

循序渐进：工信部再次征求数据安全管理办法意见

作者：段志超 | 蔡克蒙¹

2022年2月10日，根据2021年9月30日公布的《工业和信息化领域数据安全管理办法（试行）》（征求意见稿）（“《管理办法》”）收到的公开意见，工业和信息化部（“工信部”）对该法规草案进行了修改完善，再次面向社会征求意见，反馈截止时间为2022年2月21日。

2021年以来，针对如何落实《中华人民共和国数据安全法》（“《数据安全法》”）以及《中华人民共和国个人信息保护法》（“《个人信息保护法》”），工信部和国家互联网信息办公室（“网信办”）分别出台了具体的实施细则，并侧重于不同领域。针对工业和信息化领域数据安全，工信部出台了上述《管理办法》，对接《数据安全法》等法律法规要求，在工业和信息化领域对国家数据安全管理制度进行细化，明确开展数据分类分级保护、重要数据管理等具体要求，构建工业和信息化领域数据安全监管体系²。针对网络数据³，网信办于2021年11月14日，公布了《网络数据安全条例（征求意见稿）》（“《网络数据条例》”）。该条例针对《数据安全法》和《个人信息保护法》中的相关制度设计了实施路径；针对上位法中的相关要求进行了细化和明确；并创设增加了一些新的要求，例如重要数据处理者备案要求和年度报告要求、数据出境安全管理义务、网络平台责任等。

目前《管理办法》和《网络数据条例》均处在编写阶段，两者作为数据安全领域的两大主要监管部门工信部和网信办分别出台的实施细则，虽然部分内容存在交叉，但同时也强调了与数据本身属性相关的监管内容，潜在地为工信部和网信办之间的监管范围和路径做出了区别。

修改后的《管理办法》条目由原先的八章四十四条缩减为八章四十一条。

《管理办法》主要修改内容有：

- 强调个人信息单独保护：新增《个人信息保护法》作为目的依据。
- 扩充数据定义：将无线电数据纳入适用范围。
- 明晰监管机构职权范围：明确工信部对地方监管部门的督促指导作用。

¹ 实习生赵怡冰对本文的写作亦有贡献。

² 参见《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》起草说明，访问地址：https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20219/1d1668e46e644b42b04a95db43854607.pdf。

³ “网络数据”指任何以电子方式对信息的记录，英文翻译为“cyber data”，不限于利用“网络”（internet 或 network）产生或在其中处理的数据。访问地址：https://mp.weixin.qq.com/s/3uewzfnMEP_2Rr9SpaULnw。

- 修改分级分类标准：判定标准和细分标准发生变化。
- 明确备案机制：补充备案申请、审批、变更相关要求。
- 严格主体责任：法定代表人负责制，加强内部管理。
- 更新全生命周期合规要求：取消核心数据不得出境，新增核心数据跨主体处理要求。
- 统筹协调数据安全审查：灵活化安全评估、监督协助等要求。

我们将在下文对比《管理办法》（0930版）和《管理办法》（0210版），梳理此次修订的重要内容，并同时提出我们的解读。

一、强调个人信息单独保护：新增《个人信息保护法》作为依据

在《管理办法》（0930版）的起草说明中曾强调《管理办法》秉承《数据安全法》将个人信息纳入重要数据目录和核心数据目录进行重点保护的工作理念，将个人信息纳入数据全生命周期安全管理，不再单独提出个人信息保护的要求⁴。因此《管理办法》（0930版）将《网络安全法》、《数据安全法》作为上位法基础，但并未提及《个人信息保护法》。但在此次最新发布的《管理办法》（0210版）中，新增了《中华人民共和国个人信息保护法》作为目的依据，并且在具体条款中也调整了关于个人信息的规定，例如：

- 在第八条【分级分类方法】的数据分类类别列举中，删除了“个人信息”的表述，保留了原先的管理数据、运维数据、研发数据等非个人信息；
- 在第八章附则中新增第三十七条【个人信息保护】，“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。”

综上所述，《管理办法》（0210版）调整了对于个人信息的规制思路，由原先的“纳入重要数据目录和核心数据目录统一管理”到强调个人信息的单独保护。此变化是为了与此前发布的相关法律文件形成统一。在《管理办法》（0930版）发布后，2021年11月14日《网络数据条例》公开向社会征求意见，其中明确了重要数据和核心数据的定义，并不包含个人信息。此外，无论是2021年9月23日全国信息安全标准化技术委员会秘书处发布的国家标准《信息安全技术 重要数据识别指南》征求意见稿（“《指南》”）第一版，还是2022年1月13日发布的《指南》修订版，其中重要数据的定义中，均明确说明“重要数据不包括国家秘密和个人信息，但基于海量个人信息形成的统计数据、衍生数据有可能属于重要数据。”为实现法律规定的统一协调，此次《管理办法》（0210版）中改变了对于个人信息管理的思路，强调《个人信息保护法》作为个人信息保护基础性法律的作用。

