ICS 35.240
CCS L 70

团 体 标 准

T/CECC XX —202X

数据产品开发应用合规指南

Data product development and application compliance guide

202X-XX-XX 发布 202X-XX-XX 实施

中国电子商会 发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由北京之合网络科技公司（智合标准中心）提出并负责组织。

本文件由中国电子商会归口。

本文件起草单位：

本文件主要起草人：

引　　言

为应对数据要素市场化配置中数据产品开发应用面临的安全治理与权益保护挑战，促进数据产业合规有序发展，引导数据处理活动符合安全与发展协同推进的要求，根据《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》等法律法规，以及《关键信息基础设施安全保护条例》《网络数据安全管理条例》《数据出境安全评估办法》等相关部门规章，结合我国数据领域技术创新与产业发展实际，制定本文件。

数据产品开发应用合规指南

1 范围

本文件规定了数据产品在规划、设计、开发、测试、封装、部署、交易、运营、下线及处置的各个应用环节中应遵循的数据产品开发应用合规原则与合规要求，以及可供借鉴参考的具体合规手段与合规方法。

本文件适用于指导数据产品提供者向中华人民共和国境内公众提供数据产品过程中所开展的数据产品开发应用合规工作。

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 42755-2023 人工智能 面向机器学习的数据标注规程

GB/T 43697-2024 数据安全技术 数据分类分级规则

T/CECC 027-2024 生成式人工智能数据应用合规指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据产品 Data Product

经过采集、加工、分析、整合等处理过程、形成可独立或组合使用，以满足特定用户需求的数据集、数据服务、数据报告、算法模型等产出物。

注：本文件所指的数据产品，包括但不限于数据集、数据API接口、数据分析报告、可视化数据应用、基于数据的算法模型，以及封装了数据资源和数据处理能力的应用软件或服务等。

3.2 **数据处理** Data Processing

数据的收集、存储、使用、加工、传输、提供、公开、删除等活动。

3.3

个人信息 Personal Information

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。

[来源：GB/T 42574-2023，定义 3.1]

3.4

敏感个人信息 Sensitive Personal Information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。

注：敏感个人信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满14周岁未成年人的个人信息。

[来源：GB/T 42574-2023，定义 3.2]

3.5

去标识化 De-identification

个人信息经过处理，使其在不借助额外信息的情况下，无法识别特定自然人的过程。

3.6

匿名化 Anonymization

个人信息经过处理，使其无法识别特定自然人且不能复原的过程。

3.7

数据分类分级 Data Classification and Grading

根据数据在国家安全、公共利益以及个人、组织合法权益方面的重要性和遭到篡改、破坏、泄露或者非法获取、非法利用后可能造成的危害程度，对数据进行分类并确定不同安全保护等级的过程。

3.8

个人信息保护影响评估 Personal Information Protection Impact Assessment；PIA

在数据处理活动开始前，对该活动可能对个人信息主体权益造成的影响（风险）进行分析、评估，并提出相应保护措施的过程。

3.9

提供者 Provider

以交互界面、可编程接口等形式面向我国境内公众提供生成式人工智能服务的组织或个人。
[来源：T/CECC 027-2024，定义 3.4]

3.10

数据资产 Data Asset

特定主体合法拥有或者控制的、能进行货币计量的，且能带来经济利益或社会效益的数据资源。
[来源：数据领域常用名词解释（第一批），国家数据局]

4 合规原则

数据产品开发应用应符合以下合规原则：

a) 合法、正当、必要与诚信原则：数据产品的开发与应用，其数据来源、处理目的和方式均应具备合法性基础，不得违反法律法规的规定。处理活动应具有正当性，不得采用误导、欺诈、胁迫等方式。数据处理应限于实现处理目的的最小范围，并遵循诚信原则，不得损害个人、组织及社会的合法权益；

b) 目的明确与最小化原则：在数据产品规划之初，应明确、具体地界定数据处理的目的。数据收集范围应与处理目的直接相关，并遵循最小必要原则，即仅收集和使用为实现该目的所必需的数据。不得因数据产品的迭代或功能扩展而进行超出初始目的的、无明确告知同意的数据处理活动；

