附件 1

工业和信息化领域数据安全合规指引

（征求意见稿）

征求意见稿

编制说明

数据作为新型生产要素，是数字化、网络化、智能化的基础，已快速融入生产、分配、流通等各环节，保障数据安全，事关国家安全大局。工业和信息化领域是数字经济发展的主阵地和先导区，是推进数字经济做强做优做大的主力军。随着数字化转型进入全面加速期，数据资产的价值和重要性不断提升，数据泄露、篡改、破坏导致的影响日趋严重。国家层面对数据安全更加重视，《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》《数据出境安全评估办法》《促进和规范数据跨境流动规定》《工业和信息化领域数据安全管理办法（试行）》等数据安全相关法律政策不断颁布实施，为开展数据安全监管和保护工作提供了根本遵循，对数据处理者落实数据安全保护责任义务指明了方向、提出了要求。

为引导工业和信息化领域数据处理者合法合规开展数据处理活动，编制《工业和信息化领域数据安全合规指引》，聚焦数据处理者在履行数据安全保护义务过程中的难点问题，明确数据安全合规依据，提供实务指引，指导数据处理者开展数据安全合规管理，提升数据安全保护能力。

编制单位[1]

中国钢铁工业协会、中国有色金属工业协会、中国石油和化学工业联合会、中国建筑材料联合会、中国机械工业联合会、中国汽车工业协会、中国纺织工业联合会、中国轻工业联合会、中国电子信息行业联合会、中国计算机行业协会、中国通信标准化协会、中国通信企业协会、中国互联网协会、中国中小企业国际合作协会、中国通信学会、工业和信息化部商用密码应用产业促进联盟、工业信息安全产业发展联盟。

征求意见稿

[1] 编制单位顺序按监管部门行业排序。

目 录

征求意见稿

征求意见稿

1 工业和信息化领域数据安全合规建设概述

1.1 数据安全合规建设目的

为引导工业和信息化领域数据处理者合法合规开展数据处理活动，履行数据安全保护义务，保障数据安全，根据我国现行数据安全法律法规以及工业和信息化领域相关政策标准，制定本指引。

1.2 数据安全合规建设依据

《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》

《促进和规范数据跨境流动规定》

《数据出境安全评估办法》

《数据出境安全评估申报指南（第二版）》

《个人信息出境标准合同办法》

《个人信息保护认证实施规则》

《工业和信息化领域数据安全管理办法（试行）》

《工业和信息化领域数据安全风险评估实施细则（试行）》

《工业和信息化领域数据安全事件应急预案（试行）》

《工业领域重要数据识别指南》

《工业企业数据安全防护要求》

《工业领域数据安全风险评估规范》

《电信领域重要数据识别指南》

《电信领域数据安全分级防护要求》

《电信领域数据安全风险评估规范》

1.3 适用范围

工业和信息化领域数据处理者可参照本指引开展数据处理活动，包括数据收集、存储、使用、加工、传输、提供、公开、销毁等。

本指引所称工业和信息化领域数据处理者是指数据处理活动中自主决定处理目的、处理方式的工业企业、软件和信息技术服务企业、取得电信业务经营许可证的电信业务经营者和无线电频率、台（站）使用单位等工业和信息化领域各类主体。数据处理过程中涉及工业和信息化领域数据的其他有关主体，可参照本指引落实数据安全责任义务。

1.4 术语和定义

1.4.1 重要数据

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、公共利益的工业和信息化领域数据（包括原始数据和汇聚、整合、分析等处理中以及处理后的衍生数据）。危害程度从国家安全、行业安全等方面进行研判，详细判断标准可参照《工业和信息化领域数据安全管理办法（试行）》。仅影响工业和信息化领域数据处理者自身的数据一般不作为重要数据。

1.4.2 核心数据

一旦遭到篡改、破坏、泄露或者非法获取、非法利用，严重危害国家安全、公共利益的工业和信息化领域数据（包括原始数据和汇聚、整合、分析等处理中以及处理后的衍生数据）。危害程度从国家安全、行业安全等方面进行研判，详细判断标准可参照《工业和信息化领域数据安全管理办法（试行）》。

1.4.3 一般数据

核心数据、重要数据之外的其他数据。

1.4.4 重要数据和核心数据处理者

数据处理活动中自主决定重要数据和核心数据处理目的、处理方式的主体。

1.4.5 一般数据处理者

数据处理活动中自主决定一般数据处理目的、处理方式的主体。

1.4.6 行业监管部门

负责对本地区本领域工业和信息化领域数据处理者的数据处理活动和安全保护进行监督管理的工业和信息化主管部门、通信管理局和无线电管理机构，统称为行业监管部门。

1.4.7 工业数据

工业领域各行业企业在研发设计、生产制造、经营管理、

征求意见稿

运行维护、平台运营等过程中产生和收集的数据。

1.4.8 电信数据

在电信业务经营活动中产生和收集的数据。

征求意见稿

2 数据分类分级

2.1 梳理数据资产清单

（1）每年对本单位数据资产至少开展一次全面梳理，形成数据资产清单，并跟踪维护。数据资产清单包含数据类型、级别、规模、数据处理方式、存储位置、用途、出境情况、共享应用情况等内容，详见附件。

（2）梳理过程中，可综合考虑业务规模、种类，数据数量、种类，涉及系统的复杂程度等因素，组建由管理层、数据安全管理责任部门、数据所属部门（包括职能部门和业务部门）等人员组成的工作团队，制定工作计划，分解任务，全面、系统梳理数据资产。

2.2 数据分类

（1）按所属行业要求、特点、业务需求、数据来源和用途等，对数据进行分类，具体可采取“所属行业——业务条线——关键业务——业务属性分类”的方式制定数据分类规则，并可以逐级细化。

（2）工业数据分类可参考研发数据域（研发设计数据、开发测试数据）、生产数据域（控制信息、工况状态、工艺参数、系统日志）、运维数据域（物流数据、产品售后服务数据）、管理数据域（系统设备资产信息、客户与产品信息、产品供应链数据、业务统计数据、人事财务数据等）、外部数据域（与其他主体共享的数据等），并分别细化。

（3）电信数据分类可参考网络规划运维数据域（网络规划建设、网络运行维护等）、安全保障数据域（网络与数据安全保障、物理安全保障、应急通信保障等）、经济运行与业务发展数据域（发展战略与重大决策、关系国家安全和公共利益的非公开统计数据等）、关键技术成果数据域（涉及电信领域出口管制物项相关数据，重大科技成果、国家科技计划等活动中产生的先进技术数据等），并分别细化。