二、扩充数据定义：将无线电数据纳入适用范围

《管理办法》（0210版）在第三条数据定义中修改了如下表述：

- 明晰了工业和信息化领域数据包括三类：即工业数据、电信数据和无线电数据。
- 删除行业领域的具体列举：在《管理办法》（0930版）中，对工业和信息化领域进行了列举，如“原材料工业、装备工业、消费品工业、电子信息制造业、软件和信息技术服务业、民爆等行业领域”。

⁴ 参见《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》起草说明，访问地址：https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20219/1d1668e46e644b42b04a95db43854607.pdf。

但是在《管理办法》（0210版）中，删除了列举表述，而是用“工业和信息化领域”作为统称，此修改更有抽象概括性，避免了无法穷尽列举和实践变化导致的法律不兼容问题。

- 新增无线电数据的定义：即“无线电数据是指在开展无线电业务活动中产生和收集的无线电频率、台（站）等电波参数数据”。《管理办法》（0210版）在定义条款中将无线电数据纳入适用范围的同时，还对应修改了配套制度，例如新增“无线电频率、台（站）使用单位”作为工业和信息化领域数据处理者；新增无线电管理机构作为监管机构之一；将电磁受影响纳入重要数据与核心数据判定标准。

三、明晰监管机构职权范围：明确工信部对地方监管部门的督促指导作用

《管理办法》（0210版）中对中央和地方主管部门的职权进行了进一步明晰：

- 中央层面：要求工信部的监督管理活动需要遵守国家数据安全工作协调机制统筹安排。此前提的补充是为了解决此前数据监管“九龙治水”的局面，强调数据安全工作的统筹协调。
- 地方层面：《管理办法》（0930版）中并未明晰层层监管的架构，尤其是中央层面对地方层面的监督。《管理办法》（0210版）进行了修改，明确了工信部负责督促指导各省、自治区、直辖市及计划单列市、新疆生产建设兵团的地方工业和信息化主管部门、地方通信管理局和地方无线电管理机构；由地方工业和信息化主管部门、地方通信管理局和地方无线电管理机构负责监督本地区的数据处理活动。
- 强调上述行业（领域）监管部门需依照有关法律、行政法规的规定，依法配合有关部门开展的数据安全监管相关工作。

四、修改分级分类标准：判定标准和细分标准发生变化

《管理办法》再次重申了《数据安全法》确立的数据分类分级管理要求，在《管理办法》（0210版）对分级分类工作要求、方法、一般数据、重要数据以及核心数据判断标准进行了修改调整。主要体现在以下方面：

- 工作要求：《管理办法》（0210版）中将【分级分类工作要求】提前到第七条；地方工业和信息化主管部门、通信管理局、无线电管理机构新增了重要数据和核心数据具体目录上报更新义务；删除了企业应当坚持先分类后分级的工作方法。
- 分级分类方法：补充新增工业和信息化领域数据处理者可在一般数据、重要数据和核心数据三级基础上细分数据的类别和级别。
- 判定标准：取消“恢复数据或消除负面影响所需付出的代价程度”作为一般数据或重要数据的判定标准；在核心数据判断标准中，新增无线电数据场景。

然而，此次修改并未对“重大影响”、“严重影响”、“重大损害”等判断因素进行量化，故企业如何在实践中落实重要数据和核心数据的分级分类工作仍有待主管部门提供更明确的指引。

五、明确备案机制：补充备案申请、审批、变更相关要求

《管理办法》（0210版）在《管理办法》（0930版）的基础上，针对重要数据和核心数据目录备案义务

进行了进一步细化和明晰，具体表现如下：

- **备案机构：**明确工业和信息化领域数据处理者应当将本单位重要数据和核心数据目录向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）备案。
- **备案内容：**调整了语言表述，对原先备案内容进行了更为严谨的整合；并明确备案内容不包括数据内容本身。
- **备案审核时间：**要求地方工信部门、通信管理局、无线电管理机构在工业和信息化领域数据处理者提交备案申请的二十个工作日内完成审核工作。
- **审核结果：**予以备案应发放备案凭证，同时将备案情况报工信部；不予备案的应当及时反馈备案申请人并说明理由。
- **备案变更要求：**重要数据和核心数据的类别或规模变化 30%以上的，或者其它备案内容发生重大变化，工业和信息化领域数据处理者应当在发生变化的三个月内履行备案变更手续。
- **更新备案要求：**销毁重要数据和核心数据需要向工信部门、通管局、无线电管理机构更新备案。

