T/JNBDA

济 南 市 大 数 据 协 会 团 体 标 准

T/JNBDA 0004-2025

数据合规工作指南

Data Compliance Guidelines

2025 - 11- 13 发布　　2025 - 11 - 13 实施

济南市大数据协会发布

目 录

前言 I
1.范围 1
2.规范性引用文件 1
3.术语和定义 1
3.1 数据生存周期 data lifecycle 1
3.2 数据提供者 data provider 1
3.3 数据治理 data governance 1
3.4 个人信息（Personal Information） 1
3.5 敏感个人信息（Sensitive Personal Information） 2
3.6数据合规风险评估（Data Compliance Risk Assessment） 2
4.数据合规管理框架 2
4.1 组织架构 2
4.2 制度体系 2
5.数据生命周期合规要求 3
5.1 数据收集和使用 3
5.2 数据存储 3
5.3 数据共享与转让 4
5.4 数据传输 4
5.5 数据销毁 4
6.数据交易合规 5
6.1 数据提供方责任 5
6.2 数据购买方责任 5
7.数据出境合规 5
7.1 数据出境风险自评估 5
7.2 数据出境安全保护责任 5
7.3 个人信息出境合规 5
8.合规评估与审计 6
8.1 内部评估 6
8.2 第三方审计 6
9.附则 6
参考文献 7

前　言

本文件按照GB/T1.1-2020《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。

本文件由济南大数据协会提出并归口。

本文件起草单位：泰和泰律师事务所。

本文件主要参与单位：山东长纳数字科技有限公司、北京市盈科（济南）律师事务所、济南公共交通集团有限公司、山东利诚大数据有限公司、山东土地数字科技集团有限公司、山东众成清泰（济南）律师事务所、国家石油天然气管网集团有限公司山东分公司、华唐能源科技（山东）有限公司、济南建工集团有限公司、济南农村商业银行股份有限公司、济南先行数字城市科技有限公司、济南章丘国开大数据集团有限公司、金现代信息产业股份有限公司、明曦金道（山东）数据科技有限公司、普联软件股份有限公司、日照中医医院、山东邦维信息科技有限公司、山东丞华企业投资控股有限公司、山东轨道交通信息有限公司、山东和同信息科技股份有限公司、山东领潮软件科技有限公司、山东鲁商科技集团有限公司、山东旗帜信息有限公司、山东数字文化集团有限公司、山东双泽信息技术有限公司、山东微笑数据科技有限公司、山东鹰格信息工程有限公司、泰山财产保险股份有限公司、同圆设计集团股份有限公司。

本文件主要起草人：尹晓东、郑娟、黄怡敏、刘大亮、付增洋、王文娟、张华勇、刘国泰。

数据合规工作指南

1.范围

本指南规定了数据全生命周期管理的合规要求、操作规范及评估方法，适用于数据处理活动，以及通过数据交易平台进行数据交易的企业、机构及第三方服务提供者。旨在为各类组织提供数据合规工作的通用指引，帮助其建立、实施、维护和持续改进数据合规管理体系，防范数据合规风险。

适用场景：

数据采集、存储、使用、共享、传输、删除、销毁全流程

数据交易平台运营及参与方

跨境数据流通

数据资产入表与价值化实现

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 38667-2020 信息技术 大数据数据分类指南

GB/T 35770-2017 合规管理体系指南

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 41479 信息安全技术 网络数据处理安全要求

T/CFE II 0003-2022 数据合规管理体系要求

3.术语和定义

下列术语和定义适用于本文件：

3.1 数据生存周期 data lifecycle

将原始数据转化为可用于行动的知识的一组过程。

3.2 数据提供者 data provider

大数据参考体系结构中的一种逻辑功能构件,它将新的数据或信息引人大数据系统注:数据提供者一般包括:企业、公共机构、科学家、调研人员、从事数据搜索的工程师、网络应用软件、网络运营商和末端用户。

3.3 数据治理 data governance

对数据进行处置、格式化和规范化的过程。

注 1:数据治理是数据和数据系统管理的基本要素

注 2:数据治理涉及数据全生存周期管理,无论数据是处于静态、动态、未完成状态还是交易状态。

3.4 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。例如，自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

3.5 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，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，以及不满十四周岁未成年人的个人信息。