（4）必要时可聘请技术专家、第三方咨询机构参与，指导数据资产梳理、重要数据识别等工作，确保结果的准确性、规范性。

2.3 重要数据识别

（1）工业领域重要数据从国家秘密生成、国家安全、行业发展安全、出口管制物项、行业特色以及其他共 6 个维度进行识别，其中，与行业特色相关的涉及钢铁、有色金属、石化化工、装备工业、消费品、电子信息、软件和信息技术服务等行业。具体识别规则可参照《工业领域重要数据识别指南》。

电信领域重要数据从反映信息系统重要程度、影响行业发展程度、科技成果先进程度数据，以及人群覆盖程度等维度进行识别，根据数据属性首先将电信数据分为网络规划运维数据域、安全保障数据域、经济运行与业务发展数据域、关键技术成果数据域等类别，再根据数据精度、深度、敏感

程度等进行具体识别。具体识别规则可参照《电信领域重要数据识别指南》。

（2）完成全部重要数据识别工作后，根据识别结果规范填写重要数据目录备案表。备案表主要包括数据基本情况、责任主体情况、数据处理情况、数据安全情况等信息。

（3）结合本单位业务情况及业务经营管理需求，可对一般数据进行进一步细化分级。

2.4 重要数据目录报备

（1）按工作部署要求主动报送重要数据目录，如每年9月30日前向所在地行业监管部门报送重要数据目录。

（2）如重要数据目录未获得行业监管部门审核认定，则按要求修改完善目录后重新报备，或者重新开展重要数据识别和目录报送工作。

（3）根据行业监管部门审核认定的重要数据目录，按要求开展保护。

（4）目录报送前，可组织管理层、数据安全管理责任部门相关负责人、技术负责人、专家等对形成的重要数据清单进行内部评审。

2.5 重要数据目录动态更新

发生下述情形时，在发生变化的三个月内向所在地行业监管部门履行备案变更手续，更新目录备案表，说明具体情况。

（1）重要数据和核心数据的类别或规模（条目数量或者存储总量）变化30%以上。

（2）其他备案内容发生重大变化的，如重要数据和核心数据的详细描述、数据安全风险评估情况、数据安全负责人等。

（3）销毁、转移重要数据和核心数据。

征求意见稿

3 数据安全管理体系

3.1 数据安全组织架构

3.1.1 一般数据处理者

（1）配备数据安全管理责任部门

明确数据安全管理责任部门，配备数据安全管理人员。数据安全管理责任部门负责统筹本单位数据处理活动的安全监督管理，可独立设置，也可结合实际情况由职责相近的有关部门负责，主要承担以下职责:

- 组织制定本单位数据安全管理制度规范与工作计划，并推动其有效实施。
- 统筹实施、指导数据安全管理工作，并对数据安全管理情况进行评估与检查。
- 为单位内相关职能部门提供数据安全咨询与支持。
- 及时向管理层报告数据安全重大风险和数据安全工作落实情况。
- 对行业监管部门开展监管执法工作予以积极配合。

（2）开展数据安全教育与培训

- 结合业务经营需求制定数据安全培训计划，定期组织或协助相关部门开展数据安全培训，每年至少开展一次。培训范围覆盖数据安全管理人员、评估人员、审计人员以及系统开发运维、业务运营、客户服务等可能接触企业数据和个人用户数据的人员开展数据安全教育和培训的。。

- 培训内容包含岗位内数据安全有关职责、数据安全法规、本单位数据安全制度规范及工作计划、数据安全领域知识技能、数据安全保护意识和责任义务等。

- 接触一般数据的数据安全工作岗位人员年度培训时长应不少于10学时，其中实操培训时长应不少于3学时。关键岗位人员培训内容还应包括重要数据和核心数据安全管理要求、安全操作规程等，年度培训时长不少于20学时，其中实操培训时长应不少于5学时。相关人员完成培训后应进行考核评定。

3.1.2 重要数据和核心数据处理者

在满足3.1.1的基础上，做好以下工作:

（1）明确领导责任

本单位法定代表人或者主要负责人是数据安全第一责任人，领导团队中分管数据安全的成员是直接责任人。

数据安全第一责任人主要负责单位内数据安全管理制度的构建和运行，提供必要的资源保障和条件支持，牵头特别重大数据安全事件应急处置等。

数据安全直接责任人主要负责:

- 确立符合本单位战略方向的数据安全方针和目标。

- 保障数据安全管理责任部门具备独立履行职责的能力与权限。

- 审批单位内重大数据安全合规事项。

- 确保将数据安全管理要求融入单位内的业务过程。
- 解决数据安全工作中的关键问题，确保本单位数据安全工作顺利进行。
- 确保建立有效的数据安全违规举报与惩处机制。

（2）建立数据安全工作架构

设置数据安全管理责任部门并配备至少一名数据安全专职人员，建立健全覆盖数据安全管理责任部门以及研发设计、生产制造、经营管理、运行维护、外部服务、采购、销售、审计、法务等相关部门的数据安全工作体系。

数据安全管理责任部门主要负责：

- 组织制定单位内数据安全管理制度规范与工作计划，并推动其有效实施。
- 统筹实施数据安全管理工作，并对数据安全管理情况进行评估与检查。
- 建立数据安全举报与调查机制，对数据安全合规举报制定调查方案并开展调查。
- 定期组织或协助相关部门开展数据安全培训，为单位内相关部门提供数据安全咨询与支持。
- 向数据安全直接责任人报告数据安全重大风险和相关工作落实情况。
- 对行业监管部门开展监管执法工作予以积极配合。

单位内开展数据处理的各职能与业务部门配合数据安

全相关管理工作，具体职责如下:

- 结合单位内数据安全管理制度规范和工作指引，明确本部门日常数据处理活动的全生命周期要求和具体工作机制。
- 确保本部门员工遵守数据安全制度规范，履行数据安全义务。
- 配合数据安全责任部门开展监督检查、风险评估、整改等各项工作。
- 密切监测日常数据处理工作中的数据安全风险，并采取适当的安全保护措施。
- 当发现数据处理活动存在较大数据安全风险或者发生数据安全事件时，及时向数据安全管理责任部门报告，并配合采取应急处置和整改措施。

（3）设置关键岗位和职责

- 将处理重要数据和核心数据的操作人员，关键业务系统、平台管理人员及设备运维人员，高操作权限的管理人员等设定为关键岗位，明确岗位职责。
- 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。
- 要求离岗关键岗位人员签订保密承诺书，继续履行不泄露本单位重要数据和核心数据的责任义务。

3.2 数据安全管理制度

依照法规政策规定，结合所属行业领域的数据特征、数据处理场景等，建立健全覆盖数据全生命周期的差异化数据安全管理制度，制定本单位数据安全管理、数据分类分级、数据全生命周期保护管理、数据安全风险评估、数据容灾备份与恢复、数据安全应急处置、数据跨境安全传输、数据合作协议规范、个人信息保护管理、供应商管理等有关要求。