六、严格主体责任：法定代表人负责制，加强内部管理

《管理办法》(0930 版)中明确了企业落实数据安全义务的第一步将是建立健全数据安全组织架构，并进一步要求企业党委（党组）或领导班子对数据安全负主体责任、主要负责人是数据安全第一责任人、分管数据安全的负责人是数据安全直接责任人。而《管理办法》(0210 版)对原来的第十三条【主体责任】、第十四条【工作体系】、第十五条【关键岗位管理】和第十六条【数据收集】进行了整合，修改删减为第十三条【主体责任】。在内容上也进行相应调整：

- **确定法定代表人负责制：**将“本单位党委（党组）或领导班子对数据安全负主体责任”改为“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”。此调整更符合法律责任要求，党委或领导班子是行政上的设计，无法适用于所有的企业，但是法定代表人是公司法制度的核心设计，体现了责任的承担，更适合担任数据安全责任人。
- **严格内部管理制度：**针对重要数据和核心数据处理者，新增要求“建立内部登记、审批机制，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”。

对于可能处理重要数据、核心数据的企业，需要密切关注此项调整，进而重新设计内部组织架构，可能承担责任的法定代表人、主要负责人、直接责任人以及关键岗位人员需提高数据合规重视度，积极参与数据安全的各类培训，提升数据治理专业能力。

七、更新全生命周期合规要求：取消核心数据不得出境，新增核心数据跨主体处理要求

《管理办法》(0210 版)针对数据全生命周期的不同环节，再次更新了适用各级别数据的通用要求、以及处理重要数据与核心数据应遵守的额外要求。如下合规变化值得企业关注：

- **数据存储：**新增存储重要数据和核心数据的，需定期开展数据恢复测试。
- **数据使用加工：**删除“未经个人、单位等同意，不得使用数据挖掘、关联分析等技术手段针对特定主体进行精准画像、数据复原等加工处理活动”。

- 数据公开：删除“对涉及个人隐私、个人信息、商业秘密、保密商务信息不得公开”。
- 数据销毁：新增“销毁重要数据和核心数据的，应当及时向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）更新备案”。
- 数据出境：取消核心数据不得出境的要求，统一核心数据和重要数据出境监管要求，即确需向境外提供时，应当依法依规进行数据出境安全评估。
- 核心数据跨主体处理：新增第二十四条，要求跨主体提供、转移、委托处理核心数据的，应当评估安全风险，采取必要的安全保护措施，并经由地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报工信部。工信部按照有关规定进行审查。
- 用户权利响应：《管理办法》（0930 版）中第二十九条【举报投诉处理】中曾要求“工业和电信数据处理者应当建立用户投诉处理机制，公布电子邮件、电话、传真、在线客服等便捷有效的联系方式，配备受理用户投诉的人员接收数据安全相关投诉，并自接到投诉之日起 15 个工作日内答复投诉人”，此为强制性义务。但是在《管理办法》（0210 版）中删除了该表述，并改为了“鼓励工业和信息化领域数据处理者建立用户投诉处理机制”，减轻了数据处理者应对用户投诉的合规义务。

八、统筹协调数据安全审查：灵活化安全评估、监督协助等要求

根据此前的《管理办法》（0930 版），国家通过数据安全检测、评估、认证，以及监督检查、安全审查，落实数据安全监督管理。企业需要履行开展安全评估、协助监督检查以及通过数据安全审查的合规义务。此次，《管理办法》（0210 版）对第五章【数据安全监测、认证、评估管理】和第六章【监督检查】进行了灵活化调整，主要体现在以下方面：

