中国科学院厅局文件

传播字〔2022〕12号

中国科学院网络安全和信息化领导小组办公室关于印发《中国科学院数据安全管理办法（试行）》的通知

院属各单位、院机关各部门:

现将《中国科学院数据安全管理办法（试行）》印发给你们，请认真贯彻落实。

中国科学院网络安全和信息化领导小组办公室

（代章）

2022年12月30日

（此件不予公开）

中国科学院数据安全管理办法（试行）

第一章　总　　则

第一条 为加强数据安全管理，保障数据安全，促进数据共享利用，维护国家安全和发展利益，根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国国家安全法》等法律法规，结合中国科学院实际，制定本办法。

第二条 本办法所称数据，是指科研和管理活动过程中收集或产生的，任何以电子或者其他方式对信息的记录，包括在科学研究过程中产生的科学数据，科研条件、综合管理、信息系统运维过程中收集和产生的数据，以及经过统计、关联、挖掘、聚合等加工活动而产生的衍生数据等。

本办法所称数据处理者，是指包括但不限于数据持有者、数据管理者、数据使用者、数据服务者等数据处理活动中自主决定处理目的、处理方式的各类主体。数据处理活动包括但不限于数据收集、存储、使用、加工、传输、提供、公开等活动。

第三条 中国科学院数据安全工作总体目标是以贯彻总体国家安全观的目的为出发点，统筹安全与开放共享，建立院所两级的数据安全工作协调机制，落实数据安全责任，实施数据

分类分级保护，建立健全数据安全基础制度，规范数据跨境和跨主体流动，促进数据安全规范利用。

第四条 中国科学院支持开展数据安全知识宣传普及活动，提高数据安全保护意识和水平，推动各单位、科研人员共同参与数据安全工作，形成共同维护数据安全和促进数据发展的良好环境。

第二章　组织机构与工作职责

第五条 按照“谁管业务，谁管业务数据，谁管数据安全”原则，建立院所两级数据安全责任体系。在中国科学院党组的领导下，院机关、各分院对本部门的数据安全工作负主体责任，对职责范围内数据安全负监管责任；院属各单位对本单位数据安全负主体责任。

第六条 中国科学院网络安全和信息化领导小组（简称“院网信领导小组”）在国家数据安全工作协调机制统筹协调下，负责监督指导数据安全工作，向中国科学院党组负责。下设中国科学院数据安全工作协调小组（简称“院协调小组”），具体负责落实国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，监督并指导院数据安全工作。

第七条 中国科学院网络安全和信息化领导小组办公室（以下简称“院网信办”）是中国科学院数据安全工作的管理部门。下设中

国科学院数据安全工作推进组（简称“院工作推进组”），具体协调院机关各部门开展数据分类分级、重要数据和核心数据目录报送等工作。院网信办具体职责包括：

（一）贯彻执行院网信领导小组、院协调小组工作部署，研究制定数据安全管理相关实施办法和规定；

（二）统筹协调中国科学院与数据安全国家管理部门、属地管理部门及其它部委的数据安全工作；

（三）统筹协调并指导院机关各部门、各分院、院属各单位落实数据安全主体责任；

（四）负责科学数据中心体系建设，并按照“应建尽建”原则，指导院属各单位建设数据中心，为数据安全管理提供条件保障；

（五）负责向国家数据安全工作协调机制办公室报送全院重要数据和核心数据目录信息；

（六）负责定期监管、审查全院数据安全保护工作，制定全院数据安全保护考核评估体系，定期考核全院数据安全保护工作；

（七）统筹建立院数据安全风险监测和预警机制，协调全院数据安全应急事件处置；

（八）负责面向全院组织开展数据安全宣传教育和培训；

（九）负责重要数据出境安全评估管理与咨询工作。

第八条 院机关各部门职责：

（一）落实本部门数据安全主体责任，做好本部门数据安全

定期监管、审查等工作;

（二）负责本部门数据分类，以及重要数据和核心数据目录报送、动态更新工作;

（三）负责业务所属范围内的院属各单位重要数据和核心数据目录审核、数据安全保护考核评估、风险评估等工作。

第九条 各分院职责:

（一）负责在本系统内贯彻执行党和国家关于数据安全工作的方针政策和法律法规，落实院数据安全工作各项部署;

（二）落实本单位的数据安全主体责任，负责本单位重要数据和核心数据目录报送和动态更新工作，做好数据安全保护考核评估、风险评估、应急预案设置和应急事件处置等工作;

（三）督促检查本系统各单位的数据安全工作，对发现问题和隐患及时督办整改;

（四）督促指导本系统各单位妥善处理各类数据安全案件、事件和事故，相关情况及时上报属地管理部门和院网信办;

（五）组织和督促开展数据安全宣传教育和培训;

（六）负责与属地数据安全管理部门的沟通和协调。

第十条 院属各单位是数据安全工作的责任主体和实施主体，应明确领导班子主要负责人是第一责任人，分管数据安全的班子成员是直接责任人，其他成员对职责范围内的数据安全负领导责任。原则上由本单位网信领导小组负责指导数据安全

