



团 体 标 准

T/CFIS XXXX—XXXX

互联网企业合规建设评价体系

（征求意见稿）

（本草案完成时间：2022-10-08）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX-XX-XX 发布

XXXX-XX-XX 实施

中国网络社会组织联合会 发布



版权保护文件

版权所有归属于该标准的发布机构。除非有其他规定，否则未经许可，此发行物及其章节不得以其他形式或任何手段进行复制、再版或使用，包括电子版，影印件，或发布在互联网及内部网络等。使用许可可于发布机构获取。

目 次

1 适用范围 1

2 规范性引用文件 1

3 术语和定义 1

4 评价机制 2

5 评价指标 6

附 录 A 名词解释 27

附 录 B 相关法律法规依据 29

参考文献 34



互联网企业合规建设评价体系

1 适用范围

本标准规定了互联网企业合规建设的术语和定义，互联网企业合规建设评价体系框架、实施步骤、评价方式及持续改进的建议。

本标准适用于互联网企业，包括互联网平台、数字内容与媒体、互联网信息等企业(以下简称“企业”)。法律法规对企业合规管理另有专门规定的，从其规定。行业监管部门对企业境外经营合规管理另有专门规定的，有关行业企业应当遵守其规定。

2 规范性引用文件

GB/T35770-2017《合规管理体系指南》

ISO 37301:2021《合规管理体系要求及使用指南》(Compliance management systems — Requirements with guidance for use) 国际标准

国际标准化组织 ISO19600《合规性管理体系标准-指南》框架体系

3 术语和定义

3.1 互联网企业 Internet enterprise

设立并提供互联网相关产品与服务的企业，包括但不限于各类互联网平台、网络服务提供商、互联网服务提供商、互联网内容提供商、应用服务提供商、互联网数据中心、应用基础设施提供商等。

[注：为表述简便，本文件所指的“企业”如无特殊说明，均指互联网企业。]

3.2 合规 Compliance

企业及其员工的经营管理行为符合有关法律法规、国际条约、监管规定、行业准则、商业惯例、道德规范和企业依法制定的章程及规章制度等要求。

3.3 合规风险 Compliance risk

企业或其员工因违规行为遭受法律制裁、监管处罚、重大财产损失或声誉损失以及其他负面影响的可能性。

3.4 竞争合规 Competition Compliance

互联网企业及其员工的经营管理行为符合《反垄断法》《反不正当竞争法》等法律、法规、规章和指南及其他规范性文件（以下统称竞争法）规定的要求。

3.5 环境影响评价 Environmental impact assessment

是指对规划和建设项目实施后可能造成的环境影响进行分析、预测和评估，提出预防或者减轻不良环境影响的对策和措施，进行跟踪监测的方法与制度。

3.6 平台 platform

通过网络信息技术，使相互依赖的双边或者多边主体在特定载体提供的规则下交互，以此共同创造价值的商业组织形态。

3.7 平台经营者 undertakings of the platform

向自然人、法人及其他市场主体提供经营场所、交易撮合、信息交流等互联网平台服务的经营者。

3.8 平台内经营者 in-platform undertakings

在平台内提供商品或者服务的经营者。平台经营者在运营平台的同时，也可能直接通过平台提供商品。

3.9 合格 conformity

满足第三方评估机构提出的要求。

3.10 不合格 nonconformity

未满足第三方评估机构提出的要求。

3.11 纠正措施 corrective action

为了消除造成不合格的原因并防止其再发生所采取的措施。

3.12 持续改进 continuous improvement

提高合规的循环活动。

4 评价机制

4.1 评价目标

以倡导合规经营价值观为导向，以推动互联网行业健康发展为目标，以促进互联网企业自我规范管理为着力点，围绕合规战略规划、合规主体责任、合规风险识别和合规整改措施，建立契合互联网企业核心业务流程的合规建设评估体系，形成企业自评估与第三方评估相结合的合规评估机制，培育合规文化，强化网站平台信息内容管理、平台内经营者监督审核、网络安全保障、数字市场秩序维护等互联网企业主体责任，健全管理制度，完善运行规则，切实防范化解各种风险隐患，积极营造清朗网络空间。

4.1.1 合规目标的设定与策划

互联网企业应在相关职能和层级上建立合规目标。

合规目标应：

- 与战略方向一致；
- 适宜时，可测评；
- 结合适用的要求；
- 予以传达；
- 予以监督；
- 适宜时，予以更新；
- 作为文件化信息随时可调取使用。

互联网企业策划如何实现合规目标时，应确定：

- 做什么；
- 需要什么资源；
- 谁负责；
- 如何完成；
- 结果如何评价。

4.1.2 目标实现过程中的风险应对

策划实现合规建设目标时，应结合互联网企业所处环境以及利益相关方的需求，识别和应对可能发生的合规风险，从而：

- 确保合规管理能够实现预计目标；
- 预防或者减少非预期的影响；
- 实现持续改进。

应策划以下活动：

- 应对风险的措施；
- 如何将措施纳入合规管理过程并实施；
- 评价这些措施的有效性。

4.2 评价原则

4.2.1 标准性原则

互联网企业合规建设评价体系应参照本标准规定的评估框架进行实施。

4.2.2 可控性原则

评估方在评估实施过程中，应严格按照标准的评估方法对服务过程、人员和工具等进行控制，保证合规建设评估实施过程的安全可控。

4.2.2.1 服务可控性

企业委托第三方评估机构开展合规建设评估的，应要求评估方在评估工作开始前介绍评估服务流程，明确需要协调配合的工作内容，确保评估工作顺利开展。

4.2.2.2 人员与信息可控性

所有参与评估的人员应签署保密协议，应对评估过程数据和结果数据严格管理，未经被评估方授权，第三方评估机构不得泄露给任何单位和个人。

4.2.2.3 过程可控性

评估方应成立评估实施团队，采取项目组长负责制，应对评估工作进行记录并形成相关记录文档，达到项目过程的可控。

4.2.2.4 工具可控性

评估方应确保评估工具如工具软件、测试策略等的可操作性，并在评估实施前通告用户，获得被评估方许可后方可实施评估。

4.2.3 最小影响原则

评估方在评估过程中应采用最小影响原则，对于评估所需要的数据与参考资料，需与被评估方沟通并进行应急备份。

4.3 评价方式

4.3.1 企业自评

在开展效果评价时，企业应考虑面临的合规要求变化情况，不断调整合规管理目标，更新合规风险管理措施，以满足内外部合规管理要求。

企业进行合规建设评价后应形成评估报告，供决策层、高级管理层和业务部门等使用。评估报告内容包括风险评估实施概况、合规风险基本评价、原因机制、可能的损失、处置建议、应对措施等。

4.3.2 第三方评估

第三方评估机构可以是标准化组织、律师事务所、高等院校、行业协会或社会团体等专业机构。评估机构应具有独立性、专业性。

第三方评估机构应当对评估对象的评估过程、评估结果、评估档案以及涉及企业商业秘密的其他内容履行保密义务，违法向任何人披露评估内容的应当承担相应法律责任。

评估机构和评估对象应分别对评估档案进行存档留存，包括问题和材料清单、访谈交流问题清单、工作底稿、评估报告等。相关评估档案应至少保留三年。

4.4 评价结果

评估机构应根据风险情况，形成评估结果，评估结果宜有分数形式呈现，针对不同评估重点以及部分关键合规风险，可按照一定权重分别打分。对于关键合规风险指标得分以及总分均超过相应标准的，可评估为合格，否则为不合格。

4.4.1 持续改进

企业应根据合规评价结果，进入合规风险再识别和合规制度再制定的持续改进阶段，保障合规管理体系、主体责任、风险识别、整改措施全环节的稳健运行。

企业应积极配合监管机构的监督检查，并根据监管要求及时改进合规管理体系和风险识别能力。

4.4.2 不合格及纠正措施

经第三方评估不合格的，企业应采取下列措施：

（1）对不合格做出反应，并视情况：

—— 采取控制和纠正措施；

—— 处理后果。

（2）通过以下活动评估采取避免其再次发生或者在其他地方发生的措施的需求，以消除造成不合格的原因：

—— 确定造成不合格的原因；

—— 确定是否存在或者可能发生类似的不合格。

—— 实施任何必要的措施；

—— 评审所采取的任何纠正措施的有效性；

—— 如必要，修正某项合规评价指标。

—— 纠正措施应与不合格的影响相适应。企业应保存并可随时调取使用作为以下事项证据的文件化信息：

—— 不合格的性质及所采取的后续措施；

—— 任何纠正措施的结果。

4.4.3 复评

评估结果为不合格的，评估对象应采取纠正措施，明确整改任务和完成时限。纠正工作完成后，企业可以向评估机构申请开展复评，复评合格的，视为评估合格。

4.5 评价保障

4.5.1 组织管理

4.5.1.1 制度建设

互联网企业应结合本企业经营业态进行分类分级识别合规义务，并依据所识别的合规义务进行制度框架体系建设。制度建设应具备可长效循环、健康运转的运营机制。

（1）制度设计应：

—— 与合规目标相一致。

—— 与合规义务相适配，有效支撑合规管理。

—— 确保可执行、可实施、可落地。

（2）制度管理应：

—— 有规范的制度管理流程，包含制度需求确认、制度拟定、制度评估、制度审批、制度生效、制度迭代等环节；

—— 有明确的责任人，对制度框架体系的设计、规划、落实和维护负责；

—— 有可视化的制度管理产品，对制度发布、备案、推送、查阅、更新、下线进行生命周期管理；

—— 有独立的检查审计，对制度内容和管理运转进行监督评价。

制度应与业务相融合，贴合业务链路，指导业务合规。

（3）制度实施应：

—— 明确岗位职责，定岗定责；

—— 映射业务流程和产品卡口。

4.5.1.2 领导职责

(1) 互联网企业的最高管理者或者其授权委托人应通过下列方式对该互联网企业的合规管理工作负责：

- 确保互联网企业的合规目标与其战略方向保持一致；
- 确保互联网企业的合规管理要求与其业务流程相融合；
- 确保合规管理所需的资源配置到位；
- 确保建立合规的考核和奖惩机制；
- 持续推进合规目标实现；
- 持续改进合规管理；
- 作出合规承诺。

(2) 互联网企业的中高层管理者应通过下列方式对其职责范围内的合规管理工作负责：

- 将合规管理的要求融入其分管的业务流程；
- 配合与支持合规管理工作，推动其分管业务领域的员工共同参与合规管理；
- 培养员工的合规意识，提高员工合规能力，持续推进其分管业务领域内的全部员工遵守企业的合规目标和相关合规要求；
- 鼓励并支持员工对企业内的不合规事项进行内部举报；
- 根据要求积极参与合规相关事件和问题的处理和解决；
- 作出合规承诺。

4.5.1.3 员工要求

互联网企业全体员工的行为应符合如下要求：

- 遵守互联网企业的合规管理要求；
- 按照要求参加合规培训；
- 充分了解合规管理的重要性；
- 充分了解自身岗位与合规的关系；
- 充分了解不符合合规管理要求的后果与责任；
- 充分了解合规管理的内部举报流程；
- 发现有潜在合规风险的产品或业务时，依照流程及时开展合规风险评估。