- 放宽认证机构管理：此前《管理办法》（0930 版）第三十二条明确要求工业和信息化部 and 地方监管部门建立数据安全检测、评估与认证机构管理制度，制定机构认定标准，开展机构选拔认定、资质授权、日常管理和推荐目录发布等工作。但《管理办法》（0210 版）中删除了由监管部门开展机构选拔以及资质授权的要求，改为了“工业和信息化部鼓励、引导具备相应资质的机构，依据相关标准开展行业数据安全检测、认证工作”。
- 取消一般数据处理者的自评估要求：《管理办法》（0930 版）第三十三条鼓励一般数据处理者开展安全自评估，但是在《管理办法》（0210 版）中删除了该表述，仅强调重要数据和核心数据处理者应自行或委托第三方评估机构展开评估。
- 取消预留检查接口要求：《管理办法》（0930 版）第三十四条规定，企业有配合行业监管部门开展监督检查、并预留检查接口的义务。对于企业而言，主管部门可通过检查接口访问并审查的数据范围、接口的技术标准与调用条件，可能是企业最为关心的事项。但在《管理办法》（0210 版）中删除了预留检查接口这项要求，仅为笼统地要求企业配合监管部门检查。
- 统筹协调数据安全审查：《管理办法》（0930 版）第三十五条规定，工信部在国家数据安全工作协调机制指导下，对影响或可能影响国家安全的工业和电信数据处理活动开展数据安全审查。另一方面，2022 年 1 月 4 日，网信办、中国证券监督管理委员会等十三部委正式联合出台了修订后的《网络安全审查办法》，其中将数据处理活动纳入了审查范围，其中“核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险”是网络安全审查重点评估的因素。可见，若依据《管理办法》（0930 版）则数据处理者会同同时面对基于工信部《管理办法》与网信办《网

络安全审查办法》的双重审查。此次《管理办法》（0210版）中删除了“对影响或可能影响国家安全的工业和电信数据处理活动开展数据安全审查相关工作”的要求，仅强调工信部需在国家数据安全工作协调机制指导下开展数据安全审查工作，对未来工信部和网信办如何统筹协调数据安全审查保留了灵活性。

九、结语

本次《管理办法》（0210版）修改内容较多，除了以上重要实质合规义务的修改，在语言表述以及法律责任承担上也进行了调整（例如删除了将数据处理者的安全管理责任纳入信用管理和失信名单的要求）。此次调整体现了《管理办法》与相关法律法规的统筹协调，修正了相关概念表述，灵活调整了监管和合规思路。

《管理办法》作为工业和信息化领域数据安全管理的顶层设计，提出了多项新增和细化的合规要求，建议工业和信息化领域数据处理者密切关注。

《工业和信息化领域数据安全管理办法（试行）》（征求意见稿）修订对比

蓝色为删除部分，红色为增加内容

	工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）
第一章 总则	第一章 总则
第一条【目的依据】为了规范工业和信息化领域数据处理活动，加强数据安全，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家安全和利益，根据《中华人民共和国民法典》《中华人民共和国数据安全法》《中华人民共和国网络安全法》等法律法规，制定本办法。	第一条【目的依据】为了规范工业和信息化领域数据处理活动，加强数据安全，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家安全和利益，根据《 <u>中华人民共和国民法典</u> 》《中华人民共和国数据安全法》《中华人民共和国网络安全法》 <u>《中华人民共和国个人信息保护法》</u> 《中华人民共和国国家安全法》《 <u>中华人民共和国民法典</u> 》等法律法规，制定本办法。-
第二条【适用范围】在中华人民共和国境内开展的工业和电信数据处理活动及其安全监管，应当遵守相关法律、行政法规和本办法的要求。	第二条【适用范围】在中华人民共和国境内开展的工业和信息化领域数据处理活动及其安全监管，应当遵守相关法律、行政法规和本办法的要求。-
第三条【数据定义】工业数据是指原材料工业、装备工业、消费品工业、电子信息制造业、软件和信息技术服务业、民爆等行业领域，在研发设计、生产制造、经营管理、运维服务、平台运营、应用服务等过程中收集和产生的数据。 电信数据是指在电信业务经营活动中收集和产生的数据。 工业和电信数据处理者是指对工业、电信数据进行收集、存储、使用、加工、传输、提供、公开等数据处理活动的工业企业、软件和信息技术服务企业以及取得电信业务经营许可证的电信业务经营者等工业和信息化领域各类主体。	第三条【数据定义】 <u>工业数据是指原材料工业、装备工业、消费品工业、电子信息制造业、软件和信息技术服务业、民爆等行业领域，在研发设计工业和信息化领域数据包括工业数据、电信数据和无线电数据。</u> <u>工业数据是指工业各行业各领域</u> 在研发设计、生产制造、经营管理、运行维护、平台运营、 <u>应用服务</u> 等过程中产生和收集的数据。 电信数据是指在电信业务经营活动中 <u>产生和收集收集</u> 和产生的数据。 <u>无线电数据是指在开展无线电业务活动中产生和收集的无线电频率、台（站）等电波参数数据。</u> 工业和信息化领域数据处理者是指对 <u>工业和信息化领域数据</u> 进行收集、存储、使用、加工、传输、提供、公开等数据处理活动的工业企业、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 <u>和无线电频率、台（站）使用单位</u> 等工业和信息化领域各类主体。
第四条【监管机构】工业和信息化部负责对工业和电信数据处理者的数据处理活动和安全保护进行监督管理。各省、自治区、直辖市及计划单列市、新疆生产建设兵团工业和信息化主管部门（以下统称地方	第四条【监管机构】 <u>工业和信息化部负责对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。</u> <u>在国家数据安全工作协调机制统筹协调下，工业和信息化部负责督促指导</u> 各省、自治区、直辖

