ICS 35.030
CCS L 80

T/CCIA

中 国 网 络 安 全 产 业 联 盟 技 术 规 范

T/CCIA XXX—XXXX

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

（征求意见稿）

2022-09-06

XXXX－XX－XX 发布　　XXXX－XX－XX 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、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、完美世界（北京）软件科技发展有限公司、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、启明星辰信息技术集团股份有限公司、上海冰鉴信息科技有限公司、上海安全至尚科技有限公司、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、孟洁、张朝、武扬、王海棠、薛颖、刘玉红、严孝馨、刘金利、周瑞群、李超然、王昕、张艺伟、张栌文、张雪、彭晋、胡娴、黄蓉、葛梦莹、孙硕、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和实施相关活动提供指南,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组织社会价值,最大限度地致力于可持续发展。

本文件适用于处理数据的组织,还适用于第三方评价组织在履行数据安全和个人信息保护社会责任的水平。在应用本文件时,建议组织充分考虑自身规模、性质、行业特征等。

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

RB/T 178—2018 合格评定 社会责任要求

RB/T 179—2018 合格评定 社会责任评价指南

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

组织参照GB/T 36000—2015第5章提出的原则，根据第5-9章中的主题，确定数据安全和个人信息保护社会责任事项及优先事项。第5-9章中的主题并不完全适用于所有组织，组织在满足适用的法律法规要求的基础上，可结合所在地区的经济、社会和环境发展水平、自身特点和发展阶段及利益相关方期望，识别确定每项社会责任主题中适用的具体内容。

组织或第三方可根据附录A给出的评价方法，识别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成熟度。

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，是指组织所担负的历史使命、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来讲至关重要。

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：

——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，体现数据安全和个人信息保护在产品或服务的设计需求中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。公开的承诺和说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：

——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，并选择以承诺、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,一般包含:社会责任方针、目标、方案和措施。工作目标，是指组织依实际情况及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：

——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在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，是指组织中实际实施社会责任工作的部门或人员。资源支持，是指组织为推动社会责任工作提供财务、人力、环境等资源。以上对于数据安全和个人信息保护社会责任相关工作的实施层面来说是必不可少的。

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：

——指定具体的高管担任数据安全和个人信息保护社会责任工作的牵头人。

注 1：担任牵头人的高管职务、姓名、联系方式至少在组织层面予以公开。

——设立专门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：选择设立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,包括发布包含数据安全和个人信息保护的社会责任报告等形式。

——指定相关部门或人员就社会面的数据安全和个人信息保护得相关问题积极沟通回应,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。

注 3：获取社会面的信息渠道包括：新闻媒体报道、互联网社交、信息发布等平台的热议话题、设立的投诉、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条令、政策、方针、活动等使组织内部透彻理解，以达到思想意识的一致。内部培训，是指组织以自身力量对员工通过各种方式、手段使其在知识、技能、态度等诸方面有所改进，以达到预期标准。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意识和认可度。

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：

——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）开展进行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，如牵头人、相关部门负责人、社会责任报告编制人进行重点培训。

注 2：外部专家宜具备在履行社会责任方面的经验、参与过数据安全和个人信息保护的社会公益活动，优先选择受到权威组织表彰和社会广泛肯定的专家。

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，对员工的需要予以不同程度的满足或者限制，以激发员工的需要、动机、欲望，充分挖掘潜力、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：

——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置。

——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，并对取得积极社会反响的予以奖励。

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

产品或服务的数据安全和个人信息保护合规性是在产品或服务生命周期符合法律法规、监管机关部门规章、相关产品或服务强制性标准，以确保产品或服务的质量，降低合规性风险。 合规性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、 第三方评估、第三方审计、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：

——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。

——评估或审计的依据还包括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。

——引入独立第三方评估后，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合规性。

——发布数据安全和个人信息保护相关的合规白皮书（或说明书、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、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，不断完善数据安全和个人信息保护合规水平。

6.2 技术的创新性和先进性

6.2.1 议题描述

产品或相关技术服务的创新性是基于当前技术发展水平下，能更高效、低成本解决特定问题，或能提升生产力水平或具备对经济发展、社会进步有促进作用，能通过研究成果转化、标准制定等为实现产品或服务模式创新在功能和性能上有突破性进展，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：

——鼓励构建创新性及先进性评价标准和指导方针。

——组织内部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。

——为技术创新提供学术研究、国际交流等方面的有利条件。

——搭建同业交流机制或平台，推动创新性标杆组织进行内部分享或培训，交流分享创新性方法。

——推动进行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的评比、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的产品或服务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。