4.5.2 支持保障

4.5.2.1 考核机制

互联网企业应将合规管理情况纳入对各部门和子企业负责人的年度综合考核，细化评价指标。强化考核结果运用，将合规职责履行情况作为员工考核、干部任用、评优评先等工作的重要依据。

互联网企业应建立个人违规行为记录制度，根据行为性质、发生次数、危害程度等，将其作为个人年度考评、评优评先的依据。

互联网企业应完善违规行为追责问责机制，进一步明确违规责任范围，细化惩处标准，针对反映的问题和线索，及时开展调查，按照有关规定严肃追究违规人员责任。

4.5.2.2 预算保障

互联网企业应建立经费保障机制，将合规管理体系建设经费纳入预算，健全合规管理工作预算资金管理制度，充分保障合规管理各项工作经费。

4.5.3 效能宣导

4.5.3.1 定期培训

互联网企业应将合规管理作为企业管理人员培训专题内容，不断提升企业管理人员合规意识，带头依法依规开展经营管理活动。

互联网企业应建立制度化、常态化的合规培训机制，制定年度合规培训计划，加大对企业员工的培训力度，将重点合规风险岗位人员业务培训、新员工入职必修内容纳入年度培训计划，以进一步提升员工合规意识。

4.5.3.2 文件化信息

互联网企业应建立合规管理信息系统，将规章制度、重点领域合规指南、合规人员管理、合规案例、合规培训、违规行为记录等作为重要内容。全面梳理业务流程，查找经营管理合规风险点，运用数字化手段将合规要求嵌入业务流程，明确相关条件和责任主体，针对关键节点加强合法合规性审查，强化过程管控。

4.5.3.3 文化培育

互联网企业应将合规管理作为企业文化建设重要内容，通过制定合规手册、签订合规承诺等方式将合规理念传达给全体员工，强化全员守法诚信、合规经营意识，树立依法合规、守法诚信的价值观。

5 评价指标

5.1 合规战略规划

5.1.1 总则

合规战略规划评价指标应以目标和规划为指南，与互联网企业业务相契合，围绕战略引领、管理到位、制度保障、宣贯配套，形成覆盖合规制度体系（建立制度框架、明确领导职责、制定制度管理和考核机制等）、合规组织管理体系（设计组织架构、加强内部合规审查、规范外部监督与评价等）、合规保障体系（跟踪政策与监管动向、建设信息保密配套设施与制度、增强合规建设预算等）和合规效能宣导（常态化合规培训、提高合规社会责任感与贡献等）的评价体系。

5.1.2 合规战略规划评价指标

一级指标	二级指标	评分细则	分值
合规制度体系 (30分)	制度设计（16分）	（1）建立合规制度框架	6分（每项2分）
		合规管理总纲:与合规目标相一致，明确合规管理的行为准则和纲领性要求	
		合规管理办法:明确具体合规域的合规原则性要求	
		合规管理实施细则:指导业务实践的操作指引、流程	
		（2）明确领导职责	4分（每项2分）
		明确最高管理者或其授权委托人的职责	
		明确中层管理者的职责	
		（3）建立制度化、常态化的合规培训机制	3
		（4）建立合规整改应急响应机制	3
	制度管理（10分）	（1）有规范的制度管理流程，包含制度需求确认、制度拟定、制度评估、制度审批、制度生效、制度迭代等环节	3
		（2）有明确的责任人，对制度框架体系的设计、规划、落实和维护负责	2
		（3）有可视化的制度管理产品，对制度发布、备案、推送、查阅、更新、下线进行生命周期管理；	3
		（4）有独立的检查审计，对制度内容和管理运转进行监督评价	2
	考核机制(4分)	（1）建立个人违规行为记录制度	2
		（2）构建违规行为追责问责机制	2
	加分项		
	将合规职责履行情况作为员工考核、干部任用、评优评先等工作的重要依据		5
合规组织管理	组织架构设计	（1）设置专门合规机构	2.5

一级指标	二级指标	评分细则	分值
体系（25 分）	（5 分）	（2）配备专职合规人员	2.5
	内部合规审查（10 分）	（1）设立内部审查监督管理机构及相关负责人	5
		（2）制定年度合规审查评估计划并建立合规风险排查机制	5
	外部监督与评价（10 分）	建立第三方侵权反馈、举报通知渠道	4
		设立具体及时响应及处理规则，包括下架处理、误删恢复等	4
		就投诉情况、投诉材料、处理结果等建立存档库进行备份及待查	2
合规保障体系（20 分）	合规监管政策跟踪（10 分）	（1）设立专门研究部门或团队，及时跟踪政策导向，洞察内外部环境变化	5
		（2）主办或参与政府、高校及研究机构的法律法规政策研讨活动，主办加 5 分，参与加 3 分	最高 5 分
	信息保密配套建设（6 分）	（1）合规审查及第三方评估结果涉及企业商业秘密等部分建立保密机制	3
		（2）评估档案进行存档留存	3
	预算保障（4 分）	（1）建立合规管理工作预算资金管理制度	2
		（2）将合规管理体系建设经费纳入预算	2
	【加分项】信息化系统工具配套建设(15 分)		
	（1）通过大数据手段建立合规风险智能审查系统		5
	（2）关于数据安全、网络安全和个人信息安全，具备较高的信息技术保障或相关认证		5
	（3）定期发布合规政策动态		5
合规效能宣导（25 分）	有面向全员的系统化合规培训（15 分）	（1）开展合规经营宣传、培训、考核，并就相关培训记录及成效建立档案库进行备份及待查	5
		（2）定期对从业人员进行网络安全、数据安全、竞争合规、知识产权保护、环境与劳动合规的教育、技术培训和技能考核	5
		（3）及时根据国内竞争政策调整、经营环境变化情况对业务流程、合规制度进行重新评估并进行调整；	5
	合规与社会责任活动贡献（10 分）	（1）履行消费者权益保护	2.5
		（2）履行内容治理、技术伦理、网络安全、市场秩序维护、知识产权保护、数据安全等平台主体责任	2.5
		（3）履行环境保护宣导、能源管理、资源可持续利用等方面的责任	2.5
		（4）参与和推动行业发展、服务社会等	2.5
	加分项(10 分)		
	（1）合规与社会责任报告发布		5
	（2）在企业文化和价值观中纳入合规建设内容		5

5.2 合规主体责任

5.2.1 总则

围绕信息披露和公示、账号注册管理、平台内容审核与商品/服务准入管理、网络安全、数据安全和个人信息保护等合规主体责任工作主线，建立系统、客观、量化的评价体系，明确评分细则，加强互联网企业合规业务的自我审查，为第三方评估提供合规评测依据。

5.2.2 合规主体责任评价指标

一级指标	分值	二级指标	分值	评分细则
信息披露和公示	20	用户协议、隐私条款公示	5	用户协议完整包含以下内容，并显著公示，可得 2 分：服务协议、平台公约与交易规则、算法推荐服务规则等；隐私条款完整包含以下内容，并显著公示，可得 3 分：个人信息收集使用规则、隐私保护指引、儿童隐私保护指引、第三方信息共享清单等。
		营业执照、行政许可等信息公示及所属行业内要求公示的资质、信息等	5	具备与经营业务相符的营业执照，显著公示增值电信业务许可信息，可得 2 分；按照所属行业要求完整进行相关资质公示，可得 3 分
		披露商品及服务信息	5	全面、真实、准确、及时地披露商品或者服务信息
		【加分项】披露环境信息	3	
		设立申诉和公众投诉、举报入口	5	建立并公布投诉、举报渠道，得 2 分；在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）受理并处理，得 3 分；
账号注册管理	10	用户身份核验、登记	5	制定并公开账号管理规则，得 1 分；对违法违规账号加强处置力度，建立黑名单账号数据库，得 2 分；严格落实真实身份信息登记，并采取复合验证等措施，得 2 分；
		名称、头像等信息合规审核	5	对账号名称信息进行合法合规性核验，得 1 分；建立账号名称信息动态核验巡查制度，对存量账号的名称信息进行合法合规性、真实性核验，得 1 分；以显著方式，在互联网用户账号信息页面展示账号 IP 地址属地信息，得 1 分；严格分类分级，对需要关注账号管理建立目录清单，制定管理措施，得 1 分；对申请经济、教育、医疗卫生、司法等领域信息内容生产的账号，向社会公众提供互联网新闻信息服务的账号，依据相关法律法规进行必要核验，得 1 分。
		【减分项】核验机构主体身份信息	3	公众账号信息服务平台：对账号主体真实身份信息、服务资质等进行必要核验，确保公众账号名称和运营主体业务相匹配；+/-3；电子商务平台：按照规定向市场监督管理部门报送平台内经营者的身份信息；否，-3。
		【减分项】供应商（平台内经营者）信用评价	3	公众账号信息服务平台：建立生产运营者信用等级管理体系，根据信用等级提供相应服务，+/-3；电子商务平台经营者：建立健全信用评价制度，公示信用评价规则；不得删除消费者对其平台内销售的商品或者提供的服务的评价；否，-3。
平台内容审核与商品/服务准入	30	建立信息内容审核机制	15	建立并落实总编辑负责制度，明确总编辑信息内容审核权利责任，建立总编辑全产品、全链条信息内容审核把关工作机制，得 2 分；建立识别违法和不良内容特征库，分级分类设置，并定期

一级指标	分值	二级指标	分值	评分细则
				丰富扩充，得3分（每点得1分）； 落实信息审查，对信息发布、跟帖评论进行审核，实时巡查、处置网络谣言，得2分； 完善人工审核制度，配备与服务规模相适应的专业人员和技术能力，得2分； 重点信息多节点召回复核机制：明确重点信息范围、标准、类别等，对关系国家安全、国计民生和公共利益等重点领域信息，增加审核频次，加大审核力度，得2分； 建立用户信用记录和评价制度，建立并留存处置用户违规行为记录，得2分； 建立应急处理制度：发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告，得2分。
		【加/减分项】 建立算法推荐管理制度	10	定期审核、评估、验证算法机制机理、模型等，不得设置诱导用户沉迷、过度消费等违反法律法规或者违背伦理道德的算法模型，得2分； 建立健全用于识别违法和不良信息的特征库，完善入库标准、规则和程序；算法生成合成信息作显著标识，得2分； 加强用户模型和用户标签管理，完善记入用户模型的兴趣点规则和用户标签管理规则，不得将违法和不良信息关键词记入用户兴趣点或者作为用户标签并据以推送信息，得1分； 向用户提供选择或者删除用于算法推荐服务的针对其个人特征的用户标签的功能，得1分； 算法推荐服务版面页面建立完善人工干预和用户自主选择机制，在重点环节积极呈现符合主流价值导向的信息，得2分； 向用户提供不针对其个人特征的选项，或者提供便捷的关闭算法推荐服务的选项。用户选择关闭算法推荐服务的，立即停止提供相关服务，得2分。
		建立产品或服务准入机制	5	产品、服务应当符合相关国家标准的强制性要求，得2分； 建立网络产品或服务的评价/准入标准，并依照标准进行审核，通过审核方可面向用户开放，得3分。
		【减分项】商品准入	3	电子商务经营者应当依法办理市场主体登记，要求申请进入平台销售商品或者提供服务的经营者提交其身份、地址、联系方式、行政许可等真实信息，进行核验、登记，建立登记档案，并定期核验更新。 否，-2分；
		【减分项】有无销售违禁商品	3	电子商务平台：最近3个月收到关于平台内违禁商品的相关处罚。 是，-3；
		【减分项】有无发布违禁内容	3	最近3个月收到关于平台内违禁内容的相关处罚。 是，-3；
网络安全、数据安全与个人信息保	40	按照网络安全等级保护制度履行安全保护义务	9	制定内部安全管理制度和操作规程，确定网络安全负责人，得1分； 采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施，得2分；