	<p style="text-align: center;">工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）</p>
<p>工业和信息化主管部门）负责对本地区工业数据处理者的数据处理活动和安全保护进行监督管理。各省、自治区、直辖市通信管理局（以下统称地方通信管理局）负责对本地区电信数据处理者的数据处理活动和安全保护进行监督管理。</p> <p>工业和信息化部及地方工业和信息化主管部门、通信管理局统称为行业监管部门。</p>	<p>市及计划单列市、新疆生产建设兵团工业和信息化主管部门（以下统称地方工业和信息化主管部门）<u>负责对本地区工业数据处理者的数据处理活动和安全保护进行监督管理。</u>各省、自治区、直辖市通信管理局（以下统称地方通信管理局）<u>负责对本地区电信数据处理者的数据处理活动和安全保护进行监督管理</u>和<u>各省、自治区、直辖市无线电管理机构（以下统称地方无线电管理机构）开展数据安全监管，对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。</u></p> <p>地方工业和信息化主管部门负责对本地区工业数据处理者的数据处理活动和安全保护进行监督管理。地方通信管理局负责对本地区电信数据处理者的数据处理活动和安全保护进行监督管理。<u>地方无线电管理机构负责对本地区无线电数据处理者的数据处理活动和安全保护进行监督管理。</u></p> <p>工业和信息化部及地方工业和信息化主管部门、通信管理局、<u>无线电管理机构统称为行业（领域）监管部门。</u></p> <p><u>行业（领域）监管部门依照有关法律、行政法规的规定，依法配合有关部门开展的数据安全监管相关工作。</u></p>
<p>第五条【产业发展】行业监管部门鼓励数据开发利用和数据安全技术研究，支持推广数据安全产品和服务，培育数据安全企业、研究和服务机构，壮大数据安全产业，提升数据安全保障能力，促进数据的创新应用。</p> <p>工业和电信数据处理器研发提供数据开发利用新技术、新产品、新服务，应当有利于促进经济社会和行业发展，符合社会公德和伦理。</p>	<p>第五条【产业发展】行业（<u>领域</u>）监管部门鼓励数据开发利用和数据安全技术研究，支持推广数据安全产品和服务，培育数据安全企业、研究和服务机构，<u>壮大发展</u>数据安全产业，提升数据安全保障能力，促进数据的创新应用。</p> <p>工业和信息化领域数据处理器<u>研究、开发、使用数据</u>新技术、新产品、新服务，应当有利于促进经济社会和行业发展，符合社会公德和伦理。</p>
<p>第六条【标准制定】行业监管部门推进工业和信息化领域数据开发利用和数据安全标准体系建设，组织开展行业标准制修订工作。鼓励支持企业、研究机构、高等院校、行业组织等不同主体，开展国际标准、国家标准、团体标准、企业标准制定。引导工业和电信数据处理器开展数据管理、数据安全贯标达标工作。</p>	<p>第六条【标准制定】行业（<u>领域</u>）监管部门推进工业和信息化领域数据开发利用和数据安全标准体系建设，组织开展行业相关标准制修订工作。鼓励支持企业、研究机构、高等院校、行业组织等不同主体，<u>合作</u>开展国际标准、国家标准、<u>行业标准、团体标准、企业标准</u>制定。引导<u>工业和信息化领域</u>数据处理器开展数据管理、数据安全贯标达标工作。</p>