3.6 数据合规风险评估（Data Compliance Risk Assessment）

对组织在数据处理活动中可能面临的合规风险进行识别、分析、评价，并制定应对措施的过程。

4.数据合规管理框架

4.1 组织架构

4.1.1 数据合规第一责任人

应当由数据持有人法定代表人或主要负责人担任，履行以下职责：审批年度合规计划及重大合规事项（如数据跨境传输、重要数据共享），确保合规资源投 入（人力、技术、资金），每季度听取合规汇报，对数据安全事件负领导责任，72 小时内启动应急预案。

4.1.2 数据合规管理专职部门

要求人员配置不少于3人（年处理数据量超100万条的企业需配置5人以上）。 职责包括：制定合规制度、流程及应急预案（每半年更新一次），组织全员合规培训（新员工入职 30 日内完成基础培训，每年至少2 次进阶培训），处理合规举报（响应时限≤5 个工作 日，复杂案件≤15 个工作 日）。

4.1.3 个人信息保护负责人

处理超过 100 万用户个人信息的企业需指定专人，需具备法律或信息安全专业背景，负责统筹个人信息合规，每季度向监管部门提交合规报告，监督第三方合作方合规性，定期审计数据处理活动，公开联系方式，接受用户咨询与投诉。

4.2 制度体系

4.2.1 合规风险评估机制

每年 12 月前完成全流程自评估，覆盖以下维度：技术措施有效性、监管动态响应能力、历史违规事件整改率；完成评估后需要出具报告，评估报告需包含：风险点清单（含整改措施及责任人）、合规投入产出分析、下一年度合规优化计划。

4.2.2 数据分类分级与安全管理机制

根据数据的敏感程度和重要性，进行差异化管控以降低风险。

数据分类分级标准：按“敏感程度”：如个人信息分为“一般个人信息”如姓名、电话和“敏感个人信息”如生物识别、医疗记录、金融账户等，后者需更严格保护如单独同意、加密存储。

按“业务重要性”：如商业秘密或核心技术数据、普通经营数据，明确不同级别数据的访问权限、传输限制。

安全技术措施：规定数据安全防护手段，如加密、脱敏、防火墙、入侵检测，敏感数据需强制加密。

安全管理措施：包括机房/系统的物理安全，如门禁、监控；账号管理如密码复杂度、定期更换；安全日志审计（留存至少6个月）。

4.2.3 合规审查与风险管控机制

合规审计制度：定期（如每季度/每年）由法务部或第三方机构对数据处理活动进行审计，检查是否符合制度及法规，形成审计报告并整改问题。

风险评估机制：针对高风险场景（如数据跨境、大规模个人信息共享），提前开展合规风险评估（如识别“未获同意收集”“泄露风险”等），制定应对措施。

第三方合作合规管理：对数据处理外包商（如云服务商、数据标注公司）进行准入审查（资质、安全能力），签订合规协议（明确数据安全责任、违约赔偿等），定期核查其合规性。

5.数据生命周期合规要求

5.1 数据收集和使用

5.1.1 以爬虫手段收集到数据

采取爬虫手段收集到的数据，需要遵循以下要求：

a)禁止突破网站反爬机制

b)禁止抓取非公开数据

c)禁止干扰网站正常运营

d)向目标网站备案爬虫用途，设置爬虫访问频率限制，标注爬取数据来源及时间戳

5.1.2 以购买、交换等手段收集数据

通过向第三方购买、交换、共享等方式收集数据的，应当符合法律、法规要求，对第三方的资质以及获取和持有数据的合规性进行必要审查，要求其作出数据来源合法性承诺并提供必要证明。对从第三方获取的数据，数据获得人应当承担与直接收集的数据同等的安全保护责任与合规义务。

5.1.3 在提供产品、服务过程中收集数据

在提供产品、服务过程中收集个人信息，应当符合最小必要原则，仅收集与实现产品或服务的业务功能直接相关的个人信息。不得因个人不同意提供非必要个人信息，而拒绝向其提供基本功能或服务。

基于开发新型业务功能、提升服务体验等目的，超出必要范围收集用户个人信息的，应当征得个人同意。如需使用在提供产品、服务过程中收集到的数据，应当事先获得相关数据主体的授权同意。