——对具备创新性、先进性且产业实践效果良好的产品或服务，进一步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、获取的国家发明等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技术或服务,创立行业的知名品牌,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

根据处理的数据的目的，向用户提供所需的产品或服务，为用户的数据和个人信息提供保护，并且为用户提供相关数据和个人信息处理的权益。

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：

——用户提供数据后即可获得与所处理数据相关的服务。

注：不为用户使用服务设置不合理的条件，如捆绑其他服务、增加收集数据的类型、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、服务设置为基础服务的一部分。

——通过不断优化数据处理的流程、步骤、时机、场景，减少了收集数据的类型和保留时间，增加了对脱敏、去标识化、匿名化后数据的处理。

——在不影响用户权益的前提下，通过优化算法等方式挖掘数据价值，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、数据处理活动审计。例如，可以查询、复制、更正、删除、迁移等，可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，定期评价投诉、举报的数量、处理率、处理评价，以优化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，以支撑监管机关开展社会治理活动，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。主要表现形式有产品或服务使用指引、投诉举报处理机制、应急处理机制、为监管机关提供社会治理相关技术、服务支持等。

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：

——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。

——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。

——向社会面公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：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、服务。

——对可能造成用户数据安全和个人信息保护不利影响的行为、信息等能快速响应、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技术活动，使得多元人群能公平、自由的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、更严格的个人信息保护方案、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：

——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和服务，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。

——参与未成年人、老年人、残障人士相关数据安全和个人信息保护标准制定，形成行业协同。

——投入资源推广特殊人群使用的产品或服务，以及引导其关注使用产品或服务时保护个人信息。

——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。

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

处理规则的透明性是指个人信息处理者应以适当方式公开其对个人信息处理的处理规则，明示处理的目的、方式和范围，从而确保个人信息被处理的情况对于个人信息处理活动的相关方是清晰透明、容易获知的。对于其他的数据处理者，也可根据其实际情况，向利益相关方适度公开数据处理的规则，以增进其信任，便于其进行监督、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：

——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 第 5 章。

——建立与合作方沟通的机制，能就数据处理的目的、方式、范围等规则进行及时沟通、审核确认。

——向利益相关方提供数据处理规则问询、答疑的渠道，针对复杂、难懂、关注度高的数据处理规则，可进一步解释说明以增进理解。

——数据处理规则可能影响到利益相关方重大权益的，需采取单独告知等方式重点说明，确保对方能够理解后做出巨顶。

——数据处理规则影响范围十分广泛，或有关法律法规规定的，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。

7.2 知识和技术成果共享

7.2.1 议题描述

知识与技术成果主要表现形式为产权，产权既包括有形产权和知识产权,也包括土地和其他有形资产的权益,版权、专利权、地理标志权及其他权利的权益。承认数据安全和个人信息保护专有产权既可促进投资、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：

——实施能够推动尊重技术成果和知识的政策、做法和管理程序。
——开展恰当的调查,以确信其享有知识和技术成果的使用权或处置权。
——不参与侵犯数据安全和个人信息保护相关知识和技术成果共享的活动,包括滥用支配地位、假冒和盗版。
——对所获得或使用的知识和技术成果共享支付合理的补偿。
——在行使并保护自身由知识和技术成果共享时,考虑社会期望、人权及个人的基本需求。
——鼓励开展知识及成果的价值链创新，并提升知识及及技术成果在价值链可持续性和先进性。
——推动形成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及技术成果共享。
——可自行或与其他组织合作，推动探索多种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；
- 向开源社区等分享部分源代码；
- 向具有法定职能的组织共享威胁、事件情报。

—促进可广泛适用的数据安全和个人信息保护先进技术推广及应用，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

评估平台规则的有效性是为了评估平台在推动此项工作中的各项程序、制度、细则、规定等的落实情况，明晰并评估当前规则落地现状，为后续的各项程序、制度、细则规定等提供可下一步规则的优化空间，同时，作为平台主体方，定期对外公布平台规则的执行效果可提升外部平台的品牌度及内部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：

——组织在进行平台运营时所制定的平台规则，需关注相关法律法规的要求，引导平台中的组织、个人等更好地执行保护数据安全和个人信息保护的策略、采取更为有效的安全措施。
——将平台规则执行效果纳入到合规审计等监督环节的流程中，以推动平台规则能切实有效执行。
——形成适应于社会责任绩效的计算框架用以衡量平台规则的执行效果,推动执行效果在计算框架内的执行规则、评估标准、评估规范落地。
——开展定期的整体执行效果评估，并形成根据评估效果优化的流程与制度，以便于正确评估执行效果水平。
——为保证执行效果评价客观性，效果评估流程中，评审过程中引入三方或权威机构的咨询建议，保证平台规则执行效果的客观性；
——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。