一级指标	分值	二级指标	分值	评分细则
护				采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月，得 2 分； 采取数据分类、重要数据备份和加密等措施，得 2 分； 依法取得网络安全等级保护备案证明，并依法定期完成等级保护测评，得 2 分。
		建立全流程数据安全管理制度	5	制定数据安全管理制度，确定数据安全负责人，得 1 分； 在法律、行政法规规定的目的和范围内收集、使用数据，得 2 分； 每年定期开展人员管理与培训，并保存记录，得 2 分； 【减分项】涉及数据出境的，按规定进行数据安全评估工作，若否，-2。
		建立个人信息保护制度	11	制定内部管理制度和操作规程，确定个人信息保护负责人，得 1 分； 对个人信息实行分类管理，得 2 分； 采取相应的加密、去标识化等安全技术措施，得 2 分； 合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训，得 2 分； 设置专门的儿童个人信息保护规则，并指定专人负责儿童个人信息保护，得 2 分； 按照最小必要性原则收集个人信息，得 2 分。
		设立应急预案	3	建立网络安全、数据安全、个人信息保护应急处置机制，得 1 分； 进行风险监测，发现安全缺陷、漏洞等风险时，立即采取补救措施，得 1 分； 发生事件时，应当立即采取处置措施，按照规定及时告知利害关系人，并向有关主管部门报告，得 1 分；
		【减分项】个人信息保护制度	10	提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，否，-2 分； 按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督，否，-2 分； 制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务，否，-2 分； 对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务，否，-2 分； 定期发布个人信息保护社会责任报告，接受社会监督，否，-2 分；
		保障网络产品、服务安全	6	发现其网络产品、服务存在安全缺陷、漏洞等风险时，立即采取补救措施，按照规定及时告知用户并向有关主管部门报告，得 2 分； 网络产品、服务的提供者应当为其产品、服务持续提供安全维护，在规定或者当事人约定的期限内，不得终止提供安全维护，得 2 分； 网络产品、服务具有收集用户信息功能的，向用户明示并取得同意，得 2 分。
		保障网络数据安全	6	采取技术措施和其他必要措施，保障网络安全、稳定运行，得 2 分； 对数据、个人信息处理活动负责，并采取必要措施保障所

一级指标	分值	二级指标	分值	评分细则
				处理的数据、个人信息的安全，得 2 分； 有效应对网络安全事件，防范网络违法犯罪活动，得 2 分。
		【减分项】风险评估	2	重要数据的处理者：定期对数据处理活动开展风险评估，并向有关主管部门报送风险评估报告。风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况。 是，0 分，否，-2 分；
		【减分项】未成年人保护与老年人关怀	2	建立健全防沉迷制度，不得向未成年人提供诱导其沉迷的产品和服务，及时修改可能造成未成年人沉迷的内容、功能或者规则，并定期向社会公布防沉迷工作情况。 【加分项】+2
			12	未成年人用户数量巨大、在未成年人群体具有显著影响力的重要互联网平台服务提供者： 在互联网平台服务的设计、研发、运营等阶段，充分考虑未成年人特点，定期开展未成年人网络保护影响评估； 提供青少年模式或者未成年人专区等； 建立未成年人网络保护合规制度体系，成立主要由外部成员组成的独立机构，对未成年人网络保护情况进行监督； 制定专门的平台规则，明确平台内产品或者服务提供者未成年人网络保护的义务，并以显著方式提示未成年人用户依法享有的网络保护权利和遭受网络侵害的救济途径； 对严重违法法律、行政法规侵害未成年人身心健康或者侵犯未成年人其他合法权益的平台内的产品或者服务提供者，停止提供服务； 每年发布专门的未成年人网络保护社会责任报告，并通过公众评议等方式接受社会监督。
			6	网络游戏、网络直播、网络音视频、网络社交等网络服务提供者： 设立青少年模式，呈现青少年专属精选内容； 按要求设置使用时段、时长、功能，并为监护人提供时间管理、权限管理、消费管理等功能； 合理设置未成年人单次消费数额和单日累计消费数额上限。
			6	网络游戏服务提供者： 要求未成年人用户进行实名制认证，并接入统一的未成年人网络游戏电子身份认证系统等必要手段验证其真实身份信息； 建立、完善预防未成年人沉迷网络游戏的游戏规则； 落实适龄提示标准规范，对游戏产品进行分类并显著提示。
			2	进行适老化、无障碍改造。【加分项】2 分
		【加分项】网络安全保险	2	
		【减分项】算法备案	2	具有舆论属性或者社会动员能力的算法推荐服务提供者，在提供服务之日起十个工作日内通过互联网信息服务算法备案系统履行备案手续，并按规定办理变更手续、注销备案手续。 若否，-2 分。

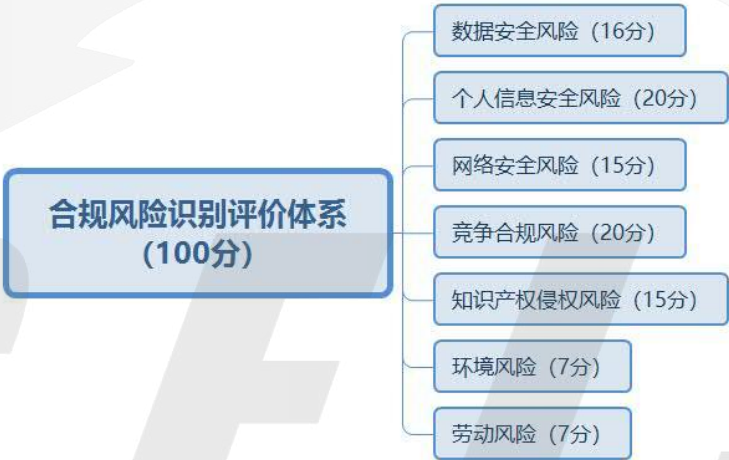
5.3 合规风险识别

5.3.1 总则

企业应当建立必要的制度和流程，识别新的和变更的合规要求。企业可围绕关键岗位或者核心业务流程，按照数据安全、个人信息保护、网络安全、竞争合规、知识产权保护、环境风险、劳资关系等维度，通过合规咨询、审核、考核和违规查处等内部途径识别上述合规风险，也可通过外部法律顾问咨询、持续跟踪监管机构有关信息、参加行业组织研讨等方式获悉外部监管要求的变化，识别上述合规风险。

企业境外分支机构可通过聘请法律顾问、梳理行业合规案例等方式动态了解掌握业务所涉国家(地区)政治经济和法律环境的变化，及时采取应对措施，有效识别各类合规风险。

5.3.2 合规风险识别评价体系



5.3.2.1 数据安全风险识别评价体系

一级指标	分值	二级指标	分值
数据安全 风险识别	16 分	【1】数据采集 明确数据采集渠道、数据格式、采集流程和采集方式等相关数据采集要求，并对数据来源的合法性和正当性进行确认与查验；	1.5（应全部达标）
		【2】数据存储 基于数据分类分级，明确相应的数据存储保护措施，包括加密存储、访问控制、存储介质安全策略、备份恢复等。	1.5（应全部达标）
		【3】数据使用 （1）明确数据的使用目的和范围符合，确保国家法律、法规要求，并基于数据分类分级，明确相应的数据使用安全要求，包括访问控制、数据脱敏等； （2）明确第三方应用数据安全，通过合同等方式明确双方数据安全保护责任和义务。	2（应全部达标）
		【4】数据加工 明确对数据加工结果输出和使用的安全检查、风险评估和授权流程；	1.5（应全部达标）
		【5】数据传输 （1）基于数据分类分级，明确相应的数据加密传输要求，并明确加密算法要求和密钥管理要求； （2）明确数据接口管理规范与技术管控措施。	2（应全部达标）
		【6】数据提供	1.5（应全部达

一级指标	分值	二级指标	分值
		明确第三方处理数据的安全要求，通过合同等方式明确接收方数据处理目的、期限、处理方式、保护措施、双方权利和义务。	标)
		【7】数据公开 明确数据公开范围、内容、审核流程、控制措施等要求。	2(应全部达标)
		【8】重要数据管理 涉及重要数据处理的应遵循以下要求： (1) 明确数据安全负责人和管理机构； (2) 制定重要数据的处理活动记录管理要求与模板，并按要求执行记录； (3) 定期开展重要数据处理活动的风险评估，并报送风险评估报告给主管部门 (4) 重要数据出境的符合《数据安全法》相关规定	4(应全部达标)
		加分项 (+2 分)	
		通过数据安全保护认证。 采用自动化工具落实数据分类分级管理。	每达标一项加 1 分
		减分项 (-8 分)	
		违规向境外传输国家秘密/国家核心数据/限制性技术数据； 非法获取、持有国家秘密载体； 非法复制、记录、存储国家秘密； 违反国家核心数据管理制度，危害国家主权、安全和发展利益	-4(若出现一项情况则全部扣分)
		过去 12 个月内发生严重的数据安全事件时，放任事件发展而不进行处理；在符合上报条件时，隐瞒事件未向主管机构进行告知；在符合通知要求时，隐瞒事件未通知受影响的主体。	-2(若出现一项情况则全部扣分)
		过去 12 个月内公司收到监管机构出具的与数据安全相关的： (1) 处罚决定。 (2) 监管意见。 (3) 风险提示。 (4) 公司运营的数据产品被主管机构处罚。	-2(若出现一项情况则全部扣分)

5.3.2.2 个人信息侵权风险识别评价体系

一级指标	分值	二级指标	分值
个人信息安全风险	20	【1】个人信息来源合规 直接收集：个人信息收集需符合法定条件（即《个人信息保护法》第十三条）。 间接收集：审查第三方是否有权向公司提供个人信息，并保存审查记录；第三方已经告知个人其将向公司提供个人信息；可要求第三方提供个人信息来源合法承诺函。 从公开渠道获取：相关个人信息系通过合法方式已公开的信息；处理公开个人信息的目的符合个人信息公开时个人的隐私期待；涉及通过爬虫等自动化手段获取个人信息的，事先综合考虑目标网站访问控制措施、涉及各方的竞争关系、目标数据的性质、拟采取手段的合法性与正当性、对目标网站的影响等因素，制定合规采集方案。 充分告知：通过隐私政策，签订协议，弹窗等显著方式，向个人信息主体清晰充分告知收集、使用个人信息的目的、方式和范围等规则。 目的限制：实际收集的个人信息类型需与明示的收集目的之间具有直接关联，符合最小必要原则，对于超出范围收集的个人信息应删除或	3.5 (每项 0.7 分，最高 3.5 分，应全部达标)