	<p>工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）</p>
<p>第二章 数据分类分级管理</p>	<p>第二章 数据分类分级管理</p>
	<p>第十一条 第七条【分类分级工作要求】工业和信息化部组织制定工业和信息化领域数据分类分级、重要数据和核心数据识别认定、数据分级防护等<u>标准规范制度规范</u>，指导开展数据分类分级<u>防护管理工作</u>，<u>形成制定</u>行业重要数据和核心数据具体目录并实施动态管理。</p> <p>地方工业和信息化主管部门、通信管理局、<u>无线电管理机构</u>组织开展本地区<u>工业、电信行业工业和信息化领域</u>数据分类分级<u>防护管理</u>及重要数据和核心数据识别<u>认定</u>工作，<u>确定形成本地区行业（领域）重要数据和核心数据具体目录并上报工业和信息化部，目录发生变化的，应当及时上报更新。</u></p> <p><u>工业和电信数据处理者应当建立健全数据分类分级管理制度，将重要数据和核心数据目录报送地方工业和信息化主管部门或通信管理局，并采取措施开展数据分级防护，对重要数据进行重点保护，对核心数据在重要数据保护基础上实施更严格的管理和保护。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。</u></p> <p><u>工业和信息化领域数据处理者应当定期梳理数据，按照相关标准规范识别重要数据和核心数据并形成目录。</u></p>
<p>第七条【分类分级方法】工业和电信数据处理者应当坚持先分类后分级，定期梳理，根据行业要求、业务需求、数据来源和用途等因素对数据进行分类和标识，形成数据分类清单。数据分类类别包括但不限于研发数据、生产运行数据、管理数据、运维数据、业务服务数据、个人信息等。</p> <p>工业和信息化部按照国家有关规定，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，将工业和电信数据分为一般数据、重要数据和核心数据三级。</p>	<p>第七条 第八条【分类分级方法】<u>工业和电信数据处理者应当坚持先分类后分级</u>，根据行业要求、<u>特点、业务需求、数据来源和用途等因素，对数据进行分类和标识，形成数据分类清单。</u><u>工业和信息化领域数据分类类别包括但不限于</u>研发数据、生产运行数据、管理数据、运维数据、业务服务数据等。<u>个人信息等</u></p> <p><u>工业和信息化部按照国家有关规定</u>，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，<u>将工业和电信数据工业和信息化领域数据</u>分为一般数据、重要数据和核心数据三级。</p> <p><u>工业和信息化领域数据处理者可在此基础上细分数据的类别和级别。</u></p>

	<p>工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）</p>
<p>第八条【一般数据】危害程度符合下列条件之一的数据为一般数据：</p> <p>（一）对公共利益或者个人、组织合法权益造成较小影响，社会负面影响小；</p> <p>（二）受影响的用户和企业数量较少、生产生活区域范围较小、持续时间较短，对企业经营、行业发展、技术进步和产业生态等影响较小；</p> <p>（三）恢复数据或消除负面影响所需付出的代价小；</p> <p>（四）其他未纳入重要数据、核心数据目录的数据。</p>	<p>第八条<u>第九条</u>【一般数据】危害程度符合下列条件之一的数据为一般数据：</p> <p>（一）对公共利益或者个人、组织合法权益造成较小影响，社会负面影响小；</p> <p>（二）受影响的用户和企业数量较少、生产生活区域范围较小、持续时间较短，对企业经营、行业发展、技术进步和产业生态等影响较小；</p> <p>（三）恢复数据或消除负面影响所需付出的代价小；</p> <p>（四）其他未纳入重要数据、核心数据目录的数据。</p>
<p>第九条【重要数据】危害程度符合下列条件之一的数据为重要数据：</p> <p>（一）对政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核安全等构成威胁，影响海外利益、生物、太空、极地、深海、人工智能等重点领域国家安全相关数据的安全；</p> <p>（二）对工业、电信行业发展、生产、运行和经济利益等造成影响；</p> <p>（三）造成重大数据安全事件或生产安全事故，对公共利益或者个人、组织合法权益造成严重影响，社会负面影响大；</p> <p>（四）引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或者影响持续时间长，对行业发展、技术进步和产业生态等造成严重影响；</p> <p>（五）恢复数据或消除负面影响所需付出的代价大；</p> <p>（六）经行业监管部门评估确定的其他重要数据。</p>	<p>第九条<u>第十条</u>【重要数据】危害程度符合下列条件之一的数据为重要数据：</p> <p>（一）（一）对政治、国土、军事、经济、文化、社会、科技、<u>电磁</u>、网络、生态、资源、核安全等构成威胁，影响海外利益、生物、太空、极地、深海、人工智能等<u>重点领域国家安全相关数据的安全与国家安全相关的重点领域</u>；</p> <p>（二）对工业、电信行业发展<u>对工业和信息化领域发展</u>、生产、运行和经济利益等造成<u>严重</u>影响；</p> <p>（三）造成重大数据安全事件或生产安全事故，对公共利益或者个人、组织合法权益造成严重影响，社会负面影响大；</p> <p>（四）引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或者影响持续时间长，对行业发展、技术进步和产业生态等造成严重影响+；</p> <p>（五）恢复数据或消除负面影响所需付出的代价大； 经工业和信息化部评估确定的其他重要数据。</p>
<p>第十条【核心数据】危害程度符合下列条件之一的数据为核心数据：</p> <p>（一）对政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核安全等构成严重威胁，严重影响海外利益、生物、太空、极地、深海、人工智能等重点领域国家安全相关数据的安全；</p> <p>（二）对工业、电信行业及其重要骨干企业、关键信息基础设施、重要资源等造成严重影响；</p> <p>（三）对工业生产运营、电信和互联网运行和服务等</p>	<p>第十条<u>第十一条</u>【核心数据】危害程度符合下列条件之一的数据为核心数据：-</p> <p>（一）对政治、国土、军事、经济、文化、社会、科技、<u>电磁</u>、网络、生态、资源、核安全等构成严重威胁，严重影响海外利益、生物、太空、极地、深海、人工智能等<u>重点领域国家安全相关数据的安全与国家安全相关的重点领域</u>；</p> <p>（二）对工业、电信行业及其重要骨干企业<u>对工业和信息化领域及其重要骨干企业</u>、关键信息基础设施</p>

