ICS 35.240
CCS L 67

团　　体　　标　　准

T/CERS XXXX-YYYY

能源大数据 数据合规管理要求

Energy big data—Requirements for the data compliance management

（征求意见稿）

20××－××－××发布　　20××－××－××实施

中国能源研究会　发布

目　　次

前　言

本文件按照《中国能源研究会标准管理办法（修订稿）》的要求，依据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专利的责任。

本文件由中国能源研究会提出。

本文件由中国能源研究会信息通信专委会技术归口和解释。

本文件起草单位：

本文件主要起草人：

本文件首次发布。

能源大数据 数据合规管理要求

1 范围

本文件规定了能源大数据中心数据识别、数据获取、数据传输、数据存储、数据应用、数据对外开放、数据退役等数据合规重点环节的管理要求等。

本文件适用于能源大数据能源数据中心建设运营过程中数据合规管理。

2 规范性引用文件

下列文件对本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 36073—2018 数据管理能力成熟度评估模型

GB/T 43697—2024 数据安全技术 数据分类分级规则

T/CSEE 0309.3—2022 能源大数据 第3部分：分级分类

T/CERS 0006—2023 能源企业数字化转型能力评价导则

3 术语和定义

下列术语和定义适用于本文件。

3.1

能源企业 energy enterprises

从事电力、石油石化、煤炭、燃气、新能源、核能等主营业务的企业，或支撑以上主营业务开展的咨询、相关设备制造等服务的企业。

[来源：T/CERS 0006—2023，3.1]

3.2

能源大数据合规 energy big data compliance

企业及其员工在收集、存储、使用、处理、共享、转让、跨境或非跨境传输、流动、保护能源大数据的行为需符合国际条约、国内法律法规规章、其他规范性文件、行业准则、商业惯例、社会道德以及企业章程、规章制度的要求。

3.3

能源大数据分级 energy big data classification

根据能源大数据在遭到篡改、破坏、泄露或者非法获取、非法利用后的影响程度，按照一定的原则和方法进行分级的过程。

[来源：T/CSEE 0309.3—2022，3.2]

3.4

国家安全 national security

国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。

3.5

公共利益 public interest

能够满足一定范围内所有人生存、享受和发展的、具有公共效用的资源和条件。

3.6

核心数据 core data

对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的,一旦被非法使用或共享,可能直接影响国家安全、国民经济命脉、重要民生和重大公共利益等的能源领域数据。

3.7

重要数据 important data

一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的能源领域数据。

注：重要数据如安全生产、运行的数据，关键系统组件、设备供应链等数据。

3.8

一般数据 general data

能源企业及能源大数据中心在经营管理过程中产生的，除核心数据和重要数据以外的非敏感类数据。

3.9

公开数据 public data

能源企业在提供公共服务过程中收集、产生的数据。

3.10

数据退役 data exit operations

对历史数据的管理,根据法律法规、业务、技术等方面需求对历史数据的保留和销毁,执行历史数据的归档、迁移和销毁工作,确保组织对历史数据的管理符合外部监管机构和内部业务用户的需求,而非仅满足信息技术需求。

3.11

数据归档 data archiving

将不再经常使用的数据迁移到一个单独的存储设备来进行长期保存的过程。

注：数据归档是数据退役阶段的一个环节，迁移后的数据仍然支持历史查询操作。

3.12

数据沉寂 data silence

数据经过数据归档后，达到一定的期限不再被使用，仅保留日后查询而采取的操作。

注：数据沉寂是数据退役阶段的一个环节。

3.13

数据销毁 data destruction

数据经过归档环节达到一定的期限确定不再被使用，按照规则执行的销毁、擦除操作。

注：数据销毁是数据退役阶段的一个环节，包括离开使用环境的数据介质上的数据擦除。

4 能源大数据合规管理概述

数据合规管理贯穿整个能源大数据生存周期，数据合规管理涉及数据识别、数据获取、数据传输、数据存储、数据应用、数据对外开放、数据退役等多个环节，对这些重要环节均需提出合规管理要求。

