践案例（续）

章节	相关行动和期望	示范案例
7 公平运行、竞争与合作	7.1 数据处理规则的透明性	**示例 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 与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。 **示例 2：**某科技公司，就向客户提供的信息技术服务中涉及的的信息核验、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。
	7.2 知识和技术成果共享	**示例 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、教材与讲义等内容建设成数字知识库，面向社会开放共享。 **示例 2：**某文化创意设计产业博览会，将诸多知名艺术家、自由创作者的优秀作品，利用区块链等技术构建安全、可信的数字艺术品平台。
	7.3 构建有效的平台规则	**示例 1：**某地方政府惠民服务平台，针对餐饮、教培、美容等行业中，市民关心的预付款的资金安全问题，开发了资金监管体系、商户评价标准等。 **示例 2：**某银行，对供应商中涉及假冒伪劣商品、违规用户营销等行为，一经确认，马上除名且永不录用，并在银行官网公示。
	7.4 供应商规则共建及协助	**示例 1：**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，并在供应商招标与管理考核中，加大数据安全、技术创新等指标的权重。 **示例 2：**某银行，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。
	7.5 公平竞争环境构建	**示例 1：**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、市场资源支持以及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、数据技术等方面提供“终身免费培训计划”。 **示例 2：**某投资公司，对投资企业及其高管，定期开展头脑风暴及反垄断培训，并聘请业界专家、律师等组成委员会，就数据的跨领域应用可行性、安全性及是否涉及垄断风险出具背调报告。

表B.1 社会责任履行实践案例（续）

章节	相关行动和期望	示范案例
8 消费者权益保护	8.1 个人人身、财产利益保护	**示例 1：**设立“叫醒热线”，当识别到消费者财产利益等存在风险时，通过打电话、发提醒、在线问答等形式唤醒消费者。 **示例 2：**在 App 等客户端设立“消费者权益保护”频道，用户可以查看和管理“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及获取与其权益相关的功能或服务。 **示例 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。
	8.2 消费者投诉及争议处理	**示例 1：**实现 7*24 全天候在线客服，承诺 3 分钟内响应消费者咨询。对消费者投诉，保证 48 小时内响应。 **示例 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、求职咨询、道具使用等，方便消费者快速定位及解决问题。 **示例 3：**配备充足的人工客服团队，保证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、账号安全反馈组等，确保人工客服能够准确、迅速的帮助消费者解决问题。 **示例 4：**通过设置匿名投诉、个人信息脱敏展示等功能，保护投诉者的隐私，避免侵扰投诉者私人生活的安宁。
	8.3 接受中立社会组织监督	**示例 1：**在 App 等客户端设置“规则中心”，集中、统一的展示平台内的规则情况、规则更新情况及规则解读等，便于外部机构或人员查阅及监督。 **示例 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、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； **示例 3：**定期公示组织在提升数据安全和个人信息保护能力方面的采取的措施及取得的成果； **示例 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。
	8.4 消费者教育和意识培养	**示例 1：**在 App 等客户端设置在线学习专区，提升消费者权益保护意识。用视频、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。 **示例 2：**在 App 等客户端设置“安全学院”聚合全国 30 多个省、市、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。 **示例 3：**在 App 等客户端设置“全民个人信息保护意识试炼”，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。

表B.1 社会责任履行实践案例（续）

章节	相关行动和期望	示范案例
9 公益参与和社会发展	9.1 慈善捐助和公益事业	**示例 1:**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、工作； **示例 2:**设立专门奖项，向数据安全和个人信息保护优秀人才、团体、项目等进行奖励；
	9.2 活动举办和科普宣传	**示例 1:**参与或承办国家、行业或地区的数据安全或个人信息保护的宣传活动； **示例 2:**通过 APP 广告页面宣传数据安全或个人信息保护活动；
	9.3 行业自治和工作联动	**示例 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。 **示例 2：**协助某监管部门对侵害个人信息权益的黑色产业链进行打击，并提供了多条线索。
	9.4 就业创造和产业投资	**示例 1:**与行业学会、高校、研究所等机构合作开展数据安全或个人信息保护研究课题； **示例 2:**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。