对重要数据与核心数据实施更加严格的制度管理和操作规范，设置更为严格的数据处理权限、建立内部登记审批机制，采取记录访问和操作留痕等方式，强化重要数据与核心数据的安全保障。

3.3 权限管理

3.3.1 一般数据处理者

（1）制定数据访问处理权限管理制度。明确数据权限分配、开通、使用、变更、注销等要求和审批流程，避免出现越权访问、下载、复制、修改数据等行为。

（2）严格实施人员权限管理，按照最小授权原则合理确定数据访问与操作权限、分配账号权限，仅在完成职责所需的范围内授予特定人员最小必要的数据操作权限。建立并定期更新权限分配情况台账，确保权限到人。

（3）合理界定相关人员的数据访问和处理权限，对数据处理、数据安全管理、日志审计等岗位角色进行分离设置，

严格控制超级管理员权限账号数量，确保超级管理员权限账号存在的必要性。

3.3.2 重要数据和核心数据处理者

在满足 3.3.1 的基础上，做好以下工作:

（1）配备权限管理配套保障功能，如限制非正常登录次数、登录连接超时自动退出、配置口令遗忘申请和重置流程、账号口令加密保护、低活跃度账号监测、沉默账号定期检测关闭等措施。

（2)定期审计重要数据和核心数据相关账号分配台账，重点关注离职人员账号回收、账号权限变更、沉默账号安全等问题，在人员变更、调离或终止劳动合同时，及时变更或终止其数据处理权限。

（3）采用对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等商用密码技术对重要的权限数据（例如用户权限列表、系统权限列表等）进行完整性保护，防止权限数据被非授权篡改。

3.4 内部审批、登记

3.4.1 一般数据处理者

根据业务经营需求，可参照重要数据和核心数据处理者要求建设应用。

3.4.2 重要数据和核心数据处理者

（1）针对重要数据和核心数据对外提供、委托处理、转移、销毁、公开、出境，跨组织机构或者使用公共信息网络进行传输，以及批量复制、传输、使用加工、提供和销毁等情形建立内部登记、审批机制，明确重要数据和核心数据访问处理单次授权、多人审批和行为审计等要求和登记、审批流程。通过专线或线下方式访问处理重要数据和核心数据的，应对数据处理方式、数据流转区域范围、数据承载介质等管理要求和登记、审批流程进行明确。

（2）审批时应提交相关数据操作所涉及的数据处理主体、数据数量、类别、级别、处理方式、目的、范围、时效，以及审批人员和时间。审批通过后，对上述信息进行记录，形成台账，通过线下表单、邮件等方式进行审批的还应留存原始审批记录，方便溯源查询。

（3）审批程序上履行先审后做的要求，避免出现审批时间和数据处理时间倒挂情形。

3.5 系统与设备安全管理

3.5.1 一般数据处理者

（1）对数据库、研发终端、关键业务设备、开发代码库等数据载体及数据采集系统进行安全配置，建立安全配置清单，定期进行配置审计。

（2）密切关注数据载体的重大安全漏洞及其补丁发布，及时采取升级措施，短期内无法升级的，开展针对性安全加

固。

（3）强化数据载体的登录账户、口令管理，避免使用默认口令或弱口令，定期更新口令，禁止账号共享。

（4）在服务器、工程师站等主机上部署防病毒软件或采用应用软件白名单技术，防范勒索病毒等造成的数据破坏攻击行为。

（5）采取最小化原则，避免关键业务系统面向互联网开通 HTTP、FTP、Telnet、RDP 等高风险通用网络服务，对必要开通的网络服务采取安全接入代理等手段进行用户身份认证和应用鉴权。

3.5.2 重要数据和核心数据处理者

在满足 3.5.1 的基础上，做好以下工作:

（1）对涉及重要数据和核心数据处理活动的数据载体的加强访问控制，设置多因子身份鉴别、口令复杂度策略、账号锁定策略等安全措施。

（2）对涉及重要数据和核心数据处理活动的数据载体，通过防火墙、网闸等防护设备设置合理的隔离方式，包括物理隔离、逻辑隔离、网络隔离等。

（3）对关键业务系统的开发、测试和生产环境进行逻辑或物理隔离。

（4）处理重要数据的系统应满足三级及以上网络安全等级保护要求，处理核心数据的系统依照关键信息基础设施

安全保护有关规定从严保护。

3.6 容灾备份

3.6.1 一般数据处理者

根据业务经营需求，可参照重要数据和核心数据处理者要求建设应用。

3.6.2 重要数据和核心数据处理者

（1）数据安全管理责任部门组织数据所属部门明确重要数据和核心数据的备份要求和操作规程，制定备份策略，策略内容应包括数据备份对象、责任人、操作步骤、周期、备份方式（如全量备份、增量备份）、异地备份要求、存储介质、命名规则、保存期、责任人以及有效性测试周期等。对核心数据存储设备进行硬件冗余，启用实时数据备份功能，保证主设备出现故障时冗余设备可以及时切换并恢复数据。

（2）数据所属部门按照备份策略，对重要数据和核心数据分别开展备份。

（3）数据安全管理责任部门对是否备份、是否按要求备份等情况进行验证与检查。

（4）数据安全管理责任部门组织数据所属部门根据策略的要求定期执行备份介质有效性测试，确保备份介质内的数据可恢复，并填写形成测试报告，留存相关记录。

（5）涉及非电子化重要数据和核心数据的，应明确相

关数据备份单独存放、专门管理等要求，并建立包括备份数据名称、类别级别、数据规模、备份介质、存放地点、备份周期和责任人等信息的台账，同时明确台账视同重要数据进行管理。

3.7 第三方管理

3.7.1 一般数据处理者

根据业务经营需求，可参照重要数据和核心数据处理者要求建设应用。

3.7.2 重要数据和核心数据处理者

3.7.2.1 数据提供方

（1）开展事前评估

对提供数据的内容开展合规性与必要性评估，评估内容包括数据提供的必要性，涉及数据的数量、类别、级别、范围、使用用途等，是否存在数据泄露等风险，以及采取的保护措施等，确保数据提供正当、必要。

（2）审核数据接收方保护能力

对数据接收方的数据安全保护能力进行评估和审核，审核内容包括数据安全风险评估结果、数据安全制度设置和日常管理（企业管理制度建立情况、管理落实机制建设情况、相关工作记录等）、技术手段应用（数据保护、风险监测等技术手段能力说明、建设规范、应用截图）等。

（3）签订数据安全协议

征求意见稿

通过签订合同协议等方式明确不同类型数据提供的安全保护方式以及双方数据安全责任和义务。数据安全协议可参考下述内容:

- 数据提供的基本情况，如数据类型、级别、使用目的、用途、范围、数据安全保护要求等。
- 明确禁止不缓存、窃取、泄漏、滥用、非法向其他人提供本单位数据等要求，不将加工后的数据还原成原始数据。
- 明确数据接受方员工在本单位平台系统中的权限范围（应符合最小化原则）等。
- 履行保密义务。
- 合作结束后，要求数据接收方及时销毁数据。
- 违约责任和处罚条款。发生数据安全事件或存在数据安全风险，立刻暂停合作，进行整改。整改未完成前，不开展数据合作。
- 遵守本单位相关管理办法，配备相应的数据安全保护措施，并接受必要的安全监控和审计等。

（4）人员管理

- 根据岗位职责对数据接收方人员设置相应的平台系统、物理设施访问权限。

● 对接触重要数据和核心数据，涉及数据批量操作，对关键业务系统拥有管理权限的数据接收方人员进行背景审查和保密审查。

● 在数据接收方人员转岗或离岗前，要求数据接收方提供相关人员转岗或离岗申请书，用人部门根据相关规定完成相关人员的账号回收、审核、权限调整等工作，并签署转岗或离岗审批意见，签订数据安全保密承诺书，数据接受方人员方可转岗或离岗。

（5）建立管理台账

建立数据接收方管理台账，梳理形成并定期更新本单位涉及的数据接收方清单，包含单位名称、业务或系统、数据接收形式、合作期限、数据接收方联系人、数据接收方是否发生过数据安全事件等，加强对数据接收方数据使用情况的监督管理。

3.7.2.2 数据接收方

（1）数据合规性审查

审核数据提供方身份，并对数据提供方提供的数据来源的合法性进行确认，留存审核、交易记录，确保数据的真实性、有效性、安全性，避免收集不明来源的数据。

（2）落实数据安全保护

● 根据数据安全协议在数据服务合作过程中履行数据安全保护责任，按照数据级别落实防护要求。

- 配合数据提供方开展数据提供前的数据保护能力评估与审核、数据提供中的数据安全保护情况的监督检查等工作。

- 若发生数据安全事件或发现重大数据安全风险，第一时间向数据提供方报告，并立刻采取处置措施，消减危害影响。

3.8 日志管理

3.8.1 一般数据处理者

（1）数据全生命周期处理过程中对数据处理、权限管理、人员操作、数据授权访问、批量操作、开放共享、销毁、数据接口调用等重点环节实施日志留存管理，日志记录包括执行时间、操作账号、处理方式、授权情况、IP 地址、登录信息等，能够对识别和追溯数据操作和访问行为提供支撑。

（2）日志留存时间不少于 6 个月。

（3）可通过建立统一安全审计平台（或通过其他具备日志审计能力的方式）对数据处理活动定期开展审计活动，形成审计报告，并对审计发现的问题进行处理，形成闭环管理。

3.8.2 重要数据和核心数据处理者

在满足 3.8.1 的基础上，做好以下工作:

（1）对日志访问和处理加强管理。

征求意见稿

（2）对高风险操作（如批量复制、批量传输、批量销毁等操作）日志进行备份和完整性校验，保障日志文件的可用性和真实性。

（3）通过统一安全审计平台（或在通过其他具备日志审计能力的方式）对重要数据和核心数据收集、传输、访问、使用、提供等进行定期审计，形成审计报告，并对审计发现的问题进行处理，形成闭环管理。

（4）记录维护数据安全所需的日志。涉及安全事件处置溯源的，相关日志留存时间不少于1年；涉及向他人提供、委托处理、共同处理重要数据的，相关日志留存时间不少于3年；涉及核心数据安全、事件处置、溯源相关日志留存时间不少于3年。

（5）采用对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等商用密码技术对重要的日志数据（例如系统管理员或用户登陆、查询、删除、添加、修改等操作的日志等）进行存储完整性保护，防止重要日志数据被非授权篡改。

3.9 监督检查

可结合实际需要建立数据安全监督检查机制，对本单位内数据安全管理情况和落实效果进行监督检查，保障监督检查工作的标准化、制度化、精细化、规范化。

3.9.1 监督检查工作机制

（1）本单位数据安全管理责任部门负责对各职能与业务部门进行数据安全义务落实情况的监督、检查、核查、督促、整改等工作。

（2）可于每年年初结合上一年监督检查情况，制定本年度监督检查计划。

（3）可按照每半年至少开展一次的频率，组织相关部门开展监督检查。

（4）针对地方行业监管部门发现并通报的重大数据安全事件，或外部形势发生的重大变化，数据安全管理责任部门可适时增加监督检查频率或进行专项监督检查。

3.9.2 监督检查内容

（1）数据分类分级落实情况，如数据资产梳理范围是否全面，新上线系统等新增数据资产是否纳入梳理范围，是否有新增重要数据和核心数据，已识别的重要数据和核心数据是否发生变更等。

（2）数据安全教育培训情况，如是否按照制度要求完成教育培训，覆盖人员、培训内容、培训时长和频率等是否符合有关要求。

（3）技术措施部署情况，如是否基于数据分类分级情况配备相应的数据安全保护措施（数据加密、操作权限管理、数据流动记录、人员操作记录、数据备份与恢复等技术能力和措施是否落实到位）。

（4）监测溯源技术能力落实情况，如是否具备相应技术手段开展重要数据和核心数据实现安全风险监测、数据安全事件溯源等。

（5）接口安全情况，如是否明确数据接口调用安全控制措施、数据接口使用规则及协议，是否具备接口鉴权、接口调用审计、接口调用日志记录等技术能力。

（6）数据使用情况，如是否建立数据使用正当性的内部审批责任制度，是否采取必要的访问控制措施对用户个人信息、重要数据等对外披露使用去标识化措施。

（7）数据合作情况，如是否明确数据共享涉及机构或部门的相关职责和权限、明确共享数据相关使用者的数据保护责任，是否针对数据共享涉及的数据类型、数据内容、数据格式、以及常见场景制定细化的规范要求，是否建立规范的数据共享的审核流程，在开展第三方业务合作时是否采取事前审核、合同约束、信用管理等手段，业务合作结束后是否督促业务合作方依照合同约定及时关闭数据接口、删除数据。

（8）其他监督检查内容。

3.9.3 监督检查问题处置

（1）与被检查对象沟通确认数据安全监督检查中发现的问题并签字。

（2）针对发现的问题，由数据安全管理责任部门发起

整改，并跟踪整改情况。

3.10 配合监管

（1）建立监管执法配合机制，受到行业监管部门调查时立即通知数据安全负责人、数据安全管理部门负责人和相关职能部门负责人等人员，明确监管调查对接人员。

（2）对行业监管部门的监管执法予以配合、协助，对包括组织运作、制度文件、技术系统、算法原理、数据处理程序等进行解释说明，提供相关真实资料信息，安全开放相关数据访问、提供必要技术支持等。