一级指标	分值	二级指标	分值
		匿名化处理。	
		【2】个人信息存储合规 执行个人信息分级分类管理：根据数据类型和敏感程度进行划分，不同级别和类别对应不同处理措施。 明确个人信息保存期限与期限届满的处理措施：保证个人信息存储时间为满足使用目的的最小时间，并且符合法定留存期限的要求，例如商品和服务信息、交易记录需保存 3 年。超出存储期限后，对个人信息进行删除或匿名化处理。 依法采取去标识化措施：将可用于恢复识别个人的信息与去标识化后的信息分开存储，加强访问和使用的权限管理。 停止收集：停止运营其产品或服务时，应将所持有的个人信息进行删除或匿名化处理。	2（每项 0.5 分，应全部达标）
		【3】对外提供个人信息合规 依法进行个人信息安全影响评估并留存评估报告，评估因素应结合具体业务场景有所侧重，例如根据委托处理、向其他个人信息处理者提供、公开个人信息等场景采取不同评估标准。 签署协议：通过合同等形式与第三方确定其应满足的个人信息安全要求，以及在个人信息安全方面分别承担的责任和义务。 告知并获得授权：涉及个人信息共享和转让的，需要依法向个人信息主体告知共享、转让的目的、数据范围、以及后果，征得个人信息主体的授权同意。 监督个人信息受托处理者：涉及委托第三方处理个人信息的，应定期或不定期对受委托者进行审计，或要求受委托者提供合规自评估或第三方评估报告。 公开个人信息：原则上不应公开处理的个人信息，除非向个人信息主体告知公开个人信息的目的、类型、必要性，并事先征得个人信息主体的单独同意。 管理第三方接入 SDK：若服务或产品嵌入了第三方 SDK，事先对拟接入的 SDK 进行合规审核，并应制定 SDK 清单，披露 SDK 的名称、收集的个人信息类型、收集目的、SDK 提供者名称、联系方式、隐私政策等内容。	3（每项 0.5 分，应全部达标）
		【4】个人信息使用合规 目的特定，最小必要：在业务活动中所使用的个人信息应具有合法的收集来源，使用目的应与收集目的具有合理关联。 敏感个人信息使用需充分必要：只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，公司方可处理敏感个人信息；处理前依法开展个人信息保护影响评估；原则上不将生物特征识别信息作为唯一实现业务目标的方式。	1（每项 0.5 分，应全部达标）
		【5】算法推荐服务合规（放主体责任） 画像管理：不得将违法和不良信息关键词记入用户兴趣点或者作为用户标签；应向用户提供选择或者删除用于算法推荐服务的针对其个人特征的用户标签的功能。 参数设置：不应将浏览次数、支付意愿、支付能力、依赖程度、交易频次、交易时使用的终端设备品牌等作为与用户进行交易的条件参数。 审核算法模型：公司应当定期审核、评估、验证算法机制机理、模型、数据和应用结果等。 提供关闭选项：公司应当向用户提供不针对其个人特征的选项，或者	3.5（每项 0.5 分，应全部达标）

一级指标	分值	二级指标	分值
		向用户提供便捷的关闭算法推荐服务的选项。 公开透明：制定并公开算法推荐相关服务规则，及时、合理、有效地公开算法基本原理、优化目标、决策标准等信息，做好算法结果解释，畅通投诉通道，消除社会疑虑，促进算法公开透明。 外部投诉处理：公司应当就算法推荐服务设置并公开便捷有效的用户申诉和公众投诉、举报入口。 评估与备案：具有舆论属性或者社会动员能力的算法推荐服务提供者应当在提供服务之日起十个工作日内通过互联网信息服务算法备案系统进行备案。	
		【6】消费者个人信息保护 个性化推荐：显著区分个性化展示的内容和非个性化展示的内容。同时向消费者提供不针对其个人特征的选项。 广告营销：通过电话、短信、邮件等向消费者发送商业营销信息前应征得个人同意；公司发送商业营销信息时，应同步向消费者提供显著、简便、免费的拒绝接收方式；依法标识广告内容。 算法推荐：不得设置诱导用户沉迷、过度消费等违反法律法规或者违背伦理道德的算法模型。 有奖销售：公司应用算法向用户进行有奖销售，应当遵守《反不正当竞争法》《规范促销行为暂行规定》的规定，不得通过利用算法操纵中奖概率、中奖结果、中奖人员等欺骗方式进行有奖销售。 金融消费者信息：金融机构处理消费者信息时，不得：未按规定保存客户身份资料或交易记录；未经授权查询征信信息；违规查询个人客户储蓄存款交易信息；违法违规购买或出售消费者个人金融信息等。	2.5（每项 0.5 分，应全部达标）
		【7】不满 14 周岁未成年人个人信息保护 应当设置专门的未成年人个人信息保护规则和用户协议，并指定专人负责未成年人个人信息保护。 收集、使用、转移、披露未成年人个人信息的，应当以显著、清晰的方式告知其监护人，并应当征得未成年人监护人的同意。 权限管理：以最小授权为原则，严格设定内部信息访问权限，控制未成年人个人信息知悉范围，记录数据访问情况；访问未成年人个人信息的，应当经过未成年人个人信息保护负责人或者其授权的管理人员审批，记录访问情况，并采取技术措施，避免违法复制、下载未成年人个人信息。 算法不得诱导未成年人沉迷：应当开发适合未成年人使用的模式；不得向未成年人推送可能引发未成年人模仿不安全行为和违反社会公德行为、诱导未成年人不良嗜好等可能影响未成年人身心健康的信息，不得利用算法推荐服务诱导未成年人沉迷网络。	2（每项 0.5 分，应全部达标）
		【8】个人信息出境相关规定 应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使法定权利的方式和程序等事项。 依法取得个人的单独同意；与境外接收方签署数据传输协议；依法进行评估与认证。	1（每项 0.5 分，应全部达标）
		【9】保障个人信息主体行权 以显著方式公布个人信息主体行权响应途径，例如客服电话，维权平台或通道，权利响应邮箱等，以响应个人依法行使的权利，包括但不限于个人信息查询权、更正权、删除权、撤回同意权、注销账户权、复制权、可携带权等。	1.5（每项 0.5 分，应全部达标）

一级指标	分值	二级指标	分值
		保障消费者权益：搭售商品应告知消费者；未经消费者允许，不得随意删除其评价；不得虚构交易、编造用户评价。 及时响应主体请求：在 15 个工作日内处理并反馈个人权利请求。	
		加分项（+5 分）	
		设置隐私政策摘要，并通过交互式选择界面体现隐私政策的摘要内容。【多层级、互动式呈现，加分】 建立用户权利请求与投诉建议响应自动化在线平台。 建立个人信息保护影响评估标准工具。 通过个人信息保护技术认证，如 ISO27701 隐私信息管理体系认证、ISO29151 个人身份信息保护认证等。 识别新出台的法律法规对公司业务的影响，并组织合规人员培训学习。	每达标一项加 1 分
		减分项（-10 分）	
		涉及个人信息处理的产品，未设置清晰易懂的隐私政策，或未向用户进行充分告知。	-2（若出现一项情况则全部扣分）
		采用一次概括授权、默认授权、与其他授权捆绑、停止安装使用等方式，强迫或变相强迫用户同意收集、使用与经营活动无直接关系的个人信息。	-2（若出现一项情况则全部扣分）
		发生对个人信息主体权益造成严重危害的安全事件时，放任事件发展而不进行处理；在符合上报条件时，隐瞒事件未向主管机构进行告知；在符合通知要求时，隐瞒事件未通知受影响的主体。	-2（若出现一项情况则全部扣分）
		实施虚构原价、虚假优惠折价等不正当价格行为，对用户收取未予以标明的费用；或根据用户的偏好、交易习惯等特征，在交易价格等交易条件上实行不合理的差别待遇。	-2（若出现一项情况则全部扣分）
		过去 12 个月内公司收到监管机构出具的与个人信息安全相关的：处罚决定。 监管意见。 风险提示。 公司运营的 App 被工信部或网信办等主管机构通报批评或下架处罚。	-2（若出现一项情况则全部扣分）

5.3.2.3 网络安全风险识别评价体系

一级指标	分值	二级指标	分值
网络安全风险识别	15	网络安全识别 （1）资产识别和资产管理措施 互联网企业需要有完备的信息资产识别管理、漏洞管理和漏洞发现机制，需定期对自身的资产的数量和质量进行梳理	2（应全部达标）
		网络安全防护 （1）是否对人员的行为和活动进行充分的管理 互联网企业需要从对企业信息资产的访问控制、对人员的权限管理、对信息资产和日常活动进行审计、以及管理企业人员的安全意识四个方面具有完善的管理体系（2）开发和运维管理措施 互联网企业需要在系统的开发和运维两个方面具备完善的开发和运维规范，包括且不限于代码、系统和软硬件的测试、性能、运维人员资质等	5（第一项 3 分，第二项 2 分）
		网络安全监测评估 信息安全认证&合规建设 互联网企业需通过必要的信息安全管理体系认证，并构建信息安全合规建设体系，此项不满足不扣分 安全风险管理和评估	4（每项 2 分）

一级指标	分值	二级指标	分值
		互联网企业需在一定期限内进行网络安全审查，并针对自身的网络安全风险进行评估，此项不满足不扣分	
		【4】关键信息基础设施安全保障 采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。 对重要系统和数据库进行容灾备份。 采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。 自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估。	4（每项 1 分）
		减分项（-10 分）	
		过去 12 个月内发生对网络安全造成严重危害的安全事件时，放任事件发展而不进行处理；在符合上报条件时，隐瞒事件未向主管机构进行告知。	-2（若出现一项情况则全部扣分）
		设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组；利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。	-2（若出现一项情况则全部扣分）
		非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，为其提供技术支持、广告推广、支付结算等帮助。	-2（若出现一项情况则全部扣分）
		关键信息基础设施的运营者违反法律规定，使用未经安全审查或者安全审查未通过的网络产品或者服务；违法在境外存储网络数据；违法向境外提供网络数据。	-2（若出现一项情况则全部扣分）
		过去 12 个月内公司收到监管机构出具的与网络安全相关的：处罚决定。 监管意见。 风险提示。 公司运营的网站等被主管机构处罚。	-2（若出现一项情况则全部扣分）