	<p style="text-align: center;">工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）</p>
<p>造成重大损害，导致大范围停工停产、大面积网络与服务瘫痪、大量业务处理能力丧失等；</p> <p>（四）经工业和信息化部评估确定的其他核心数据。</p>	<p>施、重要资源等造成严重重大影响；</p> <p>（三）对工业生产运营、<u>电信和互联网电信网络（含互联网）</u>运行和服务、<u>无线电业务开展</u>等造成重大损害，导致大范围停工停产、大面积<u>无线电业务中断、大规模</u>网络与服务瘫痪、大量业务处理能力丧失等； -</p> <p>（四）经工业和信息化部评估确定的其他核心数据。</p>
<p>第十一条【分类分级工作要求】工业和信息化部组织制定工业和信息化领域数据分类分级、重要数据和核心数据识别认定及数据分级防护等制度规范，形成行业重要数据和核心数据具体目录并实施动态管理，指导开展数据分类分级防护工作。</p> <p>地方工业和信息化主管部门、通信管理局组织开展本地区工业、电信行业数据分类分级防护及重要数据和核心数据识别认定工作，形成本地区行业重要数据和核心数据具体目录并上报工业和信息化部。</p> <p>工业和电信数据处理者应当建立健全数据分类分级管理制度，将重要数据和核心数据目录报送地方工业和信息化主管部门或通信管理局，并采取措施开展数据分级防护，对重要数据进行重点保护，对核心数据在重要数据保护基础上实施更严格的管理和保护。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。</p>	<p>第十一条第七条【分类分级工作要求】工业和信息化部组织制定工业和信息化领域数据分类分级、重要数据和核心数据识别认定、数据分级防护等标准规范制度规范，指导开展数据分类分级防护管理工作，形成制定行业重要数据和核心数据具体目录并实施动态管理。</p> <p>地方工业和信息化主管部门、通信管理局、<u>无线电管理机构</u>组织开展本地区<u>工业、电信行业工业和信息化领域</u>数据分类分级防护管理及重要数据和核心数据识别认定工作，<u>确定形成本地区行业（领域）</u>重要数据和核心数据具体目录并上报工业和信息化部，<u>目录发生变化的，应当及时上报更新。</u></p> <p><u>工业和电信数据处理者应当建立健全数据分类分级管理制度，将重要数据和核心数据目录报送地方工业和信息化主管部门或通信管理局，并采取措施开展数据分级防护，对重要数据进行重点保护，对核心数据在重要数据保护基础上实施更严格的管理和保护。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。</u></p> <p><u>工业和信息化领域数据处理者应当定期梳理数据，按照相关标准规范识别重要数据和核心数据并形成目录。</u></p>
<p>第十二条【重要数据和核心数据备案管理】工业和信息化部建立工业和信息化领域重要数据和核心数据备案管理制度，统筹建设备案管理平台。备案内容包括数据的数量、类别、处理目的和方式、使用范围、主体责任、安全保护措施等基本情况，数据提供、公开、出境、承接，以及数据安全风险、事件处置等情况。</p> <p>地方工业和信息化主管部门、通信管理局应当分别对本地区工业、电信行业重要数据和核心数据备案</p>	<p>第十二条【重要数据和核心数据目录备案管理】<u>工业和信息化部建立工业和信息化领域重要数据和核心数据备案管理制度，统筹建设备案管理平台。</u><u>工业和信息化领域数据处理者应当将本单位重要数据和核心数据目录向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）备案。</u>备案内容包括但不限于数据的数量、类别、级别、规模、处理目的和方式、使用范围、主体责任<u>责任主体、对外共享、跨境传</u></p>