（3）针对行业监管部门提出的风险事项、薄弱环节，积极开展合规整改，采取有效措施减轻、消除危害影响。

征求意见稿

4 数据全生命周期保护

4.1 数据收集

4.1.1 涉及一般数据

（1）采取合法、正当的方式收集数据。

（2）数据收集过程中，可结合具体管理、业务场景，制定数据收集规则，规范数据收集渠道、数据格式、收集流程、收集方式和存储期限，采用人工核查或技术措施对外部数据的真实性、有效性、完整性和安全性进行鉴别，避免收集不明来源的数据。

（3）涉及收集个人信息的，应按照最小必要、公开透明原则，明确收集目的、使用方式、使用范围，并得到用户授权。

4.1.2 涉及重要数据和核心数据

在满足 4.1.1 的基础上，做好以下工作:

（1）采取技术监测、签署安全协议、账号权限管控、监督检查、安全审计等措施加强对重要数据和核心数据收集人员、设备系统的管理，并对收集来源、时间、类型、数量、频度、流向等进行记录。

（2）对数据收集所涉及的软硬件工具、设备、系统、平台、接口以及相关技术等，采取必要的测试、认证、鉴权等安全防护措施，防止针对数据采集环节的网络攻击。

（3）通过与数据提供方签署相关协议、承诺书等方式，

直接或间接获取重要数据和核心数据，明确双方法律责任。

（4）在发生产品或服务停止运营、用户终止服务等情况时，立即停止对相关数据的采集。涉及个人信息的，可采取用户协议或隐私政策文件等明确方便快捷的注销流程，并按照用户协议或隐私政策文件规定对收集数据进行销毁处理。

4.2 数据存储

4.2.1 涉及一般数据

（1）制定数据存储安全策略和操作规程，对存储数据的访问操作进行身份鉴别和访问控制。

（2）采用物理安全措施保障存储载体的设备数据访问或调试接口不暴露，避免存储数据被泄露、篡改或破坏。

（3）依据企业业务需要制定数据备份策略，按需要定期开展数据备份。

4.2.2 涉及重要数据和核心数据

在满足 4.2.1 的基础上，做好以下工作:

（1）制定重要数据和核心数据存储管理要求和操作、审批流程，明确相关数据存储系统或载体管理要求、访问控制、存储周期、日志留存、销毁流程、保障措施等要求。涉及容灾备份的，可参考“3.6 容灾备份”相关要求。

（2）对存储重要数据和核心数据的数据载体，采用对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、

基于公钥密码算法的数字签名机制和对称密码算法的加解密机制等商用密码技术进行安全存储，防止重要数据和核心数据被非授权篡改和非法窃取。直接提供存储服务的系统或平台不宜直接通过公共信息网络访问。

（3）对重要数据和核心数据存储载体进行安全管理，确保存放在安全环境中，并实行存储环境专人管理，对载体进行分类和标识管理，并建立数据存储载体管理台账，记录载体名称，所涉数据数量、类别级别，存放地点，使用、维护、标记和销毁等情况和相应审批记录，并定期盘点。

（4）对备份数据定期开展数据恢复测试，并实施不低于源数据的防护要求。

4.3 数据使用加工

4.3.1 涉及一般数据

（1）数据使用加工应遵循合理必要原则，制定数据使用加工管理要求、安全策略和操作规程，包括数据使用加工审批流程、结果发布、安全保护规则等。

（2）制定自动化决策安全策略，使用数据挖掘、关联分析等技术手段对特定主体进行精准画像、数据复原等加工处理活动前，需经过审批或征求用户个人同意。

（3）利用数据进行自动化决策的，保证决策的透明度和结果公平合理。

4.3.2 涉及重要数据和核心数据

在满足 4.3.1 的基础上，做好以下工作:

（1）加强访问控制，对重要数据和核心数据的使用加工进行授权和验证，并遵循最小化访问原则。

（2）严格管理原始数据使用加工过程中的数据获取方式，采用多级审批、权限管理、访问控制、数据加密、脱敏、接口鉴权等措施，避免涉及重要数据和核心数据的原始数据发生超权限、超范围使用加工的情况，并定期检查数据操作行为。

（3）在不影响数据使用加工的情况下，对重要数据和核心数据脱敏后再进行处理。明确数据脱敏规则、方法、流程等，并建立数据脱敏处理技术应用安全评估机制。未脱敏的数据原则上不得用于业务系统的开发测试。

（4）对测试过程中产生的过程性数据进行加强防护。

4.4 数据传输

4.4.1 涉及一般数据

（1）根据业务流程、职责内容、网络部署、安全风险等情况，合理划分企业网络系统安全域，区分域内、域间等不同数据传输场景，并且根据传输的数据类型、级别和应用场景，制定安全策略、采取保护措施，建立安全传输信道。

（2）可建立数据传输接口安全管理工作规范，明确技术管控措施，具备系统间接口和设备的认证鉴权能力，未通过认证鉴权的设备禁止接入。

4.4.2 涉及重要数据和核心数据

在满足 4.4.1 的基础上，做好以下工作:

（1）传输重要数据和核心数据时，采用对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制、对称密码算法的加解密机制和公钥算法数字信封等商用密码技术进行传输机密性和完整性保护，保证重要数据和核心数据的传输安全。

（2）对跨组织机构或使用互联网进行的数据传输事项进行前置审批，安全边界配备数据访问控制、身份认证等保障措施。根据传输的数据级别，明确相匹配的数据传输加密要求（数据加密、数据签名、散列等）。

（3）对传输接口管理和技术管控措施部署情况进行梳理，形成接口梳理情况清单并动态进行更新。清单包括：存在数据传输接口的业务系统、对端单位、对端系统、实现方式、接口类型（如实时调用接口、文件传输接口等）、对外接口传输数据种类以及目前使用的安全防护措施(如访问控制、加密、数据脱敏、日志审计等)，对照清单及时监控发现低活跃接口或废置接口，并采取相应处理措施。对涉及传输重要数据、核心数据等接口，实施数据加密、双重鉴权验证等更为严格的保障措施,包括流量监控、调用过载保护等,定期对接口权限控制、传输等相关功能进行安全评估，核实安全措施的有效性。