5.3.2.4 竞争合规风险识别评价体系

一级指标	分值	二级指标	评分标准
		基础项（20）	
		经营者集中申报（3）	2 分 每项 1 分，应全部满足。
反垄断和反不正当竞争风险（20）		针对经营者集中： 对过往交易完成了经营者集中合规排查； 对于应报未报的交易，及时进行了补报；	
		针对横向垄断协议： 不得与具有竞争关系的经营者达成横向垄断协议，包括固定价格、分割市场、限制产（销）量、限制新技术（产品）、联合抵制交易等；不得从事敏感行为，例如与其他竞争者交换价格、销量、成本、客户等敏感信息，开展其他意思联络或协调一致行为等； 参加行业协会会议和与其他竞争者会议时，严格遵守反垄断合规行为规范。	1 分
		针对纵向垄断协议： 不得与交易相对人达成纵向垄断协议，包括固定转售价格和限定最低转售价格； 确保与交易相对人的其他敏感条款合规，包括销售渠道限制、销售区	1 分

一级指标	分值	二级指标	评分标准
		域限制、不竞争或者最惠国待遇等条款。	
轴幅协议 (1)		针对轴幅协议： 不得组织、协调合作经营者之间达成垄断协议； 不参与合作经营者组织、协调的经营者之间的垄断协议； 平台经营者不得组织、协调平台内经营者或其他合作方达成垄断协议。	1 分
虚假宣传 (1)		不得从事以下虚假宣传行为：虚假交易（“刷单炒信”）、虚假排名、虚构经营数据、虚构流量数据、误导性展示评价（“隐匿差评”）、虚构互动数据、进行虚假营销、诱导性互动（“好评返现”）等。	1 分
混淆行为 (1)		不得从事以下混淆行为： 擅自使用他人有一定影响的域名主体部分、网站名称、网页等相同或近似的标识； 擅自使用与他人有一定影响的应用软件、网店、自媒体、游戏界面等的页面设计、名称、图标、形状等相同或近似的标识； 擅自将他人有一定影响的商品名称、企业名称（包括简称、字号等）社会组织名称（包括简称等）、姓名（包括笔名、艺名、译名）等标识设置为搜索关键词。	1 分
不当有奖销售 (1)		不得从事以下不当有奖销售的行为： 销售信息不明确（包括所设奖的种类、兑奖条件、奖金金额或者奖品等有奖销售信息），影响兑奖； 采用谎称有奖或者故意让内定人员中奖的欺骗方式进行有奖销售； 抽奖式的有奖销售，最高奖的金额超过五万元。	1 分
商业诋毁 (1)		不得从事以下商业诋毁的行为：恶意评价，恶意散布虚假或者误导性信息，作出虚假或者误导性的风险提示、告客户书、警告函、律师函或举报信等。	1 分
商业贿赂 (1)		不得从事以下商业贿赂的行为： 经营者不得采用财物或者其他手段贿赂交易相对方的工作人员、受交易相对方委托办理相关事务的单位或者个人，或者利用职权或者影响力影响交易的单位或者个人，以谋取交易机会或者竞争优势； 对于与交易相对人或合作方的折扣、佣金等安排，保证以明示方式进行并如实入账。	1 分
流量劫持 (1)		不得从事以下流量劫持的行为： 未经其他经营者和用户同意，强制进行跳转； 利用关键词联想等功能，设置指向自身产品或者服务的链接，欺骗或者误导用户点击等。	1 分
妨碍干扰 (1)		不得从事以下妨碍干扰的行为： 误导、欺骗、强迫用户修改、关闭、卸载、放弃使用其他经营者合法提供的网络产品或者服务； 违背用户意愿下载、安装、运行应用程序，损害消费者合法权益或者影响其他经营者合法提供的设备、功能或者其他程序正常运行； 对非基本功能的应用程序不提供卸载功能或者对应用程序卸载设置障碍，损害消费者合法权益或者影响其他经营者合法提供的设备、功能或者其他程序正常运行；（“不提供卸载预装的非基本功能应用程序”） 无正当理由，对其他经营者合法提供的网络产品或者服务实施屏蔽、拦截、修改、关闭、卸载，妨碍其下载、安装、运行、升级、转发、传播等； 调整其他经营者的网络产品或者服务在搜索结果中的自然排序位置，	1 分

一级指标	分值	二级指标	评分标准
		并实施恶意锁定。（“搜索降权”）	
	恶意不兼容（1）	在实施不兼容行为前，审查了行为的合规性。例如，考虑以下因素：主观意图、对象范围、对市场竞争秩序的影响、对其他经营者合法提供的网络产品或者服务正常运行的影响、对消费者合法权益以及社会福利的影响、是否符合诚信原则、商业道德、特定行业惯例、从业规范、自律公约等，以及是否存在其他正当理由等。 不得从事恶意不兼容的行为。例如，无正当理由时产品和替代产品之间的相互“查杀”；无正当理由拒绝开放渠道端口等。	1 分
	其他网络不正当竞争行为（2）	针对其他网络不正当竞争行为：确保业务中所涉技术手段、交易规则、交易协议、通知、商务政策、考核方式、考核指标等符合法律规定；不得从事“二选一”，限制物流选择，不当下架商品、降权搜索、限制经营、屏蔽店铺、提高服务收费，“反向刷单”，选择性屏蔽，非法数据抓取，“大数据杀熟”等行为； 不得利用服务协议、交易规则以及技术等手段，对平台内经营者在平台内的交易、交易价格以及与其他经营者的交易等进行不合理限制或者附加不合理条件，或者向平台内经营者收取不合理费用。	3 分（每项 1 分）
	滥用市场支配地位（4）	针对市场支配地位： 定期对重要产品或服务的市场份额情况进行监控以及支配地位进行评估。 针对具有或可能具有支配地位的产品或服务： 不得以不公平高价销售、以不公平的低价购买商品； 无正当理由，不得以低于成本的价格销售商品； 无正当理由，不得拒绝、限定交易（“二选一”），或对条件相同的交易相对人在交易价格等交易条件上实行差别待遇（“大数据杀熟”），附加不合理交易条件或搭售。	4 分 针对支配地位的评估，有定期评估机制得 1 分，没有不得分。 对于滥用市场支配地位行为，仅适用于具有市场支配地位的企业，应全部满足。
	加分项		
	更完善的合规制度	在基本的合规要求之外，建立了更完善的合规和风险控制的制度体系： 针对新的投资并购交易，建立了常态化的经营者集中申报义务评估体系或流程。 针对与竞争者会议或行业协会会议设置了专门的报批制度； 设置专门的竞争合规热线； 在交易中主动向经销商、竞争对手等交易主体告知并倡导合规经营原则，做出合规经营承诺； 建立定期更新了解境内外反垄断和反不正当竞争立法、执法动态的制度； 及时公示有关垄断行为、不正当竞争行为的处理结果、整改方案、整改结果。	每一项加 1 分。
	监督举报	对经营活动中发现其他经营者的违法违规行为，及时向有关部门进行检举举报，经查证后属实的。	每一次加 1 分。
	滥用行为	对于中小型企业，建立了本行业内滥用行为的监控和预防机制，包括：定期搜集整理更新学习本行业内滥用行为的违法违规案例； 定期排查评估各项交易、业务流程、产品服务中的高风险行为。 中小型企业是指具有一定用户规模、有限业务种类、有限经济体量、有限限制能力的企业。	加 1 分。
	减分项		
	行政处	对于垄断行为或者不正当竞争行为，收到监管机构的：	每一情形扣 1

一级指标	分值	二级指标	评分标准
	罚	行政处罚决定书； 监管意见且未及时整改、处理的； 约谈调查且未及时整改、处理的。	分，针对同一行为不重复扣分。
	民事诉讼	针对垄断行为或者不正当竞争行为被提起民事诉讼后，被司法机关认定实体违法或侵权属实的。	一个诉讼扣 1 分。
	多次违反	对已经被处罚、警告、约谈、调查或起诉后败诉的行为，再次从事该行为且被处罚或起诉后败诉的。	出现一次扣 1 分。
	滥用行为	对大型企业，未建立本行业内滥用行为的重点监控和预防机制，包括：定期搜集整理更新学习本行业内滥用行为的违法违规案例；定期排查评估各项交易、业务流程、产品服务中的高风险行为。大型企业是指具有较大或超大的用户规模、较广或超广业务种类、较高或超高经济体量、较多业务范围、较强或超强限制能力的企业。例如，平台上年度在中国的年活跃用户不低于 5000 万；平台上年末市值（估值）不低于 1000 亿人民币；平台具有较强的限制商户接触消费者（用户）的能力等。	扣 1 分。

5.3.2.5 知识产权侵权风险识别评价体系

一级指标	分值	二级指标	评分标准
		基础项（15）	
知识产权 违规/侵权	著作侵权 (3)	建立著作权合规/侵权预防体系，包括： 建立事前审查过滤机制，排查明显侵权风险或者商业风险，包括但不限于建立开源合规/侵权预防体系：（i）建立专业团队或长期合作顾问就开源软件侵权风险进行审查与合规，并就审查合规建立档案库进行备份及待查；（ii）建立开源软件协议模板手册及相关人员培训指南，并就模板与指南建立资料库进行备份及待查； 以及 建立职务作品、委托创作、共同创作作品权属安排方案模板、风险排查手册及相关人员培训指南，并就模板与指南建立资料库进行备份及待查；并向全员开展著作权保护宣传、培训、考试，使员工充分知悉著作权保护及合规遵从的义务及责任，并就相关培训记录及成效建立档案库进行备份及待查	基础项 每达标一项 计 1 分
	商标侵权 (3)	建立商标权合规/侵权预防体系，包括： 建立商标注册前侵权风险排查机制，并就相关的制度规则及实际运行情况建立资料库及档案库进行备案及待查； 建立（自有/第三方）商标正当、规范使用手册（避免跨类别使用或许可、侵犯他人先权利的使用、对他人商标的不规范使用），并就相关手册建立资料库进行备份及待查；以及 向全员开展商标权保护宣传、培训、考试，使员工充分知悉商标权保护及合规遵从的义务及责任，并就相关培训记录及成效建立档案库进行备份及待查	基础项 每达标一项 计 1 分
	专利侵权 (3)	建立专利权合规/侵权预防体系，包括： 建立关键产品事前自由实施分析规则，并就相关的制度规则及实际运行情况建立资料库及档案库进行备案及待查； 建立职务发明、委托发明、共同发明权属安排方案模板、风险排查手册及相关人员培训指南，并就模板与指南建立资料库进行备份及待查；并向全员开展专利权保护宣传、培训、考试，使员工充分知悉专利权保护及合规遵从的义务及责任，并就相关培训	基础项 每达标一项 计 1 分