5 能源大数据识别管理要求

5.1 能源大数据分级

具体要求如下：

a）能源大数据分级。能源大数据分级在遵照 GB/T 43697—2024 中6.1的要求上，根据影响对象、影响程度两个要素，将数据从高到低分为核心数据、重要数据、一般数据-2、一般数据-1四个级别，见表1。

b）能源大数据相关方。宜划分为能源数据生产者、能源数据汇集者（能源大数据中心）、能源数据使用者。明确能源大数据相关方的定义和在数据合规管理体系中的职责定位。

表 1 能源大数据分级识别判断规则

影响对象	影响程度			
	特别严重危害	严重危害	一般危害	无危害
国家安全	核心数据	核心数据	重要数据	一般数据-1
经济运行	核心数据	重要数据	一般数据-2	一般数据-1
社会秩序	核心数据	重要数据	一般数据-2	一般数据-1
公共利益	核心数据	重要数据	一般数据-2	一般数据-1
组织权益、个人利益	一般数据-2	一般数据-2	一般数据-2	一般数据-1

5.2 能源大数据业务识别

具体要求如下：

a）业务分类。按照服务对象、服务形式、服务类型对能源大数据中心的业务进行梳理，完成能源大数据业务视图盘点，为差异化合规管理策略的制定奠定基础。

b）关键业务识别。结合能源大数据中心建设运营实际梳理关键业务，参照能源大数据分级相关要求，结合能源数据种类、服务用户数量、社会影响范围等因素，对关键业务实施重点合规性管理。例如：煤炭领域的煤炭开采、煤化工，石油领域的油气开采、油气储存，电力领域的电力生产等。

6 能源大数据获取合规管理要求

能源数据汇集者（能源大数据中心）、能源数据使用者应根据数据获取范围、内容、渠道，制定有效的数据合规管理策略，规范数据获取行为，在收集数据时应遵守以下要求：

a）法律法规及组织数据管理制度对数据收集的目的、范围有规定的，应当在规定的目的和范围内收集数据；

b）对采集数据应进行有效性、合理性校验，支持数据一次采集、多处使用。

c）遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式收集包括个人信息在内的数据；

d）数据收集应当具有明确、合理的目的，并应与收集目的直接相关，采取对被收集方权益影响最小的方式，并提前取得被收集方授权同意；数据收集涉及个人信息时，应当限于实现处理目的的最小范围，不得过度收集个人信息；严格控制收集信息的数量和频率；

e）个人信息采集前应明示采集和使用规则、目的、方式和范围等，并取得客户信息主体授权同意，或者符合法律法规规定的其他情形，方可具体实施采集，同时需尊重和保障客户信息主体的隐私权利，不得隐瞒产品或服务所收集客户信息的用途；获取公共重要数据和外部企业一般数据，应在保障数据来源合法的前提下，取得数据主体同意后，方可具体实施采集；

f）以数据交换方式获取数据，应严格审查数据来源，按照相关要求签订合同、协议，明确数据用途和双方权益条款，落实数据安全合规义务和责任。

g）面向第三方收集数据的场景中，应确保数据授权等机制的延伸控制；

h）面向第三方采购数据时，应建立数据供应链合规管理制度，对数据提供方进行合规审查，确保所获得数据合规。

7 能源大数据传输合规管理要求

能源数据汇集者(能源大数据中心)应根据能源数据分类分级和传输渠道实施相应的合规管控策略，防范数据泄露、篡改、损毁、丢失风险，对能源数据传输的合规性负责。应采取以下措施：

a）加强数据处理系统、数据传输网络等安全防护；

b）积极应对数据传输方面数据安全事件，防范针对和利用数据传输的违法犯罪活动；

c）传输数据的系统原则上应当满足三级以上网络安全等级保护和关键信息基础设施安全保护要求，传输核心数据的系统依照有关规定从严保护；

d）传输核心数据、重要数据等敏感数据时，应采用加密、访问控制、安全审计等安全措施；

e）数据传输过程应避免手工和离线操作，做好工作记录和传输日志归档，确保重要数据可溯源、可追踪、可审计；

f）传输一般数据、核心数据、重要数据时，应符合安全防护方案要求，按规定开展网络安全等级保护测评，采取加密、安全通道等技术手段和其他必要措施，确保数据传输安全；

g）核心数据、重要数据禁止在云平台传输，在云平台传输重要数据时应加密保护。相关数据的访问和交互应加强访问控制；

h）面向第三方传输数据时，应按照要求采取安全措施并以合同形式约定。

8 能源大数据存储合规管理要求

能源数据汇集者（能源大数据中心）应根据数据分类分级、存储位置实施相应的数据存储策略，落实隔离、加密、脱敏、备份等数据存储保护技术措施，对数据存储的合规性负责。应采取以下措施：

a）对核心数据、重要数据、一般数据、公开数据进行分级分域管理，对不同级别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；

b）加强数据处理系统、数据存储环境安全防护；

c）积极应对数据存储方面数据安全事件，防范针对和利用数据存储的违法犯罪活动；

d）存储数据的系统原则上应当满足三级以上网络安全等级保护和关键信息基础设施安全保护要求，存储核心数据的系统依照有关规定从严保护；

e）存储核心数据、重要数据等敏感数据时，应采用加密、安全存储、访问控制、安全审计等安全措施；

f）防范数据泄露、篡改、损坏和丢失，加强数据访问权限管理，合理配置管理员权限，强化数据存储权限管理、监督和审计；

g）对不同等级的数据选择安全性能、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，建立能源大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；

h）公开数据可长期存储于第三方云平台，采取通用安全保护措施进行适度防护，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。