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：

——建立供应商管理规范，公开透明的供应商选择标准，明确供应商应符合的安全基线、淘汰指标等。

——设立必要的监督机制，避免利用市场优势地位向供应商滥收通道费等不合理费用，避免商业贿赂和其他腐败行为，维护供应链各企业的公平竞争。

——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进行审批、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；

——定期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，不符合条件的应执行退出、替换机制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，并未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

在互联网平台经济迅速发展的背景下，公平竞争始终是发挥市场在资源配置中决定性作用的前提。构建公平竞争环境，营造优胜劣汰的市场氛围，能够激励企业更加有效率地投资、创新，激励企业以更低的价格、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。在公平的竞争环境及宽松的政策下，互联网平台经济得以蓬勃发展。但与此同时，部分企业利用在资本、数据、流量等方面积累的优势地位，破坏公平竞争环境，客观上阻碍了新业态的创新和发展。反垄断、反不正当竞争旨在防止资本无序扩张，促进新业态有序发展、提升核心竞争力。因此，需要企业共同履行构建公平竞争环境的社会责任。

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：

——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、知识产权相关的法律法规和商业道德，将公平竞争作为企业治理、生产经营和一切商业活动的行为准则。

——杜绝以任何形式开展不正当竞争，杜绝采取任何形式的数据不正当竞争行为，如：

- 通过数据、算法、互联网平台规则等方式达成垄断协议；
- 通过非法或不正当手段处理互联网平台数据（包括互联网平台用户个人信息）；
- 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；

- 阻止其他第三方向监管部门投诉；
- 其他不正当竞争行为。

——重视数据知识产权的管理和保护，制定数据知识产权内部管理制度，在商业活动中杜绝侵犯数据知识产权的行为。

——制定并实施企业内部反腐败制度，对领导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。

——建立员工合规培训制度，通过定期合规培训等方式，提高员工在互联网平台经济背景下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；

——拥护政府部门构建互联网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，积极配合政府部门对相关的反垄断、反不正当竞争的调查和执法行动。

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、财产利益保护，是指提供的产品或服务不会为消费者带来无法接受的人身、财产损害风险，进一步的能够主动识别风险，防范损害消费者财产利益的行为发生。损害成因既包括正常使用，也包括可预见的不当使用。

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：

——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更高要求，组织不宜仅仅满足于较低的要求。

——产品或服务设计开发过程中，宜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：

- 确保在正常和合理可预见的使用情况下,提供的产品或服务,对消费者的人身、财产是安全的；
- 考虑并顾忌消费者的需求差异、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）来确保对产品或服务的合理设计；
- 评估产品或服务在所有使用阶段和条件下可能致使的人身、财产损害风险；
- 通过遵循以下优先顺序来降低风险:首先考虑采用完全消除风险的安全设计;然后考虑增设保护性装置;最后才考虑向消费者提供警示信息。

——产品或服务的使用过程中，宜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，宜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。

——消费者遭受或可能遭受人身、财产损害的，组织宜为消费者提供简捷、迅速的反馈渠道及处置方式。

——在消费者使用产品或服务前，组织宜：

- 指导消费者安全的使用产品和服务；
- 结合产品和服务的具体情况，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。

——除使用文字信息外，还宜尽可能使用符号、图片向消费者传递告知重要信息。

——避免使用敏感个人信息。如产品或服务使用敏感个人信息的，应遵守相关法律法规的要求，并脱敏展示。

——产品或服务使用过程中，如出现重大漏洞，或者包含有误导或错误的信息，应中止提供服务，通知受影响的消费者并采取补救措施。

——建立能够识别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，是组织在出售或提供产品或服务之后，所采取的处理消费者反馈的具体机制。

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：

——以清晰、显著的方式公示投诉渠道、处理方式及反馈时限。

——公示的投诉渠道应有效且高效，尽可能从组织内部实现处理渠道的转换，不得频繁要求消费者更换投诉方式。

——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，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，消费者可通过该途径反馈意见或建议，便于组织定期评审并改进。

——提供充分和有效的人工客服支持。

——处理投诉时不向消费者收取不合理费用，不要求消费者放弃其法律上的权利。

8.3 接受中立社会组织监督

8.3.1 议题描述

接受中立社会组织监督是指通过主动披露等方式使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，针对社会组织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：