一级指标	分值	二级指标	评分标准
		记录及成效建立档案库进行备份及待查；以及 建立员工前雇主离职及入职信息、声明函签署档案库、职务发明 奖励方案，并就相关方案及模板建立资料库，就员工签署模板建 立档案库进行备份及待查	
商业秘密 侵权（3）		建立商业秘密合规/侵权预防体系，包括： 建立商业秘密保密管理规则，包括设立商业秘密管理部门、对商 业秘密分级采取保密措施、对涉密主体采取保密措施、规范商业 秘密管理流程，并就相关保护内部商业秘密的制度规则建立资料 库进行备份及待查； 建立保密培训手册，就任何合作项目中获悉的他方保密信息的保 密义务遵守注意事项制定指南，对员工在商业活动中尊重与保护 他人商业秘密提出明确要求，确保员工合法、合约地开展各项业 务活动，并就相关外部商业秘密行为规范的制度规则建立资料库 进行备份及待查； 向全员开展商业秘密保护宣传、培训、考试，使员工充分知悉商 业秘密合规遵从的义务及责任，并就相关培训记录及成效建立档 案库进行备份及待查； 将商业秘密保护的管理要求融入到研发、销售、采购、人力资源 等业务流程中，定期审视并结合业务运作中发现的问题和案例持 续进行管理改进，不时更新，并就相关规则更新及版本建立档案 库进行备份及待查；以及 通过检查、审计等方式对保护商业秘密工作情况进行监督，确保 政策、制度及流程有效落地，建立问责机制，发布商业秘密违规 的问责制、信息安全违规问责定级标准等文件，对违规行为进行 问责，并就实际监督及运行情况及记录建立档案库进行备份及待 查	基础项 达标第一项 计 1 分，其余 每达标一项 计 0.5 分
域名侵权 （3）		建立域名合规/侵权预防体系，包括： 建立域名注册事前侵权风险排查机制，并就相关的制度规则及实 际运行情况建立资料库及档案库进行备案及待查；以及 建立域名备案合法合规的方案手册，并就相关手册建立资料库进 行备份及待查	基础项 每达标一项 计 1.5 分
减分项			
侵权警告 （0.5/次）		收到（1）著作权侵权；（2）商标权侵权；（3）专利权侵权；或 者（4）商业秘密侵权警告函，且未及时或妥善处理	每触发一项， 每次扣 0.5 分，扣分累计
侵权诉讼 （1-1.5/ 次）		被提起（1）著作权侵权；（2）商标权侵权；（3）专利权侵权； 或者（4）商业秘密侵权诉讼，且（i）未及时处理；（ii）被相关 权力机构认定侵权属实；（iii）被相关权力机构认定侵权属实，且 被认定属于恶意侵权，或者适用惩罚性赔偿的	每触发（i）（ii） 情形任何一 项的，每次扣 1 分，扣分累 计 每触发（iii） 情形任何一 项的，每次扣 1.5 分，扣分 累计
行政处罚 （1/次）		收到监管机构出具的各类知识产权相关的（1）处罚决定；（2） 监管意见；或者（3）风险提示等。知识产权侵权类型包括：（1） 著作权侵权；（2）商标权侵权；（3）专利权侵权；或者（4）商	每触发一项 扣 1 分，扣分 累计

一级指标	分值	二级指标	评分标准
	平台企业注意义务 (0.1-0.5/次)	业秘密侵权	
		作为平台类企业，收到协助处理知识产权受到侵害通知，未及时采取删除、屏蔽、断开链接、终止交易和服务等必要措施，导致侵权损害扩大的。知识产权侵权类型包括：（1）著作权侵权；（2）商标权侵权；（3）专利权侵权；或者（4）商业秘密侵权	每触发一项扣 0.3 分，扣分累计
		作为平台类企业，知道或者应当知道平台内经营者存在知识产权侵权行为，未采取必要措施，且相关侵权行为经相关权力机构认定属实的。知识产权侵权行为类型包括：（1）著作权侵权；（2）商标权侵权；（3）专利权侵权；或者（4）商业秘密侵权	每触发一项扣 0.2 分，扣分累计
		作为平台类企业，未建立完善知识产权侵权投诉机制，未建立明确有效的知识产权投诉渠道，未提供明确指引的	扣 0.5 分
		作为平台类企业，收到协助处理知识产权侵害通知，未及时向投诉方/被投诉方反馈处理结果的。知识产权侵权类型包括：（1）著作权侵权；（2）商标权侵权；（3）专利权侵权；或者（4）商业秘密侵权	每触发一项扣 0.1 分，扣分累计

5.3.2.6 环境风险识别评价体系

一级指标	分值	二级指标	分值
环境风险	7	【1】综合环境管理 依法进行环境影响评价。自行或委托技术单位对可能产生环境影响的项目进行环评，依法编制环境影响报告书或报告表，包括项目概况、周围环境现状、预计产生影响、保护措施及技术论证、损益分析等内容，并依法进行公开。建立环境管理体系。建立、实施、保持并持续改进环境管理体系，包括制定岗位操作手册、明确人员岗位职责、建立台账、定期巡查检修等。 建立环境保护责任和考核制度。明确单位责任人和相关人员的责任，由确定的责任主体及时开展纠偏与解决工作。 建立风险报告和防控制度。制定突发环境事件应急预案，并报环境保护主管部门和有关部门备案。在发生或者可能发生突发环境事件时，应当立即采取措施处理并及时通报可能受到影响的单位和居民，并向环境报回主管部门和有关部门报告。 依法进行信息披露。依法、及时、真实、准确、完整地披露环境管理、碳排放信息等环境信息，建立健全环境信息依法披露管理制度。	2.5（应全部达标）
		【2】绿色能效管理 （1）能源高效利用情况。 （2）倡导绿色采购，尽量选择可降解和回收再造材质的产品或首选二级能耗或高效产品。 能源资源绿色管理（能源使用管控、水资源使用管控、节能诊断服务、第三方测评等） 设备绿色管理（电器电子有害物质限制使用、废旧电子电器处理、废弃物处理）	3（应全部达标）
		【3】节能合规 加强节能管理，制定并实施节能计划和节能技术措施。定期开展节能教育和岗位节能培训。	1.5（应全部达标）

一级指标	分值	二级指标	分值
		减少办公设备待机能耗，下班及时关闭室内电源	
		加分项（+3 分）	
		积极推行无纸化办公，做好垃圾分类 可再生能源电力消纳、绿色电力证书消费、余热回收、电池梯级利用等综合能源利用 积极进行环保宣传，包括标语、海报、视频等 用能单位制定奖惩制度，对节能工作取得成绩的集体、个人给予奖励 获得国际或国家级环保认证、奖项	每达标一项加 0.5 分
		减分项（-4 分）	
		违规向水体排放、倾倒城镇垃圾和其他废弃物。	-1（若出现一项情况则全部扣分）
		擅自倾倒、堆放、丢弃、遗撒固体废物。	-1（若出现一项情况则全部扣分）
		使用或转让给他人使用列入淘汰名录的落后生产工艺、设备。	-1（若出现一项情况则全部扣分）
		过去 12 个月内（本年度内）公司收到监管机构出具的与环境保护相关的： 处罚决定。 监管意见。 风险提示。	-1（若出现一项情况则全部扣分）

5.3.2.7 劳动合规风险识别评价体系

一级指标	分值	二级指标	评分标准
劳动合规风险	用工关系（2.5）	基础项（7）	
		以合法、合规的方式进行劳动用工，包括： （1）依法建立用工关系，包括但不限于：（i）依法进行员工招聘和相应的背景调查，避免在招聘过程中侵犯候选人的个人信息、不得进行就业歧视，（ii）恰当地选择用工形式，并相应签订书面协议，对于符合劳动关系特征的员工均应依法签订书面劳动合同，其余员工应根据具体情况，恰当地在劳务派遣、服务外包和大学生实习等不同用工形式之间进行选择，（iii）依法依规签订劳动合同，包括：全日制书面劳动合同最晚应在实际用工之日起一个月内签订，劳动合同应至少具备法律规定的必备条款，依法与员工签订保密、知识产权和（如有必要的）竞业限制协议，员工的试用期时长和次数应符合法律规定等，（iv）除法律规定的特殊情形外，原则上不得与员工约定服务期和违约金，以及（v）聘用外籍员工的，应确保外籍员工持有有效的工作许可和工作居留等。 （2）合法、合规的履行用工合同，包括但不限于：（i）除符合法律规定的可单方变更劳动合同的情形外，劳动合同的变更（如工作岗位、工作内容、员工薪酬、工作地点的调整等）均应与员工协商一致，（ii）企业进行业务调整、部门整体撤销等的，应依法进行员工安置，包括企业内转岗、就劳动关系的处理与员工进行协商等，（iii）依法进行劳务派遣和服务外包员工的用工管理，包括但不限于，确保劳务派遣员工同工同酬、（除出于服务质量和安全生产之目的外）不得对服务员进行直接管理等。 （3）以合法的方式解除用工关系，包括但不限于：（i）恰当地选择劳动合同的解除方式，劳动合同的解除应确保符合法律规定的流程，如需单方解除员工的，应确保员工之情形符合法律规定的可以单方解除劳动合同的情形；（ii）劳务派遣员工的退回应符合法律规定的情	基础项 达标第一 项计 0.5 分，达标 第二、三 项各计 1 分

一级指标	分值	二级指标	评分标准
		形；（iii）员工离职的，企业应依法及时、足额支付员工的各类离职款项，包括但不限于：最后工资、法定经济补偿金、未休年休假补偿、医疗补助费（如有）和一次性伤残就业补助金（如有）等。	
	工时与休假（1.5）	依法确定员工的工时制度和休息办法，合理安排员工的工作时间，保证员工休息和休假的权利，包括： （1）制定关于工作时间的企业规章制度，合理确定不同岗位的工时制度，依法为适用特殊工时制度的岗位申请政府许可； （2）建立加班管理制度，确有必要加班的、应确保员工的加班时间不超过法律规定的最高时限，及时进行加班调休和加班费支付；以及 （3）制定关于休息与休假的企业规章制度，确保员工能依法享有所有的休息与休假，包括但不限于法定休息日、法定节假日、年休假、病假、产假、陪产假、哺乳假、育儿假等。	基础项 每达标一项计 0.5 分
	劳动报酬（1）	及时、足额支付所有员工的劳动报酬，包括： （1）在代扣代缴员工应缴的各类社会保险、住房公积金、个人所得税和其他法定扣缴项后，及时、足额向员工支付各类劳动报酬，包括但不限于基本工资、绩效工资、加班工资、奖金、各类津贴补贴等； （2）员工的劳动报酬调整和扣减应符合法律规定，包括但不限于： （i）原则上调薪应与员工协商一致（单方提高员工劳动报酬水平的除外），（ii）确保员工在休假期间可依法获得劳动报酬和/或假期待遇，不能因员工休假而无故扣减劳动报酬，（iii）因员工不胜任岗位进行调岗的，不建议同时降薪，如确有必要降薪的，应确保降薪水平在合理、员工可接受的范围内。	基础项 每达标一项计 0.5 分
	社会保险与住房公积金（1）	依法依规为员工缴纳社会保险和住房公积金，确保员工能够及时享受到社会保险待遇，包括： （1）及时、足额为员工缴纳各类社会保险（基本养老保险、基本医疗保险、生育保险、失业保险和工伤保险）和住房公积金，包括但不限于：（i）及时为入职和离职员工办理社会保险和住房公积金账户的转入和转出，（ii）依法扣缴员工的个人应缴部分和依法缴纳企业承担部分，确保每个员工的缴纳基数、缴纳比例和缴纳时间均符合法律规定； （2）在员工符合法定情形时，应及时为员工申领社会保险待遇，包括但不限于：（i）对于工伤员工，应及时安排工伤鉴定和劳动能力鉴定，确保员工的工伤保险报销和各类工伤待遇，（ii）及时为产假员工申领生育津贴，（iii）离职员工符合失业保险的申领条件的，企业应根据离职员工要求配合出具相关材料，（iv）员工达到退休年龄的，企业应及时为员工办理退休手续。	基础项 每达标一项计 0.5 分
	劳动安全与劳动保护（1）	企业应重视安全生产合规，加强职业病管理和“三期”女员工的特殊劳动保护，包括： （1）企业应重视安全生产合规，加强职业病管理，包括但不限于： （i）企业不得制定损害劳动者安全健康的考核指标，并应严格遵守安全生产相关法律法规，（ii）应配备必要的劳动安全卫生设施和劳动防护用品，及时对劳动工具的安全和合规状态进行检查，（iii）加强安全生产和职业卫生教育培训，重视劳动者身心健康，及时开展心理疏导，（iv）强化恶劣天气等特殊情形下的劳动保护，最大限度减少安全生产事故和职业病危害；以及 （2）依法为“三期”女员工提供特殊劳动保护，包括但不限于：（i）保障女员工依法享有产检假、产假、哺乳假等假期及相应假期内的劳动报酬和/或津贴，（ii）加强三期女员工的劳动保护，不得违法解除	基础项 每达标一项计 0.5 分