4.5 数据提供

4.5.1 涉及一般数据

（1）明确数据提供的范围、数量、条件、程序、时间，制定数据提供基本安全策略，确认没有超出需求和授权范围的数据。

（2）针对跨网、跨安全域的数据提供，建立安全操作规范，保障数据提供安全。

4.5.2 涉及重要数据和核心数据

在满足 4.5.1 的基础上，做好以下工作：

（1）在数据提供过程中采取必要保护措施，包括数据加密、数据水印、数据脱敏等。

（2）对数据提供行为进行监控，确保数据合理规范提供，未超出授权范围。

（3）数据接入互联网等活动中，开展数据安全风险监测，对安全风险高的网络出口和资产，加强网络边界的身份认证和访问控制。

4.6 数据公开

4.6.1 涉及一般数据

（1）根据数据公开场景，建立相应的安全策略和操作规程，明确可能对国家安全、公共利益产生影响的数据不得公开。

（2）建立数据公开审批流程，明确相关数据公开审批

征求意见稿

内容、留存记录等要求，不得超出业务场景需求和授权范围公开数据。在数据公开前由具体公开部门组织开展风险评估，研判可能存在的安全风险。

4.6.2 涉及重要数据和核心数据

在满足 4.6.1 的基础上，做好以下工作:

（1）根据数据特点、应用场景等，明确数据公开范围、内容、控制机制等数据公开安全策略和操作规程，并配备必要的数据脱敏、数据水印等技术，确保重要数据公开安全。

（2）对公开数据进行跟踪、记录，一旦发生相关数据安全事件或存在数据安全风险时，第一时间进行删除，并采取相关有效措施消除危害影响。

4.7 数据销毁

4.7.1 涉及一般数据

（1）建立数据销毁操作规程，明确销毁对象、规则、流程技术等要求。

（2）应对数据销毁过程及销毁后所涉及的资源回收情况（账号、物理资源、云资源、系统存储空间、数据共享途径等）进行记录。

4.7.2 涉及重要数据和核心数据

在满足 4.7.1 的基础上，做好以下工作:

（1）建立数据销毁操作审批机制，采用多人操作模式，并设置相关监督角色，负责监督销毁操作过程，确保数据销

毁流程合规。

（2）使用物理销毁等方法，确保重要数据和核心数据销毁后，无法恢复。

（3）引起备案内容发生变化的，履行备案变更手续。

4.8 数据委托处理

4.8.1 涉及一般数据

明确数据委托处理范围、所涉数据类别级别、条件、程序等，并明确委托方与受托方的数据安全责任和义务。

4.8.2 涉及重要数据和核心数据

在满足 4.8.1 的基础上，做好以下工作:

委托处理重要数据和核心数据的，对受托方的数据安全保护能力、资质进行评估或核实，与受托方通过合同、协议等形式明确双方的数据安全防护责任和义务。

4.9 数据转移

4.9.1 涉及一般数据

（1）发生兼并、重组、破产情形，涉及数据所属主体变更需要转移数据时，制定数据转移方案。

（2）数据转移方案内容包括转移数据基本情况（如数据类别、级别、规模、原数据所属方、数据接收方等）、数据转移风险评估（如必要性、合规性、转移影响等）、数据转移保护措施、应急响应措施等。

（3）转移数据涉及个人信息的，事先向用户告知转移保护措施、转移影响、数据接收方基本情况等，征得用户授权同意，经过处理无法识别特定个人且不能复原的除外。

4.9.2 涉及重要数据和核心数据

在满足 4.9.1 的基础上，做好以下工作:

转移重要、核心数据引起备案内容发生变化的，履行备案变更手续。

征求意见稿

5 数据安全风险监测预警、报告、处置

5.1 数据安全风险监测

5.1.1 涉及一般数据

（1）通过部署监测审计、态势感知等相关系统设备，建立数据安全风险监测预警技术能力，及时监测日常数据处理活动中的安全风险，如导入导出严重异常、违规向第三方传输、非必要端口开放、数据泄露、流量异常等。

（2）密切关注工业和信息化领域数据安全风险信息报送与共享平台通报的，以及国内外权威漏洞库及相关厂商发布的漏洞预警通知，定期开展漏洞排查与扫描检测，留存相关记录。

（3）可根据相关预警信息设置差异化告警级别，匹配对应的告警提醒方式（短信提醒、电话提醒、系统提醒等），并发送提醒相关责任人，如系统管理员、安全审计员等。

5.1.2 涉及重要数据和核心数据

在满足 5.1.1 的基础上，做好以下工作:

（1）建设数据风险监测预警能力，确保相关能力覆盖涉及操作处理重要数据和核心数据的系统，对重要数据的收集、存储、使用加工、传输、提供、公开、销毁、委托处理、转移等各生命周期环节中的合规性与执行上的一致性进行监测，并能够在发现异常行为时告警。异常行为包括重要、核心数据的违规操作，如未授权、超权限操作、批量操作、

陌生 IP 地址访问、数据库异常连接（如在设定时间内，某 IP 地址与实时数据库无任何数据交互或异常交互）等。

（2）实现核心数据处理活动的实时监控，发现异常时及时终止异常行为，并实现异常行为的可溯源。

5.2 数据安全风险信息报告

（1）对发现的数据安全风险进行研判，分析发生数据安全事件的可能性及其可能造成的影响。研判维度可从对国家安全、企业网络设备和信息系统、生产运营、经济运行等造成的影响范围和危害程度等方面考虑，具体详见《工业和信息化领域数据安全事件应急预案（试行）》。

（2）将可能造成重大及以上安全事件的风险及时向所在地行业监管部门报告。

（3）报告内容包括风险的类别、级别、涉及数据情况、产生时间、影响范围等。

5.3 数据安全风险处置

（1）当发现数据安全缺陷、漏洞等风险时，及时排查安全隐患，采取相应的处置和惩戒措施，并对存在风险隐患的环节进行加固防护。

（2）被所在地行业监管部门通知存在数据安全风险时，及时处置风险，并向所在地行业监管部门报告处置结果。处置结果内容包括风险接收情况、风险处置情况、下一步工作考虑等。

6 数据安全事件应急处置

6.1 制定应急预案

（1）根据应对数据安全事件的需要，制定本单位数据安全应急预案。

（2）应急预案内容主要包括：按照危害程度、影响范围等因素对数据安全事件进行分级，并结合分级情况，确定不同数据安全事件针对性的应急处置的方针策略、人员职责、具体措施、流程规范、物资保障等内容。

6.2 开展应急演练

（1）积极参与行业监管部门的应急演练。

（2）积极开展本单位数据安全事件应急演练，提高数据安全事件应对能力。

6.3 数据安全事件报告

（1）发现数据安全事件，立即先行判断，对后果影响自判为重大及以上或者涉及重要数据和核心数据的，立即如实向所在地行业监管部门报告。

（2）报告内容包括上报单位情况、事件基本情况、事件涉及数据情况、事件影响情况、事件处置建议等，详见《工业和信息化领域数据安全应急预案（试行）》。

6.4 应急响应

（1）当收到红色预警（特别重大事件）时，应启动I级响应。立即进入紧急状态，数据安全第一责任人牵头组建

事件应对专班，组织研究应对措施，统筹开展应急处置工作。数据安全直接责任人对应急处置工作进行具体部署，组织专班加强值班值守，相关人员保持联络畅通；持续加强监测分析，跟踪事态发展，评估影响范围和事件原因，采用有效整改处置措施，及时汇报工作进展和处置情况。