——向社会公开数据安全和个人信息保护政策，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。

——组织由外部成员组成的团队，对数据和个人信息处理活动进行监督。

——指定企业内负责数据安全和个人信息保护的人员，使其承担与社会（中立）组织对接、遵守相关安全保护措施和适用的法律法规的责任，并披露其联系方式。

——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收认证机构监督。

——赋予社会（中立）组织对企业在数据安全和个人信息保护措施进行核实和质疑的权利，如果质疑得到证实，组织应及时纠正不当行为。

——向社会（中立）组织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。

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自己的权利和责任，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：

——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。
——面向消费者就有关数据安全和个人信息保护的适用法律法规、投诉举报途径、消费者保护机构与组织等开展教育活动。
——面向消费者就产品和服务相关的数据安全和个人信息保护功能等开展教育活动。
——面向消费者就与使用有关的风险信息以及所有必要的警示信息开展教育活动。
——面向消费者就相关数据和个人信息泄露导致的风险和案例开展教育活动。
——面向消费者就使用产品或服务过程中注重保护他人的数据、个人信息开展教育活动。

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公益参与，支持政府、社会团体等机构在数据安全和个人信息保护开展活动或扩大影响力，差异化完善组织在数据安全和个人信息保护的责任范围。

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：

——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：

- 筹建或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；
- 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（尤其时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。

——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，提升社会对相关前沿技术和自我保护的了解，从而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：

——为举办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 行业自治与工作联动

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，提升社会整体数据安全或个人信息保护的氛围和治理能力。

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：

——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，以扩大工作的范围和频率。

——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，可进一步明确进行工作支撑的部门或人员，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

组织为数据安全和个人信息保护的产业链提供支持，包括：上下游协同发展、人才培养、技能认证等。

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：

——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的实习，参与有偿合作项目的，给与适当的劳动报酬。

——进行外包决策时，不影响服务质量的前提下，为新的数据安全和个人信息保护方向的外包服务商，尤其是中小企业、初创企业外包服务商创造机会。

——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

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评价等级。评价指标包括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，每项二级指标分值区间为5分，即：一星级：1-5分,二星级：6-10分，三星级：11-15分，不满足基本要求该项不得分。评估主体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管理水平进行最终评价，以确定整体评价等级。不同等级评价依据如下：

a) 一星级：遵守法律法规要求，满足数据安全和个人信息保护社会责任的基本管理要求。本级别的总分不得少于24分；

b) 二星级：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项指标中至少80%以上满足标准要求，即80%以上的二级指标项至少得6分以上。其中“★”项为必选指标，该项必须达到6分及以上。

c) 三星级：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，在五项核心主题的一项或多项指标上不断实现更高的社会责任绩效。要求24项指标至少50%以上满足指标要求，即50%以上的指标子项至少得11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	组织遵循已成文并广泛推广的核心价值观、发展理念，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。	能够影响供应链、投资以及客户等与自身经营有实质性关联的领域。
		2	★管理层承诺或声明	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，并选择以承诺、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。	组织形成对管理层承诺与担责的评估体系，定期对管理层的承诺履行进行评价，促进管理层履行承诺并担责
		3	★社会责任战略及工作目标	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在组织的社会责任战略和工作目标中。	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。	a) 持续改进数据安全和个人隐私保护社会责任绩效，结合组织的发展更新优先事项。 b) 能够影响供应链、投资以及客户等与自身经营有实质性关联的领

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)
						域
		4	★实施主体及资源支持	a) 指定具体的高管担任数据安全和个人信息保护社会责任工作的牵头人； b) 设立专门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。	a) 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，包括发布包含数据安全和个人信息保护的社会责任报告等形式； b) 指定相关部门或人员就社会面的数据安全和个人信息保护得相关问题积极沟通回应，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； c) 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。	a) 至少有 3 年的全面、客观、可追溯、有可比性的数据安全与个人隐私保护的社会责任管理绩效记录，记录应能证明数据安全与个人隐私保护的社会责任绩效的持续改进，以反映其管理制度或体系的有效运行； b) 建立了与数据安全与和人隐私保护的社会责任相关的经济或非经济措施。
		5	★内部宣贯和培训	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。	a) 在组织内部定期（每年至少一次）开展进行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； b) 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，如牵头人、相关部门负责人、社会责任报告编制人进行重点培训。	a) 建立了对内部人员的数据安全与个人信息保护的社会责任的完整培养体系，并对该体系持续改进； b) 能够影响供应链、投资以及客户等与自身经营有实质性关联的领域。
		6	内部监督和员工激励	a) 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置。 b) 鼓励相关人员积极学	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，并对取得积极社会反响的予以奖励。	a) 组织内部成立数据安全和个人信息保护社会责任工作的部门，用于接收内部人员反馈的监督意见，确保相关建议的处置； b) b) 能够影响供应链、投资以及客户等