一级指标	分值	二级指标	评分标准
		或终止“三期”女员工的劳动关系。	
		加分项	
	合规管理 (1)	进行用工合规管理体系建设，包括： (1) 企业应建立用工合规管理制度和体系，包括但不限于：(i) 依法制定劳动用工领域合规管理制度（如人事管理和劳动纪律、报销制度、商业行为守则、保密和知识产权制度、反贿赂和反腐败制度、反骚扰制度、员工舞弊相关制度、网络数据安全和个人信息保护制度等），(ii) 合理界定法律与合规部门、人事部门和业务部门等之间的用工管理职责，(iii) 保证相关管理办法的适用性和规范性，对于涉及员工切身利益的规章制度应依法进行民主协商和公示；以及 (2) 企业应加强劳动风险管控，包括但不限于：(i) 企业应结合自身实际情况，梳理劳动用工领域涉及的法律法规、规章制度，定期对劳动人事管理相关部门员工进行法规和典型用工风险的培训与提示； (iii) 定期对企业用工领域合规管理制度和劳动人事文件进行检查、审阅和更新，实现合规风险的有效防控，(iii) 及时进行具体劳动用工行为的合规风险分析，做好风险预警提示等。	加分项 每达标一 项加 0.5 分
	员工激励 制度的建 立 (1)	企业应通过“正激励”和“负激励”相结合的方式，建立合理、完善、有效的员工激励制度，包括但不限于：建立科学合理的绩效管理制度并实际实施，为员工搭建有效的薪酬福利提升和职业晋升路径，通过限制性股票、期权等多样化的激励手段进行员工激励等。 建议企业在法定要求基础上，主动增设其他带薪假期的，可获得加分。 企业在法定要求基础上，主动增设员工福利的，例如体检、商业保险等，可获得加分。	加分项 达标加 1 分
		减分项	
	劳动仲裁/ 诉讼 (0.2/ 次)	被提起各类劳动仲裁（及相应的劳动诉讼），且 (i) 未及时处理；(ii) 经劳动仲裁（或可能的诉讼一审、二审和再审），司法裁审机构全部或部分支持员工的仲裁/诉讼请求的。	每触发(i) (ii) 情形 任何一项 的，每次 扣 0.2 分， 扣分累计
	行政处罚 (0.5/次)	收到监管机构（如劳动行政部门、劳动监察机构、社会保险和住房公积金征缴机构等）出具的各类劳动相关的 (1) 处罚决定，(2) 监管意见，(3) 员工投诉的处理意见，(4) 整改通知，或者 (5) 风险提示等。	每触发一 项扣 0.5 分，扣分 累计

5.4 合规整改措施

5.4.1 总则

企业应定期对自身合规管理体系、平台主体责任、数据与网络安全保障、市场秩序维护（竞争合规）、知识产权保护、环境与劳资风险、合规改进措施等进行系统全面的评价，发现和纠正合规管理贯彻执行中存在的问题，促进合规体系的不断完善。

对已发生的合规风险或合规测试发现的合规缺陷，应提出整改意见并监督有关部门进行整改。

5.4.2 合规整改措施评价体系

一级指标	二级指标	分值
合规整改 响应机制	【1】与监管部门和评价机构的沟通	15（每项 5 分）
	1) 建立与监管部门的常态化沟通机制	

(27 分)	2) 建立与评价机构的定期评估机制	
	3) 建立长期有效的评估-反馈机制	
	【2】 针对投诉、争议等提出解决措施或方案 (1) 及时公示相关纠纷处理过程及结果, 并就相关处理结果建立档案库进行备份及待查 (2) 出现问题时, 企业积极配合, 协助处理相关问题, 并及时公示整改解决方案	12 分 (每项 6 分)
持续改进计划 (30 分)	【1】 针对不合格项制定详细整改计划 (1) 根据评估结果制定详细整改方案 (2) 设立专门合规整改部门 (3) 制定详细的内外部协同整改推进计划	15 (每项 5 分)
	【2】 制定内部整改协同推进计划 (1) 根据整改方案, 建立部门整改协同机制 (2) 定期召开部门协同会议, 定期汇报整改情况及结果, 并就相关方案及整改结果建立档案库进行备份及待查 (3) 设立合规整改负责人, 协同推进内外部沟通和联系	15 (每项 5 分)
	建立专业团队或长期合作顾问定期开展内部合规审查	
合规风险排查 (43 分)	(1) 定期排查业务开展中违反法律、规则和准则的风险 (3 分), 出具相关审查报告 (2 分), 并就相关审查评估报告建立档案库进行备份及待查 (2 分); 由公司监督部门等专门部门就相关审查报告提出的整改意见实际落实情况在至多一个月内进行记录备份 (3 分), 并计入档案库进行备份及待查 (2 分);	12 分
	(2) 定期排查各类制度文件中不符合法律、规则和准则可能引起的合规风险 (3 分), 出具相关审查报告 (2 分), 并就相关审查评估报告建立档案库进行备份及待查 (2 分);	7 分
	(3) 关注法律、规则、准则以及所在地法治环境重大变化对经营活动产生的合规风险 (3 分), 出具相关审查报告 (2 分), 并就相关审查评估报告建立档案库进行备份及待查 (2 分); 由公司监督部门等专门部门就相关审查报告提出的整改意见实际落实情况在至多一个月内进行记录备份 (3 分), 并计入档案库进行备份及待查 (2 分);	12 分
	(4) 评估企业推出新模式、新活动产生的合规风险 (3 分), 出具相关审查报告 (2 分), 并就相关审查评估报告建立档案库进行备份及待查 (2 分); 由公司监督部门等专门部门就相关审查报告提出的整改意见实际落实情况在至多一个月内进行记录备份 (3 分), 并计入档案库进行备份及待查 (2 分)。	12 分
	加分项	
	积极参与内外部合规培训	5
	积极宣贯相关政策法规	5
	积极接入相关监测平台	5

附录 A

名词解释

1 个人信息 Personal information

是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

2 数据 Data

是指任何以电子或者其他方式对信息的记录。

3 数据安全 Data security

是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

4 网络安全 Cyber security

是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

5 虚假宣传 False advertising

是指对经营者自身或者其商品的性能、功能、质量、曾获荣誉、资格资质等作虚假或者引人误解的商业宣传，欺骗、误导消费者或者相关公众。

6 混淆行为 Confusion Act

指采取不当方式，引人误认为自身商品是他人商品或者与他人存在特定联系。

7 不当有奖销售 Improper prize-giving sale

是指经营者销售商品或者提供服务，附带性地向购买者提供物品、金钱或者其他经济上的利益时，欺骗消费者、公示信息不明确，或超过特定金额。

8 商业诋毁 The discrediting

是指编造、传播虚假信息或者误导性信息，损害竞争对手的商业信誉、商品声誉。

9 商业贿赂 Commercial Bribery

是指采用财物或者其他手段贿赂交易相对方的工作人员、受交易相对方委托办理相关事务的单位或者个人，或者利用职权或者影响力影响交易的单位或者个人，以谋取交易机会或者竞争优势。

10 流量劫持 Traffic Hijacking

是指利用技术手段、通过影响用户选择或者其他方式，在未经其他经营者同意的情况下，在其合法提供的网络产品或者服务中，插入链接、强制进行目标跳转。

11 妨碍干扰 Impeding and disturbing

是指利用技术手段、通过影响用户选择或者其他方式，误导、欺骗、强迫用户修改、关闭、卸载其他经营者合法提供的网络产品或者服务。

12 恶意不兼容 Malicious incompatibility

是指利用技术手段、通过影响用户选择或者其他方式，恶意对其他经营者合法提供的网络产品或者服务实施不兼容。

13 关键产品 Critical products

指与企业主要生产经营范围相关、主营业务相关的核心产品。

14 著作权 Copyright

指依照中华人民共和国著作权法，自然人、法人或者其他组织对文学、艺术和科学作品享有的财产权利和精神权利，为避免疑义，还包括与著作权有关的权利。

15 商标权 Trademarks

指依照中华人民共和国商标法，民事主体享有的在特定的商品或服务上以区分来源为目的排他性使用特定标志的权利。

16 专利权 Patent right

指依照中华人民共和国专利法，发明人或设计人享有的，经过向国家申请，以向社会公开发明创造的内容，以及发明创造对社会具有符合法律规定的利益为前提，经过国家相关部门审查并核准授权的，根据法定程序在一定期限内就授权专利享有的权利。

17 商业秘密 Business secret

指依照反不正当竞争法，民事主体享有的不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。

18 自由实施 Freedom to Operate (FTO)

指企业在不侵犯他人专利权的情况下，有权对技术自由地进行使用和开发，并将利用该技术生产的产品或服务投入市场。

19 固体废物 Solid waste

是指在生产、生活和其他活动中产生的丧失原有利用价值或者虽未丧失利用价值但被抛弃或者放弃的固态、半固态和置于容器中的气态的物品、物质以及法律、行政法规规定纳入固体废物管理的物品、物质。经无害化加工处理，并且符合强制性国家产品质量标准，不会危害公众健康和生态安全，或者根据固体废物鉴别标准和鉴别程序认定为不属于固体废物的除外。