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

组织宜定期（通常为每年度）对数据安全和个人信息保护社会责任进行回顾和总结，由相关责任部门、人员形成数据安全和个人信息保护社会责任报告，并采取适当形式发布以披露社会责任履行情况。

数据安全和个人信息保护社会责任报告可以是单独的报告，也可以是组织整体社会责任报告的一个独立部分，报告的主体内容宜参考本文件第 5 章至第 9 章中的主题和议题（共 5 大主题，24 个议题），根据组织开展业务、消费群体、利益相关方等的特点，选择适当的结构以增加报告的可读性、传播效果。必要时，在编制社会责任报告的阶段可邀请第三方机构、外部专家等参与，以提升报告内容的完备性、权威性。

以下是通用的数据安全和个人信息保护社会责任报告模板，仅供参考：

XXXX 公司数据安全和个人信息保护社会责任报告

一、关于本报告

内容参考：展示企业对社会责任的理解、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、该报告披露信息及数据的时间维度、更多信息及投诉建议渠道等。

二、企业 CEO 致辞

内容参考：以第一人称口吻阐述过去（一年）内，企业在社会中扮演的社会角色，展示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“交汇点”，践行数据安全和个人信息保护社会责任的方向、途径。

三、社会责任履行整体情况

1、企业简介

内容参考：展示企业官方简介，以及采取何种组织架构、管理体系等履行企业社会责任。

2、关键绩效

内容参考：参照本文件第 5 章至第 9 章中的主题和议题（共 5 大主题，24 个议题），归纳效果突出的社会责任相关活动，予以重点展示。

3、高光时刻

内容参考：展示数据安全及个人信息保护方面的科技成果、专利、各类奖项，以及社会活动中被高度肯定、被表彰等的案例。

4、评级结果（如有）

内容参考：如果参与过数据安全及个人信息保护社会责任评级，可说明评级背景、评级依据、评级机构、评级结果等。

XXXX 公司数据安全和个人信息保护社会责任报告（续）

四、社会责任履行详细情况

该部分可参考本文件第 5 章至第 9 章中的主题和议题（共 5 大主题，24 个议题）框架进行编排，也可以根据自身企业文化、业务特点、用户类型等进行框架设计。该部分内容可参考本文件第 5 章至第 9 章中的内容予以归纳、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，可以详述典型案例，以丰富报告内容。

内容参考：

1、组织治理和内部管理

描述责任履行情况。

……

5、数字包容与特殊保护

描述责任履行情况。

【典型案例】

例如：介绍在数字包容与特殊保护方面产品上线的新功能，以及其应用的效果，用户的评价等。

……

五、总结与展望

内容参考：展示所总结的数据安全和个人信息保护社会责任的履行经验、成效，描绘下一步（下一年度）开展的工作、活动计划以及目标等。

六、信息反馈

内容参考：展示并公开企业对公众在其数据安全和个人信息保护社会责任工作的调研问卷、反馈及建议渠道。

七、附录（可选）

内容参考：展示识别、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，例如有关的出版物、发布成果、网站链接、新闻报道、活动纪实、证书证明等内容。

参 考 文 献

[1] 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）

[2] 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）

[3] 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）

[4] 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）

[5] 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）

[6] 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）

[7] GB/T 36001-2015 社会责任报告编写指南

[8] GB/T 36002-2015 社会责任绩效分类指引

[9] GB/T 39604-2020 社会责任管理体系 要求及使用指南

[10] GB/T 39626-2020 第三方电子商务交易平台社会责任实施指南

[11] RB/T 178—2018 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/T3837-2021 信息通信行业企业社会责任评价体系

[15] T/ISC0002-2020 互联网企业社会责任报告编写指南

[16] T/CESA16003-2021 电子信息行业社会责任治理评价指标体系