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）
				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。		与自身经营有实质性关联的领域。
二	合规性、创新性、价值体现	7	★产品或服务的合规性	产品或服务生命周期符合法律法规、监管机关部门规章、相关产品或服务强制性标准。	组织发起或引入第三方产品或服务的评估或审计系统，取得产品的合规认证。定期发布数据安全和个人信息保护方面的合规白皮书。	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。及时对安全事件进行发现及响应，并不断完善相关合规水平。
		8	技术的创新性和先进性	技术创新的取得和使用符合相应的法律法规和政策的要求。针对亟待解决问题，获得专利、权威机构认证、三方背书等系列合规认可。	采取必要的管理机制积极培养自身的创新能力。	鼓励构建创新性及先进性评价标准和知道方针。促进行业数据安全及个人信息保护的水平提升，贡献技术能力、专业服务及产品。
		9	用户使用的价值体现	用户的使用过程和服务响应结果符合相应的法律法规。利益相关方提供数据或用户提供的个人信息在符合法律法规的情况下获得处理数据相关的合法服务。	根据处理的数据的目的，向用户提供所需的产品或服务，为用户的数据和个人信息提供保护，并且为用户提供相关数据和个人信息处理的权益。	积极增强数据的安全性，提高用户的体验感。与同行积极促进数据安全及个人信息保护的各类措施。
		10	★社会治理的价值体现	社会治理的各项活动均符合相应的法律法规和政策的要求。	建立产品或服务使用指引、投诉举报处理机制、应急处理机制、为监管机关提供社会治理相关技术、服务支持等。积极履行社会责任，营造安全的网络空间环境。	与同行业的其它平台共同参与国际、国家、行业标准的编写。加入行业/产业联盟，推进数据安全按及个人信息保护生态建设和发展。
		11	★数字包容和特殊保护	按照法律法规和政策的要求，开展各种技术活动，使得多元人群能公平、自由的获取和享受技术变革和产业发展提供的便利。	建立为多元人群提供更便利的数据安全服务、更严格的个人信息保护方案、为多元人群提供更全面的和公平的社会环境。如建立严格的招聘程序，杜绝童工的招聘，提供完善的管理制度保障未成年的合法权益等。	积极响应国家的号召，与同行业积极促进数据包容的发展，同时建立对特殊人群更加完善的管理制度。
三	公平运行、竞争和合作	12	★数据处理规则的透明性	按照经营所在地关于数据处理规则披露的法律法规和政策要求，完整、真实、准确披露信息处理的规则，明示信息处理的目的、方式和范围。	建立和实施各利益相关方的个人信息处理规则披露的管理制度，确保个人可以便捷、清楚地知悉其个人信息被处理的情况。	在同业伙伴、供应链、投资以及客户等与自身经营有实质性关联的领域积极影响、合作或共同行动。

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)
		13	★知识和技术成果共享	符合经营所在地关于知识与技术成果保护的法律法规和政策要求,尊重、承认、保护数据安全和个人信息保护专有产权。	a) 建立和实施有形产权和知识产权保护的管理制度,实现对知识和技术成果的尊重和保护; b) 鼓励开展知识和技术成果共享和创新,推动知识及技术成果的可持续发展。	在同业伙伴、供应链、投资以及客户等与自身经营有实质性关联的领域积极影响或合作,实现本指标价值的共同行动。
		14	★构建有效的平台规则	按照法律法规和政策的要求,拟定平台运营所需规则,评估开展工作过程中各项程序制度、细则规定的落实情况。	建立和实施平台规则执行效果的计算框架和评估规范的管理制度,定期评估整体执行效果,并将其纳入监督环节,以明晰平台开展活动过程中各细则的开展和落实情况。	鼓励平台公开平台规则执行的评估结果,在同业伙伴、供应链、投资以及客户等与自身经营有实质性关联的领域积极影响或合作。
		15	★供应商规则共建及协助	按照法律法规和政策的要求,建立供应商的管理规范和监督机制。	建立和实施供应商的合作管理机制和应急响应机制,定期评估和审核供应商资质、排查安全风险。	a) 积极实现供应链中基于预防纠正原则的风险最小化;注重与供应商的长期合作与共赢; b) 在同业伙伴、供应链、投资以及客户等与自身经营有实质性关联的领域积极影响或合作,实现本指标价值的共同行动。
		16	公平竞争环境构建	在数据处理相关的生产经营和市场竞争活动中遵守竞争、知识产权相关的法律法规,将公平竞争作为企业治理、生产经营和一切商业活动的行为准则。	a) 建立和实施有关识别、监控、防止和报告不正当竞争的管理制度; b) 重视数据知识产权保护和企业反腐败的内部管理制度; c) 积极开展和参与公平竞争的相关培训与活动。	在同业伙伴、供应链、投资以及客户等与自身经营有实质性关联的领域积极影响或合作,杜绝任何形式的不正当竞争行为。
四	消费者权益保护	17	★个人人身、财产利益保护	a) 遵循相关法律法规要求; b) 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更高要求,组织不宜仅仅满足于较低的要求; c) 避免使用敏感个人信	a) 产品或服务设计开发过程中,采取措施最大程度的降低消费者人身、财产的风险; b) 产品或服务的使用过程中,宜建立能够识别消费者风险行为的特征库; c) 当识别消费者存在风	a) 建立能够识别违法违规行为的特征库,并持续监测、打击违法行为; b) 除使用文字信息外,还宜尽可能使用符号、图片向消费者传递告知重要信息;