5.1.4 数据分类管理

应当建立个人信息分类管理制度，结合个人信息的主体属性、具体种类、敏感程度、处理方式、应用场景、对个人权益的影响、可能存在的安全风险等因素明确个人信息分类标准，并分别确定针对不同类型个人信息的处理规则、合规义务和保护标准。敏感个人信息及未成年人个人信息处理规则应当遵循法律、法规的相关规定。

应当持续检验、监控个人信息处理活动的合法合规程度、对个人合法权益造成损害的各种风险以及相关保护措施的有效性，形成和保存个人信息保护影响评估报告和处理情况记录，并采取相应改进措施。

5.2 数据存储

5.2.1 分级分域管理

根据分类分级等内部规范对不同类型、风险等级和重要、敏感程度的数据进行分级分域管理，对不同数据进行物理隔离或强逻辑隔离，并采取相适应的安全保护措施和访问控制机制，维护数据的完整性、保密性、可用性。

可以通过加密存储、访问控制、校验技术等措施强化对重要数据和敏感个人信息的保护。

5.2.2 数据存储介质管理

根据数据类型、风险等级和重要、敏感程度等因素选择安全性能、防护级别与安全等级相适应的存储设备和介质，制定数据存储设备和介质清单，建立数据存储设备和介质管理制度，规范存储设备和介质的使用、操作、维修和故障处理， 并对传递、使用数据存储设备和介质的行为建立审批和日志记录等管控机制，强化存储设备和介质的物理安全和加密管理。

5.2.3 云平台存储

使用第三方云平台进行数据存储的，需要求云服务提供商定期报告云平台运行状态、安全状况等信息，并定期对第三方云平台的稳定性和采取的安全保护措施等进行审计，确保其具备充分的数据安全保护能力。

终止使用云平台存储服务的，有权取回数据、文档等资料并对其完整性、有效性进行验证。云服务提供商应当按照约定方式删除、销毁云平台存储的数据及副本。

5.2.4 数据备份及恢复

需要建立重要数据和个人信息的备份与恢复机制，确定数据备份的范围、频率、方法和流程，并定期对备份数据进行恢复测试和完整性校验，防范数据意外 损毁、丢失等风险。

5.3 数据共享与转让

5.3.1数据主体的明确同意

数据共享与转让前，必须获得数据主体的明确同意（法律、行政法规另有规定的除外，如为了公共卫生安全需要共享疫情相关数据）。在获得同意时，需向数据主体告知共享或转让的对象、数据种类、使用目的等信息。

5.3.2 数据接收方的安全能力评估

对数据接收方进行严格的安全能力评估，评估内容包括接收方的数据安全管理制度、技术防护措施、人员安全管理等，确保接收方具备保障数据安全的能力。

5.3.3 安全措施

数据共享与转让过程中，需采取加密传输等安全措施，防止数据在传输过程中被泄露；对于共享或转让的敏感个人信息，还可采取去标识化处理，降低数据泄露风险。

5.4 数据传输

5.4.1 数据传输的合规要求

应当采取加密等安全保护措施确保数据传输介质和环境安全，保障重要数据和敏感个人信息传输过程的安全性，防范未经授权访问和数据泄露。

5.4.2 向第三方提供数据的合规要求

因业务需要等正当理由向第三方提供或共享、委托处理数据的，应当对数据接收方进行事前资格审查并评估其数据安全保护能力。涉及提供重要数据、敏感数据的，应当留存相应的日志记录。

应当通过合同等形式与数据接收方约定处理数据的目的、范围、方式、限制与应采取的安全保护措施等事项，明确双方权利和义务，并对数据接收方的处理活动进行必要监督。发现数据接收方违反法律、法规规定或双方约定处理数据的，应当立即要求其停止相关行为并采取必要的补救措施；必要时应当暂停或终 止向其提供数据，并监督数据接收方及时返还、删除、销毁已获得的数据。

5.4.3 第三方接入场景的合规义务

产品或服务接入由第三方提供的软件开发工具包的，应当事前对接入第三方进行安全检测，评估是否存在已知的安全漏洞以及可能引起数据泄露等安全事件的行为，并建立相应的接入第三方合规管理机制，通过签署开发者服务协议等形式明确双方的权利和义务、应采取的安全保护措施、发生数据安全事件时的补救与应急处置措施以及责任承担等事项，并留存第三方接入日志记录。