工作，也可设立专门数据安全工作领导机构或组织。各单位应统一规划建设所级的数据中心，配备专职技术队伍，提供充分条件保障。院属各单位具体职责是:

（一）制定本单位数据安全管理相关实施细则;

（二）建立完善的数据安全工作体系，加强专职队伍建设，组织本单位数据处理者开展数据分类定级、重要数据和核心数据数据目录报送等工作;

（三）定期开展本单位数据安全风险评估，做好数据安全监测预警，突发情况及时向分院和院网信办报告;

（四）制定数据安全事件应急处置预案，定期开展应急演练;

（五）开展数据安全宣传教育和培训;

（六）做好重要数据出境和核心数据跨主体流动的申报工作。

第三章 数据分类分级管理

第十一条 院网信办负责组织制定中国科学院数据分类分级、重要数据和核心数据识别认定、数据分级防护等标准规范，并保持动态更新。

第十二条 数据分类遵从科学实用的原则，从落实安全主体责任、便于数据管理和使用的角度，科学选择主题明确、常见、稳定的属性或特征作为数据分类的依据，并结合实际需要对数据进行细化分类。按照“先业务领域、学科领域分类，再

业务属性分类”分类思路，中国科学院数据实施多级分类管理，一级分类包括但不限于科学数据、科研条件数据、综合管理数据和信息系统数据等。

第十三条 数据分级应遵从边界清晰、点面结合、动态更新原则。根据数据遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益等造成的危害程度，数据分为一般数据、重要数据和核心数据三级。

（一）核心数据，是指对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的重要数据，一旦被非法使用或共享，可能直接影响政治安全。主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，以及经国家有关部门评估确定的其他数据。核心数据不得跨境流动，未经批准不得跨主体流动。

（二）重要数据，是指特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。仅影响组织自身或公民个体的数据一般不作为重要数据。重要数据未经批准不得跨境流动。

（三）一般数据，是指除核心数据和重要数据以外的数据。一般数据依法流通。

第十四条 数据处理者应定期梳理数据，按照中国科学院

重要数据和核心数据识别规范或国家标准等其他规范性文件，识别重要数据和核心数据。重要数据和核心数据目录信息，由数据所属单位或部门按要求定期通过中国科学院重要数据目录报送平台报送备案，备案内容包括但不限于数据来源、类别、级别、规模、载体、处理目的、共享范围和方式、对外共享、跨境传输、责任主体、安全保护措施等基本情况，不包括数据内容本身。

第十五条 重要数据和核心数据目录报送备案流程如下：

（一）数据目录初审：院属各单位、各分院的数据目录由单位法定代表人审定，院机关各部门的数据目录由部门分管院领导审定；

（二）数据目录复审：院机关各部门按照业务分工负责对院属各单位的重要数据和核心数据目录复核，院网信办负责对院机关各部门重要数据和核心数据目录复核；

（三）数据目录审定：院网信办汇总中国科学院重要数据和核心数据目录，报院网信领导小组审定；

（四）上报国家备案：院网信办按要求将重要数据和核心数据目录报国家数据安全工作协调机制办公室审核备案。

第四章　数据全生命周期安全管理

第十六条 数据处理者当对数据处理活动安全负主体责任，

对各类数据实行分级防护，不同级别数据同时被处理且难以分别采取保护措施的，应当按照其中级别最高的要求实施保护，确保数据持续处于有效保护和合法利用的状态。

第十七条 数据处理者应建立数据全生命周期安全管理制度，针对不同级别数据，制定数据收集、存储、使用、加工、传输、提供、公开、销毁等环节的具体分级防护要求和操作规程；合理确定数据处理活动的操作权限，严格实施人员权限管理。

重要数据和核心数据处理者还应明确数据处理关键岗位和岗位职责，并要求关键岗位人员签署数据安全责任书，责任书内容包括但不限于数据安全岗位职责、义务、处罚措施、注意事项等内容；建立内部登记、审批等工作机制，对重要数据和核心数据的处理活动进行严格管理并留存记录。

第十八条 数据处理者收集数据应当遵循合法、正当的原则，不得窃取或者以其他非法方式收集数据。

数据收集过程中，应当根据数据安全级别采取相应的安全措施，加强重要数据和核心数据收集人员、设备的管理，并对收集来源、时间、类型、数量、频度、流向等进行记录。

通过间接途径获取重要数据和核心数据的，数据处理者应当与数据提供方通过签署相关协议、承诺书等方式，明确双方法律责任。

第十九条 数据处理者按照法律、行政法规等规定进行数据存储。存储重要数据和核心数据的，应当采用校验技术、密码技术等措施进行安全存储，并实施数据容灾备份和存储介质安全管理，定期开展数据恢复测试。

第二十条 数据处理者利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。使用、加工重要数据和核心数据的，还应当加强访问控制。

第二十一条 数据处理者根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。传输重要数据和核心数据的，应当采取校验技术、国产密码技术、安全传输通道或者安全传输协议等措施。