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）
				息。如产品或服务使用敏感个人信息的，应遵守相关法律法规的要求，并脱敏展示。	险行为，组织有适当的措施应对； d) 在消费者使用产品或服务前，组织将服务或产品使用中存在的风险详细告知。 e) 产品或服务使用过程中，如出现重大漏洞，或者包含有误导或错误的信息，应中止提供服务，通知受影响的消费者并采取补救措施。	
		18	★消费者投诉及争议处理	a) 以清晰、显著的方式公示投诉渠道、处理方式及反馈时限； b) 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。 c) 处理投诉时不向消费者收取不合理费用，不要求消费者放弃其法律上的权利。	a) 公示的投诉渠道应有效且高效，尽可能从组织内部实现处理渠道的转换，不得频繁要求消费者更换投诉方式； b) 提供充分和有效的人工客服支持。	a) 建立投诉处理满意度的反馈途径，消费者可通过该途径反馈意见或建议，便于组织定期评审并改进； b) 建立投诉处理库，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。
		19	接受中立社会组织监督	按照法律法规和政策的要求，社会组织或个人对组织的各类措施及成果进行评估。	社会组织建立完善且全面的信息主动披露系统，中立组织组建团队及体制对数据和个人信息实施监督，并定期公布审计结果。企业及员工应积极获取数据安全和个人信息保护的相关认证。	不同中立社会组织之间积极配合，实现更好的社会监督。中立组织积极配合国家要求，鼓励并推动组织评估的完善。
		20	消费者教育和意识培养	按照法律法规和政策的要求，实施消费者教育和意识培训的一系列活动宣传及演讲等。	实现完善的消费者教育及意识培训内容构建。多方面、多角度的开展数据安全和个人信息保护的教育活动。	同国家、其它相关企业及消费者等实施不同程度的合作，进一步完善消费者教育及意识培训的内容，同时对完善的内容进行公示，获取不同建议或贡献他人。
五	公益参与和社会发	21	慈善捐助和公益参与	符合经营所在地的公益慈善的法律法规，包括对慈善捐助、数据安全维护等的支持与捐赠。	据本企业经营的范围，通过慈善捐助和公益参与，支持政府、社会团体等机构在数据安全和个人信息保护开	将本企业的经营活动与公益组织相结合或与其它不同类型或同类型的企业进行合作，扩大企业对社会的

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)
	展				展活动或扩大影响力，差异化完善组织在数据安全和个人信息保护的责任范围。	实质性影响，进而符合社会责任战略及目标。
		22	★活动举办和科普宣传	积极支持、举办和参与个人信息保护和数据安全的相关活动，开展科普宣传活动，增强组织在数据安全或个人信息保护领域的透明性。	a) 为举办个人信息保护和数据安全相关活动提供必要的资源支持； b) 自行组织或主动参与个人信息保护和数据安全的相关活动与科普宣传，并定期评估、记录总结和报告活动效果。	积极提升企业员工、社会公众的数据安全和个人信息保护素养，在同业伙伴、供应链、投资以及客户等与自身经营有实质性关联的领域积极影响或合作，实现本指标价值的共同行动。
		23	★行业自治与工作联动	积极支持和参与行业自律、治理行动，通过联合相关领域组织、配合主管监管部门工作等形式，提升社会整体数据安全或个人信息保护的氛围和治理能力。	a) 积极参与和响应数据安全与个人信息保护的自律和治理活动； b) 与相关领域的组织形成合作； c) 协助有关部门开展数据安全和个人信息保护的相关工作； d) 将必要的工作管理进一步明确并纳入日常管理和考核。	积极提升相关企业的数据安全和个人信息保护素养，在同业伙伴、供应链、投资以及客户等与自身经营有实质性关联的领域积极影响或合作，共同增强社会的个人信息保护与数据安全意识。
		24	就业创造和产业投资	在经济可行的前提下，为个人信息保护或数据安全保护的企业和人才提供资金支持、工作或合作机会，搭建安全研究项目产品或实验平台。	建立和实施安全研究平台建设、人才培养、项目外包和企业合作等战略性投资的策略和管理制度，并定期评估、记录和报告。	积极培养人才、构建安全研究平台、共享安全研究资源，为具备优秀能力或潜力的人才与企业提供工作或合作机会，共同推进数据安全研究领域与行业发展。