c) 公开透明原则：数据处理者应以清晰易懂的方式，向个人信息主体公开数据处理规则，包括处理目的、方式、范围、存储期限、主体权利行使方式等。若数据产品涉及个人信息，应制定并公开专门的隐私政策；

d) 安全保障原则：数据处理者应履行数据安全保护义务，建立全流程数据安全管理制度，组织开展数据安全教育培训，并采取相应的技术措施和其他必要措施，保障数据免遭泄露、篡改、丢失。安全措施的强度应与数据的重要程度及面临的安全风险相匹配；

e) 个人信息主体权利保障原则：数据产品在设计和运营中，必须充分保障个人信息主体的各项法定权利，包括知情权、决定权、查阅权、复制权、更正权、删除权、撤回同意权等。应提供便捷的、清晰的渠道和机制，确保主体能够顺利行使其权利；
f) 合规设计原则：应在数据产品的初始阶段就将合规要求纳入考量，而非事后补救。在产品架构设计、功能规划、技术选型等各个环节，都应主动评估并融入数据安全与个人信息保护的控制措施，使合规成为产品的内在属性；
g) 交易过程可控原则：建立数据流通追溯机制，确保交易可监控、可审计；
h) 数据资产价值与风险管理平衡原则：在数据产品开发应用中，应平衡数据资产价值挖掘与风险管理的关系，确保在充分利用数据价值的同时，有效控制合规风险；
i) 权责一致原则：数据产品交易参与方在享有数据权益的同时，应当各自承担数据安全责任。

5 数据产品开发全生命周期合规要求

5.1 数据产品开发全生命周期阶段划分

一个完整的数据产品开发生命周期全过程，可划分为规划与需求分析、设计、开发、测试与验证、产品封装、发布与部署、流通交易、运营与维护、退出与处置等9个阶段。

5.2 各阶段合规要求

5.2.1 规划与需求分析阶段

规划与需求分析阶段是确定数据产品开发合规的关键环节。此阶段需开展如下合规性工作：

a) 合法合规性审查：评估数据产品的业务需求，就数据来源、数据内容、处理方式、处理目的是否符合《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》等法律法规的要求进行审查。如为自行生产的数据，需确保生产行为合法合规，不侵犯第三方合法权益；如为第三方提供，需审查数据来源的合法性，权属是否存在争议，并签订、保存数据处理协议或授权文件。严禁使用非法采集或来源不明的数据；
b) 必要性评估：对拟收集和使用的每一项数据（特别是个人信息）进行必要性评估，遵循最小必要原则；
c) 初步风险识别：识别数据产品可能涉及的数据安全风险和个人信息保护风险，特别是涉及生物识别信息、不满十四周岁未成年人的个人信息等敏感个人信息或数据出境、处理重要数据等高风险场景；
d) 内化合规需求：将数据安全和个人信息保护要求作为产品需求的一部分，与功能性需求一同纳入产品需求文档。

5.2.2 设计阶段

设计阶段需将合规要求转化为具体的设计方案和技术措施。此阶段需开展如下合规性工作：

a) 数据分类分级：依据 GB/T 43697-2024 及行业特定要求，对产品涉及的数据进行分类分级，并根据不同级别设计相应的安全保护策略；
b) 个人信息保护影响评估（PIA）：涉及处理敏感个人信息、利用个人信息进行自动化决策、对外提供或出境等高风险活动，必须开展 PIA。评估报告应记录处理目的、风险及已采取的保护措施；
c) 隐私增强技术应用设计：根据业务场景和数据类型，设计采用去标识化、匿名化、数据加密、差分隐私等技术方案，将可用于重识别自然人的数据单独存储；
d) 权限管理设计：设计基于角色的最小权限访问控制模型，确保不同岗位的用户只能访问其职责所需的最少数据；

e) 日志审计设计：设计全面的日志记录机制，覆盖所有对重要数据和个人信息的访问、修改、删除等操作，日志内容应包含操作人、时间、对象、操作类型等关键信息；
f) 用户权利实现机制设计：设计清晰、便捷的用户界面和后台流程，以支持用户行使其查阅、复制、更正、删除个人信息、撤回同意等权利。