20 劳动合同 Employment contract

指适格劳动者和用人单位之间确立劳动关系，明确双方权利和义务的协议。

21 劳务派遣 Labor dispatch

指由劳务派遣单位与被派遣劳动者订立劳动合同，劳务派遣单位根据与被派遣劳动者的用工单位之间签订的协议，将被派遣劳动者指派至用工单位处工作的一种用工模式。

22 服务外包 Service outsourcing

指企业将其部分业务或职能工作发包给相关具有从事该项业务承揽资质（如外包业务中涉及资质要求）的外包机构，由该机构自行安排服务人员按照发包企业的要求完成相应的业务或工作。

23 劳动报酬 Remuneration

指用人单位依据国家有关规定和劳动关系双方的约定，以货币、有价证券或其他形式支付给劳动者的报酬，包括正常工作时间工资、奖金、津贴、加班工资及特殊情况下支付的劳动报酬等。

24 特殊工时制度 Special working hour system

指企业确因生产经营特点和工作的特殊性不能实行标准工时制（即每日工作 8 小时，每周工作 40 小时），经人社保行政部门批准，所实施的其他工作和休息办法，包括综合计算工时工作制或者不定时工作制等。

附 录 B

相关法律法规依据

1 网络安全、数据安全与个人信息保护相关法律法规

《中华人民共和国国家安全法》
 《中华人民共和国网络安全法》
 《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》
 《中华人民共和国民法典》
 《中华人民共和国消费者权益保护法》
 《中华人民共和国电子商务法》
 《全国人大常委会关于维护互联网安全的决定》（2009 修正）
 《全国人大常委会关于加强网络信息保护的决定》（2012）
 《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释（法释〔2017〕10 号）》
 《网络安全审查办法》
 《互联网信息服务算法推荐管理规定》
 《计算机信息系统安全保护条例》
 《工业数据分类分级指南（试行）》
 《儿童个人信息网络保护规定》
 《电信和互联网用户个人信息保护规定》
 《汽车数据安全若干规定（试行）》
 《信息安全等级保护管理办法》
 《通信短信息服务管理规定》
 《App 违法违规收集使用个人信息行为认定方法》
 《App 违法违规收集使用个人信息自评估指南》
 《常见类型移动互联网应用程序必要个人信息范围规定》
 《个人金融信息保护技术规范》（银发〔2020〕45 号）
 《金融消费者权益保护实施办法》（中国人民银行令〔2020〕第 5 号）
 《信息安全技术 个人信息安全规范》（GB/T 35273-2020）
 《信息安全技术 个人信息安全影响评估指南》（GB-T 39335-2020）
 《网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评估指南》
 《信息安全技术 信息系统安全等级保护实施指南》（信安字〔2007〕10 号）
 《信息安全技术 信息系统安全等级保护定级指南》（信安字〔2007〕11 号）
 《网络数据安全条例（征求意见稿）》
 《数据出境安全评估办法（征求意见稿）》
 《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》
 《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》

2 竞争合规法律法规

在竞争法领域，对互联网企业的监管主要涉及到以下法律规定：

2.1 反垄断领域

《反垄断法》
 《经营者集中审查暂行规定》
 《禁止垄断协议暂行规定》
 《禁止滥用市场支配地位行为暂行规定》

《关于禁止滥用知识产权排除、限制竞争行为的规定》
 《国务院反垄断委员会关于相关市场界定的指南》
 《国务院反垄断委员会关于平台经济领域的反垄断指南》
 《国务院反垄断委员会关于知识产权领域的反垄断指南》
 《经营者反垄断合规指南》
 《企业境外反垄断合规指引》
 《最高人民法院关于审理因垄断行为引发的民事纠纷案件应用法律若干问题的规定》

2.2 反不正当竞争领域：

《反不正当竞争法》
 《关于侵犯商业秘密行为的若干规定》
 《关于禁止商业贿赂行为的暂行规定》
 《规范促销行为暂行规定》
 《关于禁止不正当有奖销售行为的若干规定（征求意见稿）》
 《禁止网络不正当竞争行为规定（公开征求意见稿）》
 《最高人民法院关于适用〈中华人民共和国反不正当竞争法〉若干问题的解释》
 《最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定》

2.3 其他和企业市场中行为相关的法律规范

《价格法》
 《价格管理条例》
 《价格违法行为行政处罚规定（修订征求意见稿）》
 《电子商务法》
 《个人信息保护法》
 《中国人民银行关于规范支付创新业务的通知》
 《网络交易监督管理办法》
 《互联网信息服务算法推荐管理规定》

3 知识产权保护领域法律法规

3.1 著作权领域

《中华人民共和国著作权法》
 《中华人民共和国著作权法实施条例》
 《著作权集体管理条例》
 《计算机软件保护条例》
 《信息网络传播权保护条例》
 《计算机软件著作权登记办法》
 《最高人民法院关于审理著作权民事纠纷案件适用法律若干问题的解释》
 《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》
 《互联网著作权行政保护办法》
 《互联网出版管理暂行规定》

3.2 商标权领域

《中华人民共和国商标法》
 《中华人民共和国商标法实施条例》
 国家工商总局关于执行修改后的《中华人民共和国商标法》有关问题的通知
 《最高人民法院关于审理商标民事纠纷案件适用法律若干问题的解释》
 《最高人民法院关于审理注册商标、企业名称与在先权利冲突的民事纠纷案件适用法律若干问题的解释》
 《最高人民法院关于审理涉及驰名商标保护的民事纠纷案件适用法律若干问题的解释》
 《最高人民法院关于人民法院对注册商标权进行财产保全的解释》

《最高人民法院关于审理商标授权确权行政案件若干问题的规定》
 《最高人民法院关于审理商标案件有关管辖和法律适用范围问题的解释》
 《集体商标、证明商标注册和管理办法》
 《工业互联网标识管理办法》
 《中国商标法律保护和执法指南》
 《商标侵权判断标准》
 《商标注册档案管理办法》

3.3 专利权领域

《中华人民共和国专利法》
 《中华人民共和国专利法实施细则》
 最高人民法院关于学习贯彻修改后的《专利法》的通知
 《最高人民法院关于审理专利纠纷案件适用法律问题的若干规定》
 《最高人民法院关于审理侵犯专利权纠纷案件应用法律若干问题的解释（二）》
 《最高人民法院关于审理专利授权确权行政案件适用法律若干问题的规定（一）》
 《专利导航指南》（GB/T39551-2020）
 《专利申请受理和审批办事指南》
 《查处假冒专利行为和办理专利标识标注不规范案件指南》
 《专利行政保护复议与应诉指引》

3.4 商业秘密领域

《中华人民共和国反不正当竞争法》
 《关于禁止侵犯商业秘密行为的若干规定》
 《最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定》
 《最高人民法院关于审理不正当竞争民事案件应用法律若干问题的解释》
 《最高人民法院关于审理因垄断行为引发的民事纠纷案件应用法律若干问题的规定》
 《最高人民法院关于审理技术合同纠纷案件适用法律若干问题的解释》
 《计算机信息系统保密管理暂行规定》

3.5 域名领域

《互联网域名管理办法》
 《最高人民法院关于审理涉及计算机网络域名民事纠纷案件适用法律若干问题的解释》

3.6 综合领域

《电子商务法》
 《中华人民共和国和美利坚合众国政府经济贸易协议》
 《企业知识产权管理规范》（北京市市场监督管理局）
 《知识产权“一件事”集成服务规范》（地方标准信息服务平台）
 《电子商务领域知识产权侵权咨询服务规范》
 《知识产权信息公共服务工作指引》
 《国家知识产权信息公共服务网点备案实施办法》

4 环境保护领域法律法规

《中华人民共和国环境保护法》
 《中华人民共和国环境影响评价法》
 《中华人民共和国水污染防治法》
 《中华人民共和国固体废物污染环境防治法》
 《中华人民共和国节约能源法》
 《企业环境信息依法披露管理办法》
 《排污许可管理办法》

《中华人民共和国水污染防治法实施细则》
 《一般工业固体废物管理台账制定指南（试行）》
 《固定资产投资项目节能审查办法》
 《环境管理体系 要求及使用指南》（GB/T 24001-2016）
 《排污单位环境管理台账及排污许可证执行报告技术规范 总则（试行）》（HJ944-2018）

5 劳动领域法律法规

5.1 综合领域

《中华人民共和国劳动法》
 《中华人民共和国劳动合同法》
 《关于贯彻执行〈中华人民共和国劳动法〉若干问题的意见》
 《关于实行劳动合同制度若干问题的通知》
 《中华人民共和国劳动争议调解仲裁法》
 《企业劳动争议协商调解规定》
 《劳动人事争议仲裁办案规则》
 《劳动人事争议仲裁组织规则》
 《最高人民法院关于审理劳动争议案件适用法律问题的解释（一）》

5.2 用工关系领域

《集体合同规定》
 《劳务派遣暂行规定》
 《劳务派遣行政许可实施办法》
 《关于非全日制用工若干问题的意见》
 《企业经济性裁减人员规定》

5.3 工时与休假领域

《职工带薪年休假条例》
 《企业职工带薪年休假实施办法》
 《全国年节及纪念日放假办法》
 《国务院关于职工工作时间的规定》
 《劳动部关于企业实行不定时工作制和综合计算工时工作制的审批办法》
 《关于职工工作时间有关问题的复函》
 《中华人民共和国人口与计划生育法》
 《企业职工患病或非因工负伤医疗期规定》
 《关于贯彻〈企业职工患病或非因工负伤医疗期规定〉的通知》

5.4 劳动报酬领域

《关于工资总额组成的规定》
 《〈关于工资总额组成的规定〉若干具体范围的解释》
 《工资支付暂行规定》
 《对〈工资支付暂行规定〉有关问题的补充规定》
 《最低工资规定》
 《工资集体协商试行办法》
 《关于职工全年月平均工作时间和工资折算问题的通知》
 《最高人民法院关于审理拒不支付劳动报酬刑事案件适用法律若干问题的解释》

5.5 社会保险与住房公积金领域

《中华人民共和国社会保险法》
 《工伤保险条例》

《失业保险条例》
《最高人民法院关于审理工伤保险行政案件若干问题的规定》
《国务院关于建立统一的企业职工基本养老保险制度的决定》
《国务院关于整合城乡居民基本医疗保险制度的意见》
《住房公积金管理条例》
《社会保险费征缴暂行条例》
《企业职工生育保险试行办法》
《最高人民法院关于审理工伤保险行政案件若干问题的规定》
《实施<中华人民共和国社会保险法>若干规定》
《社会保险行政争议处理办法》
《社会保险费征缴监督检查办法》
《失业保险金申领发放办法》
《企业年金办法》
《因工死亡职工供养亲属范围规定》
《工伤认定办法》

5.6 劳动安全与劳动保护领域

《中华人民共和国职业病防治法》
《中华人民共和国安全生产法》
《最高人民法院、最高人民检察院关于办理危害生产安全刑事案件适用法律若干问题的解释》
《中华人民共和国妇女权益保障法》
《女职工劳动保护特别规定》
《残疾人就业条例》
《禁止使用童工规定》
《未成年工特殊保护规定》
《非法用工单位伤亡人员一次性赔偿办法》

参考文献

[1]