A.2 重点关注事项

本文件将企业社会责任核心主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) 若企业在重点关注项中出现可疑行为或不道德事件，受到相关平台或机关的曝光，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，则停止评价活动。

b) 若企业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或被媒体曝光，造成恶劣社会影响，应停止评价活动。

注：评价主体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	核心主题	重点关注事件

1	消费者权益保护	伤害消费者，泄露消费者个人信息等隐私信息
2	公平运行、竞争与合作	a） 侵犯知识产权行为 b） 发生不正当竞争行为 c） 管理者存在违法行为
3	公益参与和社会发展	妨碍社区稳定（如公共安全等方面）

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，就其提出的组织履行数据安全和个人信息保护社会责任事项，常见的实践案例如下表：

表B.1 社会责任履行实践案例示例

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：**在公开报告或者内部文件中阐述关于数据安全及个人信息保护相关的愿景、目标。
	5.2 管理层承诺或声明	**示例 1：**在社会责任报告中通过一份单独的董事长致辞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。
	5.3 社会责任战略及工作目标	**示例 1：**制定并发布纲领性文件，阐述数据安全和个人信息保护的总体方针和安全策略。
	5.4 实施主体及资源支持	**示例 1：**建立数据安全和个人信息保护委员会，并由管理层担任负责人； **示例 2：**指定专门部门或团队负责数据安全和个人信息保护社会责任履行披露工作； **示例 3：**规划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。
	5.5 内部宣贯和培训	**示例 1：**建立全面的数据安全和个人信息保护管理制度体系，加强各个环节的数据安全和个人信息保护工作； **示例 2：**对数据安全和个人信息保护关键岗位的工作人员进行重点专门培训，并建立安全意识考核机制。
	5.6 内部监督和员工激励	**示例 1：**对数据安全和个人信息保护责任对应的相关惩戒措施进行书面规定，如一旦发生安全违规事件，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； **示例 2：**针对各部门制定数据安全和个人信息保护积分制度，形成量化的考核指标，并纳入整体绩效考核体系。
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**:开展技术先进性评估认证，在在网站或 APP 中进行个人信息授权获取页面体现数据安全和个人隐私保护的先进性资质； **示例 2**:定期开展专项活动，加入行业先进性组织/联盟，建立用户对品牌数据安全和个人隐私保护的先进性重视及认知； **示例 3**:组建数据安全和个人信息保护专职团队定期开展安全产品、服务合规性评审、合规自评估； **示例 4：**推动数据安全、个人信息保护相关技术的攻关，开发适宜于组织落实法律法规、国家标准、行业标准等合规性要求的技术或产品。
	6.2 技术的创新性和先进性	**示例 1：**参与数据安全、个人信息保护相关的法律法规、办法条例的制定和研讨，提出有效性建议； **示例 2：**参与国家标准、行业标准的制定和研究，将有效的技术手段、管理方法等引入到标准中，把标准成果落地转化应用； **示例 3：**参加数据安全和个人信息保护重点科研项目，建设突破性的数据安全和个人信息保护的平台、产品；