5.2.3 开发阶段

开发阶段需确保设计阶段的合规要求在代码层面得到准确实现。此阶段需开展如下合规性工作：

a) 安全开发规范遵循：开发人员应遵循安全编码规范，避免常见的安全漏洞，如 SQL 注入、跨站脚本攻击等；
b) 合规组件使用：优先使用经过安全验证的、符合国密或国际主流标准的加密库和安全组件；
c) 代码审查：实施代码审查流程，将数据安全和隐私保护相关的代码作为审查重点；
d) 开发环境数据隔离：开发和测试环境应与生产环境严格隔离，禁止在开发、测试环境中使用未经脱敏的真实生产数据。

5.2.4 测试与验证阶段

测试与验证阶段是对数据产品合规性进行系统性验证的核心环节。此阶段需开展如下合规性工作：

a) 功能性合规测试：验证隐私政策告知、用户同意获取、用户权利行使等功能是否按设计实现；
b) 数据安全测试：
    1) 漏洞扫描与渗透测试：使用自动化工具，如OWASP ZAP, Burp Suite和人工渗透测试，发现潜在的安全漏洞；
    2) 权限控制测试：验证访问控制策略是否有效，防止越权访问；
    3) 数据脱敏有效性验证：测试去标识化或匿名化处理后的数据，评估其重标识风险。
c) 隐私合规性验证：
    1) 隐私政策一致性检查：核对产品的实际数据处理行为是否与隐私政策一致；
    2) 最小必要原则验证：检查产品是否收集了超出声明范围或业务非必需的数据。
d) 合规性验证流程：应制定详细的测试计划，创建测试用例，执行测试，并生成包含评估结果、发现问题和整改建议的测试报告；
e) 输入输出：测试阶段的输入通常包括产品需求文档、设计文档、PIA 报告等；输出包括测试用例、测试报告、缺陷报告和最终的合规性验证报告。

5.2.5 产品封装阶段

产品封装阶段需确保在将数据、模型、报告等内容封装成可交付产品状态的过程中持续合规。此阶段需开展如下合规性工作：

a) 数据脱敏与加密：对封装的数据产品进行必要的脱敏处理，并对敏感数据采用加密存储；
b) 数据来源与内容二次复核：在产品封装前再次核验原始数据取得方式以及是否包含禁止交易的数据；
c) 日志与审计追踪：对封装操作全过程进行日志记录与留存，确保可追溯；
d) 数据产品信息告知：在封装包内放置数据产品信息清单，告知数据来源、数据权属、授权信息、数据类别等信息；
e) 权限控制：封装后的数据产品应设置严格的访问权限，确保只有授权用户可使用。

5.2.6 发布与部署阶段

发布与部署阶段需确保产品在上线过程中及生产环境中持续合规。此阶段需开展如下合规性工作：

a) 最终合规审查：产品上线前，应由法务、合规或数据保护官进行最终的合规审查，确认所有已知合规风险已得到有效控制；
b) 安全配置：确保服务器、数据库、网络设备等基础设施进行了安全配置，关闭不必要的端口和服务，使用强密码策略；
c) 安全部署：确保数据在传输和存储过程中的安全，例如，所有外部数据传输必须使用加密信道，如 TLS 1.2 及以上版本；
d) 上线后监控：部署完成后，立即启动安全监控机制，监测异常访问和潜在的安全威胁。

5.2.7 流通交易阶段

流通交易阶段需确保产品在进入市场进行定价、交易、权属转移的过程中合法合规。此阶段需开展如下合规性工作：

a) 权属确认：明确数据产品的所有权、使用权和收益权，避免权属纠纷。数据提供者对其合法处理数据形成的数据产品可以依法使用、取得收益和处分；
b) 数据产品定价：数据产品提供者可以依法自主定价，但不得排除、限制竞争；
c) 数据产品交易限制审查：交易前应对数据产品提供方对外提供数据是否需取得资质或许可进行审查；
d) 数据产品交易协议签署：协议一般应约定数据产品的内容、用途、交付质量、交易价格、交付方式、使用期限以及数据安全责任、承诺与保证、保密约定、违约责任、争议解决等条款；
e) 重要数据交易合规：对涉及重要数据的产品进行交易，应当事前开展数据安全风险评估；
f) 交易审计：建立交易审计机制，记录交易过程，确保可追溯、可审计。