（2）当收到橙色预警（重大事件）时，应启动 II 级响应。立即启动相应数据安全事件应急预案，进入紧急状态，数据安全直接责任人牵头研究应对措施，统筹部署开展应急处置工作，相关人员保持联络畅通；持续加强监测分析，跟踪事态发展，评估影响范围和事件原因，采取有效整改处置措施，并及时汇报工作进展和处置情况。

（3）当收到黄色预警（较大事件）时，应启动 III 级响应。持续开展监测分析，根据事态发展，评估影响范围和事件原因；加强相关业务系统应用安全加固措施，提升数据安全防护能力，及时采取整改处置措施，并及时汇报工作进展和处置情况。

（4）当收到蓝色预警（一般事件）时，应启动 IV 级响应。按照行业数据安全保护相关政策标准及时采取整改处置措施，加强数据安全防护。

6.5 先行处置

发生数据安全事件或被所在地行业监管部门通知存在数据安全事件时，立即启动应急响应工作，组织本单位应急

队伍和工作人员采取应急处置措施，开展数据恢复或追溯工作，尽可能减少对用户和社会影响，同时保存相关痕迹和证据。

6.6 总结上报

（1）重大及以上数据安全事件应急工作结束后，涉事数据处理者应当及时对事件的起因、经过、责任、评估事件造成的影响和损失进行调查，总结事件防范和应急处置工作的经验教训，提出处理意见和改进措施，并在应急工作结束后 5 个工作日内形成总结报告，报所在地行业监管部门。

（2）报告总结内容包括事件起因、经过、责任、评估事件造成的影响和损失，总结事件防范和应急处置工作的经验教训，提出处理意见和改进措施。

6.7 数据安全事件告知

（1）数据安全事件对个人、组织造成实质性危害的，及时以电话、短信、邮件等方式向所涉主体告知安全事件情况、危害后果、已采取的补救措施等内容。

（2）无法逐一告知的，可采取公告方式告知。

7 数据安全风险评估

7.1 组建评估团队

（1）开展自评估

● 在开展风险评估工作前，综合考虑组织规模、业务种类、数据数量、种类、涉及数据载体的复杂程度等因素，组建至少包括组织管理、业务运营、技术保障、安全合规等人员组成的评估团队。

● 评估团队原则上具备不少于5名专业评估人员，包括1名评估团队组长、4名评估团队成员，其中至少4人熟悉数据安全风险评估的方法和流程，掌握依据数据安全风险评估相关标准规范开展风险评估的能力，并取得工业和信息化领域数据安全风险评估相关技能评价证书。

● 评估团队组长负责统筹安排评估工作并推进评估工作开展，组织完成评估结论、编写评估报告等。

● 组建评估团队时，还可聘请相关专业技术专家和技术负责人参与、指导。

（2）委托第三方评估机构开展评估

● 与被委托机构沟通，签订书面评估委托协议或评估合同，规范开展评估工作，保障数据处理者的安全生产运行和数据安全。

● 与被委托机构共同组建评估团队，确定评估团队组长和团队成员。

- 指定本单位至少 1 名数据安全专业人员为评估工作对接人，负责协调本单位相应资源、对第三方评估机构相应工作进行管理和监督。

7.2 确定评估范围

（1）评估团队首先对本单位基本情况进行充分调研，掌握数据种类、范围、处理方式以及相关数据载体的基本情况，确定评估范围。

（2）数据安全风险评估范围覆盖本单位全部重要数据和核心数据，以及一定比例的一般数据。一般数据以抽样方式选取，尽量保证评估数据范围覆盖全部数据类别（二级子类），且数据载体避免重复。

7.3 制定评估方案

（1）评估团队可根据实际需要制定风险评估工作方案。

（2）工作方案制定过程中，需与涉及数据处理活动的业务部门积极沟通，保障评估的可行性。

（3）评估方案包括评估范围、评估依据、评估团队基本信息、工作计划、使用的评估工具情况、保障条件等。

7.4 实施风险评估

（1）评估团队首先进行数据处理活动分析，明确评估范围内数据处理活动及所对应的数据名称、类别、级别、规模，处理数据的目的和方式、使用范围、涉及的接收方及数据载体情况等。

（2）开展合规性评估，包括正当必要性评估、基础性安全评估和数据全生命周期安全评估，研判合规性评估结果，详见《工业领域数据安全风险评估规范》《电信领域数据安全风险评估规范》。

（3）开展安全风险分析，通过风险源识别判断安全事件发生的可能性级别，结合安全影响分析结果，研判数据处理活动安全风险等级（分为极高、高、中、低四个等级）。合规性评估不通过的，可以直接判定安全风险分析中的风险源识别环节结果（可能性级别）为高。

（4）形成评估结论。

（5）依据评估结论开展风险整改与复核，对评估或自查中发现的安全风险或问题进行整改或改进，并对整改措施的有效性进行复核。

7.5 形成评估报告

（1）完成实施风险评估后，经协商一致，根据评估结论形成评估报告。

（2）评估报告包含数据处理者基本情况、评估团队基本情况、数据处理活动分析、合规性评估、安全风险分析、评估结论及应对措施等。

7.6 评估时间及上报行业监管部门

（1）工业和信息化领域重要数据和核心数据处理者每年自行或委托具有工业和信息化数据安全风险评估资质的

征求意见稿

第三方评估机构开展至少一次数据安全风险评估，形成数据安全风险评估报告。一般数据处理者可定期开展数据安全风险评估。重要数据和核心数据发生重大变更时，可及时开展数据安全风险评估。

（2）工业和信息化领域重要数据和核心数据处理者于每年 12 月底前向本地区行业监管部门报送加盖本单位或第三方评估机构公章的风险评估报告。

7.7 风险评估特殊场景

（1）涉及跨主体提供、转移、委托处理核心数据情形的，纳入风险评估范围。开展数据安全风险评估过程中，涉及在数据安全风险评估结果有效期内新增跨主体提供、委托处理、转移核心数据的，及时对发生变化及其影响的部分开展风险评估。

（2）涉及新上线业务、第三方数据合作业务以及重点存量业务的，数据处理者可以开展风险评估。

征求意见稿

8 数据出境

8.1 数据安全出境评估

根据法律法规要求，对需申报数据出境安全评估的情形应按要求开展数据出境风险评估，并向国家网信部门申报数据出境安全评估，在获得批准后方可开展数据出境活动。

8.1.1 申报数据安全出境评估的情形

（1）关键信息基础设施运营者向境外提供个人信息或者重要数据。

（2）关键信息基础设施运营者以外的数据处理者向境外提供重要数据。

（3）关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供100万人以上[2]个人信息（不含敏感个人信息）。