第三方软件开发工具包具备收集、处理个人信息功能的，应当要求该第三方如实、完整披露收集、处理个人信息的具体情况，并应将相关情况及时、准确告知所涉个人，并按照法律规定征得个人同意。

5.5 数据销毁

5.5.1 数据删除与销毁的合规要求

应当建立数据删除和销毁的操作规程和管理制度，明确删除和销毁的对象、权限、流程和技术等要求，确保被销毁数据不可恢复，并对相关活动进行记录和留存。

对数据存储设备和介质进行报废处理的，应当事先采取格式化、重复删除、介质消磁等方式删除其中存储的数据，并采取物理损毁等方式对介质进行彻底销毁。

6.数据交易合规

6.1 数据提供方责任

6.1.1 数据来源合规

数据提供方应当建立针对数据来源的合规审查机制，确保数据获取手段合法合规、数据来源链路清晰，并经过所涉主体明确授权同意，不存在侵犯国家、公共利益或其他组织、个人合法权益的情况。

6.1.2 数据内容合规

数据提供方应当建立针对数据内容的合规审查机制，不得交易含有以下内容的数据产品或服务：含有未经授权的个人信息的；含有侵犯他人知识产权或商业秘密的内容的；含有未经依法开放的公共数据的；含有国家核心数据或国家秘密的；含有法律、法规规定禁止交易的其他数据的。

6.1.3 数据质量合规

数据提供方应当建立必要的数据质量校验机制，提升交易数据的准确性、完整性和及时性，并通过数据复核、交叉验证等方式强化重要数据、敏感数据的质量审查。

6.2 数据购买方责任

数据购买方应当按照约定的目的、场景和方式合规使用数据，不得将通过交易获取的数据用于违反法律法规或双方约定的其他用途。

7.数据出境合规

7.1 数据出境风险自评估

数据提供方在申报数据出境安全评估前，应当开展数据出境风险自评估，重点评估以下事项：

a)数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；

b)出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；

c)境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；

d)数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

e)与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等是否充分约定了数据安全保护责任义务；

f)其他可能影响数据出境安全的事项。

7.2 数据出境安全保护责任

a)数据提供方应当在与境外接收方订立的法律文件中明确约定数据安全保护责任义务，至少包括以下内容：

b)数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等；

c)数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施；

d)对于境外接收方将出境数据再转移给其他组织、个人的约束性要求；

e)境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施；

f)违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式；

g)出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

7.3 个人信息出境合规

数据提供方通过经专业机构进行个人信息保护认证的方式向境外提供个人信息的，应当符合 GB/T 35273《信息安全技术个人信息安全规范》以及相关法律法规的要求。

8. 合规评估与审计

8.1 内部评估

应当定期开展数据合规审计，或委托具有相关资质的外部机构进行，并形成、保存相应的数据合规审计报告。对于审计过程中发现的合规问题与安全隐患应及时采取整改措施。

可以针对风险较高的数据处理行为进行不定期审计，确保及时发现问题隐患并予以改正。

8.2 第三方审计

8.2.1 审计周期：

对于重要数据处理者做到每年 1 次。

对于普通数据处理者做到每 2 年 1 次。

对于数据交易平做到每半年 1 次。

8.2.2 审计内容

制度合规性、技术措施有效性、操作记录完整性。

9. 附则

9.1 标准修订

本标准由济南大数据局负责解释与修订，每两年评估一次。

9.2 实施日期

自发布之日起生效，过渡期内原有协议可继续执行。

参考文献

[1]《中华人民共和国数据安全法》

[2]《中华人民共和国个人信息保护法》

[3]《中华人民共和国网络安全法》

[4]《关键信息基础设施安全保护条例》

[5]《网络数据安全管理条例》

[6]《云计算服务安全评估办法》

[7] GB/T 25069-2022 信息安全技术 术语

[8] GB/T 38667-2020 信息技术 大数据 数据分类指南

[9] GB/T 43697-2024 数据安全技术 数据分类分级规则

[10] T/CFEII 0003-2022 数据合规管理体系 要求

[11] GB/T 42450-2023 信息技术 大数据 数据资源规划