9 能源大数据应用合规管理要求

能源数据汇集者（能源大数据中心）、能源数据使用者应根据能源数据分类分级情况，针对政府、企业、公众等不同服务主体，对应数据接口、分析报告等不同的应用服务提供形式，制定差异化的能源数据应用合规管控方案。应采取以下措施：

a）数据应用活动涉及核心数据、重要数据、个人信息等负面清单数据，应严格履行数据内部共享审批流程，遵循使用范围规定，保证数据应用安全；

b）数据应用活动涉及个人信息，不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围。使用敏感个人信息，应取得个人单独同意，并采用去标识化、脱敏等手段加以保护，满足个人隐私保护要求，防范个人信息泄露风险；

c）对于数据对外导出，为防止数据泄露，应收缩汇集数据导出出口，核心数据、重要数据脱离内部网络环境对外提供时，应采取数据内容防泄漏、数据脱敏、数字水印和数据审计等措施，实现数据泄露和多权利主体数据导出异常行为可追溯。在线导出数据时，应有隔离措施，确保内外网隔离安全。数据对外导出时应符合相关保密要求；

d）对于数据内部分析测试，在从生产环境导出重要数据用于内部系统测试或数据分析时，应结合业务需求对核心数据、重要数据进行脱敏并添加数字水印，确保外部测试或分析人员越权复制数据导致的泄露行为可追溯；

e）对于数据在线浏览，在线浏览核心数据、重要数据时，应根据用户权限进行差异性实时脱敏并添加与用户对应的页面中包含用户信息的数字水印，确保因拍照或截屏造成的数据泄露行为可溯源；

f）应基于内部受控环境，开展数据的在线查询和在线应用，不得自行将数据拷贝和提供他人；属于数据共享负面清单的应按照数据使用审批程序进行授权办理；

g）对能源大数据的应用应定期进行合规评估，确保数据的使用符合初始收集和共享的目的，并防止越权访问、数据滥用和安全隐患。

10　能源大数据对外开放合规管理要求

能源数据汇集者（能源大数据中心）应执行差异化的数据对外开放策略，针对不同需求主体、需求内容以及数据用途，制定并持续完善能源数据对外开放策略和流程，确保数据应用合规；对外提供数据或公开披露数据时，应充分重视风险并采取以下措施：

a）事先开展安全影响分析和风险评估，并依据评估结果采取有效的保护措施；

b）公开披露数据前告知相关方公开披露信息的目的、类型，并征得相关方明示同意；

c）开展共享、转让、委托处理等对外提供数据活动时，通过合同等形式约定双方的数据安全责任和义务；

d）对外提供核心数据、重要数据时，应严格按有关规定进行审批，与对方签订保密协议，限定数据使用目的、范围和方式，明确协议期限以及违约责任等，并采取数字水印等反泄露技术措施；

e）除公安机关、国家安全机关依法调取数据以及客户查阅本人信息外，原则上不对外提供明细业务数据。

11　能源大数据退役合规管理要求

能源数据相关方应按照业务发展和外部监管需求设计数据退役机制，开展对历史数据的退役管理，采取以下措施：

a）按照法规、业务和技术需要执行数据退役操作，完成数据的归档、迁移和清除等工作；

b）建立数据恢复检查机制，定期检查退役数据状态,确保数据在需要时可恢复；

c）提供归档数据查询，根据业务管理或监管需要,支持对相关数据进行恢复以供应用；

d）核心数据、重要数据不再继续使用时，应采取不可逆措施及时销毁，防范数据泄露；

e）当已归档一般数据达到一定期限不再被使用时，依据数据分类分级策略制定数据销毁清单、数据沉寂清单，经审定后，对后续需要使用的数据采取沉寂操作，沉寂的数据以数据库备份文件的方式储存；对不再使用的数据采取销毁操作。在数据存储介质销毁前，须确认介质中储存的数据已安全删除。