章节	相关行动和期望	示范案例
		示例 4：推动数据安全、个人信息保护相关技术的研究，形成兼具可行性、创新性、先进性的专利和论文。
	6.3 用户使用的价值体现	**示例 1**：为用户提供服务过程中涉及收集个人信息的，如果个人未授权个人信息的收集，需继续为用户提供不依赖个人信息的其他相关服务； **示例 2**：用户提出个人信息相关的投诉、举报时，在合法合规的前提下，尽早及时的向用户做出回应； **示例 3**：在产品或服务中为用户提供账号注销、个人信息匿名化等系列功能，并且有清晰的操作入口。
	6.4 社会治理的价值体现	**示例 1**：为监管机构提供技术支撑，在监管机构检查或评价组织在数据安全、个人信息保护的合规性时，提供相应的技术服务； **示例 2**：数据安全、个人信息保护相关的产品或服务提供协作通道，可与监管机构联动，发生安全事件时，及时上报和响应； **示例 3**：利用企业宣传途径，开展数据安全和个人虚信息保护相关社会治理的科普、宣传。
	6.5 数字包容与特殊保护	**示例 1**：为老年人、语言障碍、视觉障碍、未成年人等对象提供个人信息处理相关的服务时，在字体、颜色等方面提供易于阅读、易于理解的文字或图形，确保对象可快速、充分的理解个人信息的处理； **示例 2**：为不同国家语言的对象提供个人信息处理相关的服务时，除提供英文支持，可提供该国家语言的支持； **示例 3**：通过语音传达个人信息处理相关的服务时，应充分考虑听觉障碍的对象的需要，并为对象提供相应的文字或图形形式的支撑； **示例 4**：针对老年人、智力残障、未成年人等对象提供个人信息处理相关的服务时，在确认环节增加确认机制，确保本人以及监护人充分理解相关信息。
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**：在网站或 APP 中通过公开发布《个人信息保护政策》，将业务中处理个人信息的相关规则及事项告知个人，并确保个人可便利地查看； **示例 2**：如涉及使用算法对用户进行个性化推荐的，使用清晰且通俗易懂的语言、以显著方式将算法推荐服务的基本原理、目的意图和主要运行机制等算法规则予以释明，并确保用户得以便捷地查看。
	7.2 知识和技术成果共享	**示例 1**：设立并推动保护知识和技术共享的规定制度落地，并向社会公布； **示例 2**：定期组织前沿的技术及知识分享会，并组成学习社区； **示例 3**：提供知识或成果侵权及维权专业咨询及服务； 示例 4：企业内部建立知识产权和技术成果共享激励体系，并设立知识及技术成果收益共享机制；
	7.3 构建有效的平台规则	**示例 1**：内部建立对外平台执行效果的白皮书或相关报告相关流程，定期公布平台规则的执行效果，并开设发布后的建议渠道； **示例 2**：内部建立规则执行效果评估方式与组织，评审过程中引入三方或权威机构的咨询建议，保证平台规则执行效果的客观性；
	7.4 供应商规则共建及协助	**示例 1**：设立腐败、不公平待遇、违法违纪行为的投诉和举报的渠道，并严格保护举报人的信息； **示例 2**：定期与供应商开展交流会或培训会，加强合作规则、数据安全等要求的宣贯。
	7.5 公平竞争环境	**示例 1**：在企业层面制定并实施反垄断、反不正当竞争、反腐败和数据知识产权内部管理等制度，将制度文本提供给所有员工，并由员工书面签署回执，由

章节	相关行动和期望	示范案例
	构建	企业长期留存备查； **示例 2：**企业定期组织管理层及员工反垄断、反不正当竞争、反腐败和数据知识产权保护等培训，由全体员工参加，并书面形成培训记录，由企业长期留存备查； **示例 3：**在符合国家政策及法律法规的前提下，积极推动企业间的数据流动，探索行之有效的数据交易模式； **示例 4：**积极配合政府部门对反垄断、反不正当竞争的调查和执法行动，建立健全相关响应制度。
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：**基于区块链、隐私计算等先进技术，实现高性能、强隐私、高安全的区数据服务，实现数据安全和个人信息保护。
	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； 设立便捷的人工客服反馈渠道； **示例 2：**在 APP 等客户端涉诈“我的客服”频道，频道中包括常见问题、快捷工具等，方便消费者快速定位问题和解决问题； **示例 3：**反面示例，消费者关于个人信息泄露的投诉;消费者因本组织泄露其个人信息而遭受伤害或损害的案例。
	8.3 接受中立社会组织监督	**示例 1：**组织定期向社会公众发布自律准则和社会责任报告； **示例 2：**组织定期召开有外部专家参与的个人信息保护机制评审会，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、答题互动、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 32 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。
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 行业自治与工作联动	**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。

章节	相关行动和期望	示范案例
	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。

参 考 文 献

[1] GB/T 36001-2015 社会责任报告编写指南
[2] GB/T 36002-2015 社会责任绩效分类指引
[3] GB/T 39604-2020 社会责任管理体系 要求及使用指南
[4] GB/T 39626-2020 第三方电子商务交易平台社会责任实施指南
[5] SB/T 10963-2013 商业服务业企业社会责任评价准则
[6] YD/T3837-2021 信息通信行业企业社会责任评价体系
[7] T/ISC0002-2020 互联网企业社会责任报告编写指南
[8] T/CESA16003-2021 电子信息行业社会责任治理评价指标体系