5.2.8 运营与维护阶段

运营与维护阶段是保障数据产品长期合规运营的关键阶段。此阶段需开展如下合规性工作：

a) 持续监控与审计：定期对操作日志进行审计，监控数据访问和使用行为，发现违规操作或安全事件；
b) 风险评估与漏洞管理：定期进行安全风险评估，并建立漏洞管理流程，及时响应和修复新发现的安全漏洞；
c) 用户请求响应：建立并运行流畅的流程，以响应用户的权利请求，如查询、更正、删除等；
d) 隐私政策更新：当产品功能、数据处理目的或方式发生变更时，必须及时更新隐私政策，并通过显著方式通知用户，必要时重新获取同意；
e) 供应链安全管理：若数据产品依赖云服务、第三方 SDK 等第三方服务，需定期评估供应商的合规与安全状况。

5.2.9 退出与处置阶段

退出与处置阶段是在数据产品停止服务或下线时，需进行的安全处置措施。此阶段需开展如下合规性工作：

a) 用户告知：应提前向用户发布停止服务的通知；
b) 数据删除或匿名化：在服务终止后，应按照法律法规规定和与用户的约定，及时删除或匿名化处理所持有的个人信息；
c) 日志归档：根据法律法规要求，对相关日志进行归档；
d) 资产处置：对承载数据的物理介质进行销毁或安全擦除，确保数据无法被恢复。

6 重点行业数据合规特殊要求

6.1 重点行业分类

数据产品除应符合通用合规要求外，本文件根据金融、医疗健康、电子商务与零售、汽车、工业与电信、人工智能等特定行业对其业务特性和监管要求，提出了更为严格和具体的合规规范。

6.2 数据合规特殊要求

6.2.1 金融行业

金融行业数据合规特殊要求如下：

a) 数据分类分级：应严格遵循中国人民银行发布的 JR/T 0197-2020 金融数据安全 数据安全分级指南相关要求，对客户财务信息、交易记录等实施高级别保护；
b) 个人金融信息保护：应严格遵守 JR/T 0171-2020 个人金融信息保护技术规范、JR/T 0223-2021 金融数据安全 数据生命周期安全规范的相关要求，对个人金融信息的收集、处理、传输、存储等环节实施全方位技术保护；
c) 支付卡数据安全：若涉及处理银行卡信息，必须遵守支付卡行业数据安全标准（PCI DSS）的要求；
d) 加密要求：在数据传输中，强制使用高强度加密协议，如 TLS 1.2 或更高版本；在数据存储中，对敏感金融数据进行加密保护。推荐使用国密算法（如 SM 系列）与国际主流算法（如 AES）相结合的方案；
e) 审计与日志：操作日志，特别是涉及核心数据和跨境传输的日志，应至少保存六个月，部分核心业务日志可能要求保存更长时间，如 3 年。

6.2.2 医疗健康行业

医疗健康行业数据合规特殊要求如下：

a) 数据类型与敏感性：电子病历、基因信息、诊疗记录等健康医疗数据，通常应被归类为敏感个人信息或重要数据，需采取最高级别的安全保护；
b) 去标识化与匿名化：在数据用于研究、分析等二次利用场景时，必须采取严格的去标识化或匿名化技术措施。应评估并采用如 k－匿名、l－多样性、t－接近性等技术，以防范数据重标识风险；
c) 合规依据：除国家法律外，还需参考 GB/T 39725-2020 信息安全技术 健康医疗数据安全指南规定的相关要求。若业务涉及国际合作，还需关注美国《健康保险流通与责任法案》、欧盟《欧洲健康数据空间条例》等域外法规的要求；
d) 数据存储与访问：医疗健康数据原则上应在境内存储。对数据的访问应有严格的权限控制和审计记录，确保仅授权的医护人员或研究人员可以访问。

6.2.3 电子商务与零售行业

电子商务与零售行业数据合规特殊要求如下：

a) 用户画像与自动化决策：利用用户消费行为数据进行用户画像和个性化决策时，应向用户明确告知，提供不针对个人特征的选项或提供关闭或退出个性化决策的选项，不得对交易相对人实行不合理的差别待遇；
b) 大规模个人信息处理：电商平台通常处理海量用户个人信息，存在数据泄露的高风险，应作为重点关注对象，必须建立完整的数据安全防护体系和应急响应机制；
c) 用户权利保障：应提供便捷的“一站式”个人信息管理中心，方便用户查询、管理其账户信息、交易记录、地址信息等，并顺利行使各项权利；
d) 跨境电商：若涉及跨境交易，需同时遵守中国以及境外（如分支机构所在地/商品或服务提供地/消费者所在地）的个人信息保护法规。