第二十二条 数据处理者对外提供数据，应当明确提供的范围、类别、条件、程序等。提供重要数据和核心数据的，应当与数据获取方签订数据安全协议，对数据获取方数据安全保护能力进行核验，采取必要的安全保护措施。

数据处理者委托他人开展数据处理活动的，应当通过签订合同协议等方式，明确委托方与受托方的数据安全责任和义务。委托处理重要数据和核心数据的，应当对受托方的数据安全保护能力、资质进行核验。

第二十三条 数据处理者应当建立数据销毁制度，明确销毁对象、规则、流程和技术等要求，对销毁活动进行记录和留

存。个人、组织按照法律规定、合同约定等请求销毁的，数据处理者应当销毁相应数据。

数据处理者销毁重要数据和核心数据后，不得以任何理由、任何方式对销毁数据进行恢复，引起备案内容发生变化的，应当履行备案变更手续。

第二十四条 数据处理者应当在数据全生命周期处理过程中，记录数据处理、权限管理、人员操作等日志。日志留存时间按有关规定执行，无特殊规定的不少于六个月。

第五章 数据安全监测预警与应急管理

第二十五条 院网信办建立数据安全风险监测机制，组织制定数据安全监测预警接口和标准，统筹建设数据安全监测预警技术手段，形成监测、预警、处置、溯源等能力，与相关部门加强信息共享。

院机关各部门、各分院、院属各单位监管部门分别建设本部门、本系统、本单位数据安全风险监测预警机制，组织开展数据安全风险监测，按照有关规定及时发布预警信息，及时采取应对措施。开展数据安全风险监测，及时排查安全隐患，采取必要的措施防范数据安全风险。

第二十六条 院网信办建立数据安全风险信息上报和共享机制，汇集、分析、研判和通报数据安全风险信息。

院属各单位应及时向所属分院、属地管理部门上报风险情况并做好风险应急处置各项准备。各分院应立即排查相关单位风险情况，并及时上报院网信办。

第二十七条 院网信办负责制定中国科学院数据安全事件应急预案，组织协调重要数据和核心数据安全事件应急处置工作。

院机关各部门、各分院分别组织开展监管范围内的数据安全事件应急处置工作。涉及重要数据和核心数据的安全事件，应当立即上报院网信办，并及时报告事件发展和处置情况。

院属各单位在数据安全事件发生后，应当按照应急预案，及时开展应急处置，涉及重要数据和核心数据的安全事件，第一时间逐级上报。事件处置完成后及时将处置情况书面报告院网信办。

第六章 数据出境安全管理

第二十八条 数据出境安全评估坚持事前评估和持续监督相结合、风险自评估与安全评估相结合，防范数据出境安全风险，保障数据依法有序自由流动。

第二十九条 数据处理者向境外提供重要数据，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估，

同时报院网信办备案。

第三十条 数据处理者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:

（一）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;

（二）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;

（三）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;

（四）数据出境中和出境后遭受篡改、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;

（五）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（以下统称法律文件）是否充分约定了数据安全保护责任义务;

（六）其他可能影响数据出境安全的事项。

第三十一条 数据处理者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:

（一）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;

（二）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;

（三）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;

（四）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;

（五）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;

（六）出境数据遭受篡改、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。

第三十二条 已经通过评估的数据出境活动在实际处理过程中不再符合数据出境安全管理要求的，数据出境申请人应终止数据出境活动。数据出境申请人需要继续开展数据出境活动的，应当按照要求整改，整改完成后重新申报评估。

第三十三条 对于国家采取的数据跨境流动安全风险监测技术措施，任何组织和个人不得提供用于破坏、避开的程序、工具、路线等。

第七章 监督管理

第三十四条 院网信办、院机关各部门、各分院及院属各单位定期开展监管范围内的数据安全监督审查工作。院网信办适时开展监督抽查。

在履行数据安全监督管理职责中，发现数据处理活动存在较大安全风险的，可以按照规定权限和程序对数据处理者进行约谈，并要求采取措施进行整改，消除隐患。

第三十五条 数据安全监督审查内容包括但不限于以下情况：

（一）数据基本情况，如数据类别、数据级别、数据载体、数据来源、数据数量、数据精度、详细描述等；

（二）责任主体情况，如重要数据、核心数据处理者信息、所属者地区、所属主管（监管）部门等；

（三）数据处理情况，如数据处理活动方式、是否出境、是否跨主体流动等；

（四）数据安全情况，如网络安全等级保护和关键信息基础设施安全保护情况等。

第三十六条 对违反本办法规定行为的，根据事故性质和危害程度，按照相关规定对相关单位和人员给予警告、通报批评等相应处分；对违反我国法律、行政法规禁止性规定的数据

安全损害行为，及时移交具体责任部门处理，并由其依法追究刑事责任。

第八章 附　　则

第三十七条 涉及国家秘密的数据和军事数据，按照国家有关规定执行。

第三十八条 开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

第三十九条 本办法由院网信办负责解释。

第四十条 本办法自发布之日起施行。

科学传播局　　2023年1月3日印发