（4）关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供1万人以上敏感个人信息。

（5）国家网信部门规定的其他需要申报数据出境安全评估的情形。

8.1.2 申报数据安全出境评估的流程

（1）重要数据识别报备

按照本指引“2 数据分类分级”相关要求，识别、申报重要数据，准确界定需要出境的重要数据范畴。

[2] 本指引所指“以上”均含本数。

（2）事前评估

向境外提供数据前，首先开展数据出境风险自评估，并形成数据出境自评估报告。重点评估以下事项:

● 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。

● 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。

● 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。

● 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、非法利用等风险，个人信息权益维护的渠道是否通畅等。

● 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。

● 其他可能影响数据出境安全的事项。

（3）申报评估

● 根据《数据出境安全评估申报指南（第二版）》，确定数据评估申报形式。关键信息基础设施运营者以外的数据处理者申报数据出境安全评估一般适用线上申报，关键信息基础设施运营者或者其他不适合通过线上系统申报数据

出境安全评估的，采取线下申报流程。

● 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。申报数据出境安全评估，提交以下材料：申报书、数据出境风险自评估报告、与境外接收方拟订立的法律文件、安全评估工作需要的其他材料。

● 因申报材料不齐全被退回的，进行补充、更正申报材料。

（4）重新评估

通过数据出境安全评估的结果有效期为3年，自评估结果出具之日起计算。在有效期内出现以下情形之一的，重新申报评估。

● 向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或者延长个人信息和重要数据境外保存期限的。

● 境外接收方所在国家或者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、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的。

● 出现影响出境数据安全的其他情形重新申报数据出境安全评估。

（5）终止出境

● 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，在收到国家网信部门书面通知后，终止数据出境活动。

● 需要继续开展数据出境活动的，按照要求整改，整改完成后重新申报评估。

8.1.3 需要明确的数据安全保护责任义务

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:

（1）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。

（2）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。

（3）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。

（4）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，采取的安全措施。

（5）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。

（6）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。

8.1.4 通过数据出境安全评估的结果有效期

（1）通过数据出境安全评估的有效期届满，需要继续开展数据出境活动且未发生需要重新申报数据出境安全评估情形的，在有效期届满前60个工作日内通过所在地省级网信部门向国家网信部门提出延长评估结果有效期申请。

（2）经国家网信部门批准，可以延长评估结果有效期3年。

8.2 订立个人信息出境标准合同

8.2.1 订立个人信息出境标准合同的情形

（1）关键信息基础设施运营者以外的数据处理者自当年1月1日起，累计向境外提供10万人以上、不满100万人个人信息（不含敏感个人信息）的;

（2）关键信息基础设施运营者以外的数据处理者自当年1月1日起,累计向境外提供不满1万人敏感个人信息的。

8.2.2 订立个人信息出境标准合同的流程

（1）开展个人信息保护影响评估并订立合同

进行个人信息出境标准合同备案前,需要开展个人信息保护影响评估。同时，按照《个人信息出境标准合同办法》结合企业自身个人信息出境情况补充双方其他约定。

（2）材料提交

在标准合同生效之日起10个工作日内，通过数据出境申报系统开展个人信息出境标准合同备案。

（3）材料查验及反馈备案结果

收到省级网信办发放的备案编号后，根据需要在10个工作日内提交补充完善材料。逾期视为终止本次备案程序。

8.3 通过个人信息保护认证

8.3.1 通过个人信息保护认证的情形

（1）关键信息基础设施运营者以外的数据处理者自当年1月1日起，累计向境外提供10万人以上、不满100万人个人信息（不含敏感个人信息）的；

（2）关键信息基础设施运营者以外的数据处理者自当年1月1日起，累计向境外提供不满1万人敏感个人信息的。

8.3.2 通过个人信息保护认证的流程

（1）提交认证委托资料

按有关认证机构的要求如实提交认证委托资料，包括认证委托人基本材料、认证委托书、相关证明文档等。

（2）结果反馈

不符合认证要求的，按照认证机构的要求有权进行限期整改；符合认证要求的，将获得认证证书。

8.4 个人信息出境的注意事项

8.4.1 个人信息出境场景下的告知同意要求

向境外提供个人信息前，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《个人信息保护法》规定的各

征求意见稿

项权利的方式和程序等事项，并取得个人的单独同意。

8.4.2 个人信息出境场景下的个人信息保护影响评估

向境外提供个人信息的前，通过以下内容进行个人信息保护影响评估，并对处理情况进行记录。

（1）个人信息的处理目的、处理方式等是否合法、正当、必要;

（2）对个人权益的影响及安全风险;

（3）所采取的保护措施是否合法、有效并与风险程度相适应个人信息保护影响评估报告和处理情况记录至少保存 3 年。

8.5 数据出境的豁免情形

存在下列情形的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证:

（1）在国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集和产生的数据向境外提供，不包含个人信息或者重要数据的;

（2）为订立、履行个人作为一方当事人的合同，如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等，确需向境外提供个人信息的;

（3）按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息

的；

（4）紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的；

（5）关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供不满[3]10万人个人信息（不含敏感个人信息）的。

8.6 遵守出口管制要求的合规义务

（1）向境外提供涉及出口管制的数据的，需事前依法向有关部门申请出口许可证。

（2）可能危害国家安全和利益的，不向境外提供。

8.7 其他合规义务

非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

征求意见稿

[3] 本指引所称“不满”，均不包含本数。

9 数据交易

从事数据交易中介服务的机构按照数据来源可确认、使用范围可界定、交易过程可追溯、安全风险可防范的基本原则提供交易服务，并根据所负责具体交易环节制定平台准入、数据质量评估、交易管理、合规审查、信息披露、自律监管等规则，保障数据交易有效管理。

数据交易中介服务机构提供交易服务过程中开展合法性与合规性评估，并履行以下义务:

（1）要求数据提供方说明数据来源，并审核相关信息;

（2）审核数据交易双方身份和数据交易合同;

（3）留存相关审核、交易记录;

（4）监督数据交易、结算和交付;

（5）采取必要技术手段确保数据交易安全，保护个人信息、个人隐私、商业秘密、保密商务信息和重要数据;

（6）法律、法规规定的其他义务。

附件：数据资产清单

征求意见稿

附件

数据资产清单

序号	基本情况							监管要求	重要性描述			产生、使用与保护					所属部门签字确认	备注
	部门	类	级别	数据规模（条数/GB）	处理方式	详细描述	存储位置	现有管理政策	影响	面临主要安全威胁	时效	来源	用途	共享情况	保护情况	出境情况		

征求意见稿