6.2.4 汽车行业

汽车行业数据合规特殊要求如下：

a) 数据分类：需遵守《汽车数据安全管理若干规定（试行）》，将汽车数据分为重要数据和个人信息数据（包括敏感个人信息），并实施分类分级管理；
b) 处理原则：处理汽车数据应遵循“车内处理”“默认不收集”“精度范围适用”“脱敏处理”等原则；
c) 出境要求：军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等重要数据，出境前必须通过国家网信部门会同国务院有关部门组织的安全评估；
d) 年度汽车数据安全报送要求：开展重要数据处理活动，应当向网信部门报送年度汽车数据安全管理情况；
e) 智能网联汽车数据处理：数据采集方面，车辆数据采集需遵循“默认不收集”原则，确需收集的应取得用户明确同意。数据处理方面，倡导车内处理原则，除非确有必要不向车外提供。处理如行人、其他车辆信息等车外数据时需，注意第三方权益保护。

6.2.5 工业与电信行业

工业与电信行业数据合规特殊要求如下：

a) 关键信息基础设施：若数据处理者被认定为关键信息基础设施运营者，其数据处理活动需遵守更为严格的法律要求，采购的网络产品和服务可能需要通过国家安全审查；
b) 工业数据安全：需遵守《工业和信息化领域数据安全管理办法（试行）》，关注工业领域数据安全的特定标准和要求，保护工业控制系统数据、生产运营数据等的安全；
c) 电信数据：用户通信内容、定位信息等属于高度敏感数据，需在符合《电信和互联网用户个人信息保护规定》等行业法规的前提下进行处理。

6.2.6 人工智能行业

人工智能行业数据合规特殊要求如下：

a) 算法合规性：人工智能数据产品需确保算法模型的公平性、透明性和可解释性，避免算法歧视；
b) 训练数据合规：机器学习、深度学习等模型的训练数据需确保来源合法，并经过适当的脱敏处理；
c) 内容生成合规：对于生成式人工智能产品，需建立内容安全审核机制，防止生成违法和不良信息。

7 数据跨境传输合规要求

7.1 数据出境路径选择

根据《中华人民共和国个人信息保护法》及《网络数据安全管理条例》等规定，数据处理者向境外提供数据，应根据情况选择以下合规路径之一：

a) 通过国家网信部门组织的安全评估：重要数据出境，或关键信息基础设施及处理达到规定数量个人信息的数据处理者向境外提供个人信息时，必须采用此路径；
b) 进行个人信息保护认证：经专业的认证机构进行认证；
c) 与境外接收方订立标准合同：按照国家网信部门制定的标准合同范本（如《个人信息出境标准合同办法》所附标准合同范本）与境外接收方订立合同。

7.2 安全技术措施

安全技术措施要求如下：

a) 传输加密：跨境数据传输的全过程必须采用加密措施。应强制使用 TLS 1.2 及以上版本的安全传输协议，并采用高强度的加密套件；

b) 内容加密：对传输内容中的敏感数据，应在传输前进行应用层加密，确保即使传输信道被攻破，数据内容本身仍是安全的；
c) 数据脱敏：对于非必要传输原始个人信息的场景，应优先在境内完成去标识化或匿名化处理后再进行传输，可用于重标识的个人信息应存储在境内。

7.3 接收方义务与监督

对接收方的义务要求和监督要求如下：
a) 接收方评估：在传输前，应对境外接收方的数据安全保护能力进行评估，确保其能达到与中国法律法规、强制性国家标准要求相当的保护水平；
b) 日志记录与审计：必须对数据跨境传输活动进行详细的日志记录，内容包括传输时间、接收方、数据类型、数据量、是否加密等。日志应完整保存至少六个月并定期进行审计。

8 合规管理与组织保障

8.1 组织架构与职责划分

数据产品提供者宜建立适应的组织架构并明确职责权限，保障合规管理工作有章可依：
a) 设立专门岗位/部门：建议有条件的企业设立数据保护官或专门的数据合规团队，负责统筹数据产品的合规工作；
b) 明确职责：应在组织内部明确产品、研发、测试、运维、法务、审计等不同部门和岗位在数据合规方面的具体职责。

8.2 制度建设与人员培训

数据产品提供者宜建立适应的内部制度并针对重点人员开展培训，确保合规工作有效实施：
a) 建立内部合规制度：制定并发布覆盖数据产品全生命周期的数据安全与个人信息保护管理制度、操作规程和应急预案。
b) 定期培训与考核：定期对全体员工，特别是接触核心数据和个人信息的员工，进行数据合规意识和技能的培训与考核。

8.3 合规审计与持续改进

数据产品提供者宜定期开展合规审计或参与获得合规认证，持续推进管理措施优化：
a) 定期内部审计：对数据处理全流程进行记录，每年至少进行一次全面的数据合规内部审计，检查数据产品开发与运营活动是否符合内外部合规要求；
b) 外部合规认证：鼓励企业寻求第三方机构的合规审计或认证，如 ISO/IEC 27701 隐私信息管理体系认证，以自证合规能力；
c) 持续改进：基于审计结果、风险评估和法律法规的变化，持续优化合规策略和技术措施。

8.4 数据安全事件应急响应

数据产品提供者宜针对数据安全风险建立预判和处置措施，确保能够有效应对突发事件：
a) 制定应急预案：制定详细的数据安全事件应急预案，明确事件的响应级别、上报流程、处置措施、人员职责和内外部沟通机制；
b) 定期演练：定期组织应急响应演练并记录演练情况，确保在真实事件发生时，团队能够迅速、有效地进行响应，减少损失和影响；
c) 履行报告义务：一旦发生数据泄露、篡改、丢失事件，应立即启动应急预案，并按照法律规定向有关监管部门报告，并通知受影响的个人。

参 考 文 献

[1] GB/T 29490-2023 企业知识产权合规管理体系 要求
[2] GB/T 35273-2020 信息安全技术 个人信息安全规范
[3] GB/T 35770-2022 合规管理体系 要求及使用指南
[4] GB/T 39725-2020 信息安全技术 健康医疗数据安全指南
[5] GB/T 41867-2022 信息技术 人工智能 术语
[6] GB/T 41871-2022 信息安全技术 汽车数据处理安全要求
[7] GB/T 42574-2023 信息安全技术 个人信息处理中告知和同意的实施指南
[8] JR/T 0171-2020 个人金融信息保护技术规范
[9] JR/T 0197-2020 金融数据安全 数据安全分级指南
[10] JR/T 0223-2021 金融数据安全 数据生命周期安全规范
[11] ISO/IEC 27701 隐私信息管理体系认证
[12] 信息安全技术 数据交易服务安全要求（征求意见稿）
[13] 《中华人民共和国网络安全法》（中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于2016年11月7日通过，自2017年6月1日起施行）
[14] 《中华人民共和国数据安全法》（中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议于2021年6月10日通过，自2021年9月1日起施行）
[15] 《中华人民共和国个人信息保护法》（中华人民共和国第十三届全国人民代表大会常务委员会第三十次会议于2021年8月20日通过，自2021年11月1日起施行）
[16] 《网络数据安全管理条例》（2025年1月1日中华人民共和国国务院公布）
[17] 《汽车数据安全管理若干规定（试行）》（2021年10月1日国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、交通运输部公布）
[18] 《电信和互联网用户个人信息保护规定》（工业和信息化部2013年9月1日发布）
[19] 《工业和信息化领域数据安全管理办法（试行）》（工业和信息化部2022年12月8日发布）
[20] 《数据领域常用名词解释（第一批）》（国家数据局2024年12月发布）
[21] 《人类遗传资源管理条例实施细则》（2023年5月11日中华人民共和国科学技术部第3次部务会审议通过）
[22] 《征信业务管理办法》（2021年9月17日中国人民银行2021年第9次行务会议审议通过）
[23] 《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》（2022年6月22日中央全面深化改革委员会第二十六次会议审议通过）