	<p>工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）</p>
<p>内容进行审核，对不符合有关备案要求的，应当督促企业及时完善并重新进行备案。</p> <p>工业和电信数据处理器应当按照有关要求进行备案，备案内容发生变化的，应在三个月内报备变更情况，同时对整体备案情况进行更新。</p>	<p>输、安全保护措施等基本情况，数据提供、公开、出境、承接，以及数据安全风险、事件处置等情况不包括数据内容本身。</p> <p>地方工业和信息化主管部门（<u>工业领域</u>）或通信管理局（<u>电信领域</u>）或<u>无线电管理机构</u>（<u>无线电领域</u>）应当分别对本地区工业、电信行业重要数据和核心数据备案内容进行审核，对不符合有关备案要求的，应当督促企业及时完善并重新进行备案。<u>应当在工业和信息化领域数据处理器提交备案申请的二十个工作日内完成审核工作，备案内容符合要求的，予以备案并发放备案凭证，同时将备案情况报工业和信息化部；不予备案的应当及时反馈备案申请人并说明理由。</u></p> <p><u>重要数据和核心数据的类别或规模变化 30%以上的，或者其它备案内容发生重大变化的，</u>工业和信息化领域数据处理器应当在发生变化的三个月内报备变更情况，同时对整体备案情况进行更新。<u>履行备案变更手续。</u></p>
<p>第三章 数据全生命周期安全管理</p>	<p>第三章 数据全生命周期安全管理-</p>
<p>第十三条【主体责任】工业和电信数据处理器应当对数据处理活动负安全主体责任，根据数据的类型、数量、安全级别、处理方式以及对国家安全、公共利益或者个人、组织合法权益带来的影响和安全风险等，采取必要措施确保数据持续处于有效保护和合法利用的状态。</p> <p>（一）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、公开等环节的具体分级防护要求和操作规程；</p> <p>（二）明确数据安全的主要负责人和责任部门，统筹负责数据处理活动的安全监督管理；</p> <p>（三）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；</p> <p>（四）制定数据安全事件应急预案，并定期进行演练；</p> <p>（五）定期对从业人员开展数据安全教育和培训；</p> <p>（六）法律、行政法规规定的其他措施。</p>	<p>第十三条【主体责任】工业和电信<u>工业和信息化领域</u>数据处理器应当对数据处理活动负安全主体责任，根据数据的类型、数量、安全级别、处理方式以及对国家安全、公共利益或者个人、组织合法权益带来的影响和安全风险等<u>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，采取必要措施</u>确保数据持续处于有效保护和合法利用的状态。</p> <p>（一）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、公开等环节的具体分级防护要求和操作规程；</p> <p>（二）<u>明确数据安全的主要负责人和责任部门</u>根据需要配备数据安全管理人员，统筹负责数据处理活动的安全监督管理，<u>协助行业（领域）监管部门开展工作</u>；</p> <p>（三）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；-</p>

	<p>工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）</p>
	<p>（四）<u>根据应对数据安全事件的需要，制定数据安全事件应急预案</u>，并定期进行演练；</p> <p>（五）定期对从业人员开展数据安全教育和培训；</p> <p>（六）法律、行政法规<u>等</u>规定的其他措施。</p> <p><u>工业和信息化领域重要数据和核心数据处理者，还应当：</u></p> <p>（一）建立覆盖本单位相关部门的数据安全工作体系，<u>明确数据安全负责人和管理机构</u>，建立常态化沟通与协作机制。<u>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；</u></p> <p>（二）<u>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；</u></p> <p>（三）<u>建立内部登记、审批机制，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。</u></p>
<p>第十四条【工作体系】涉及重要数据和核心数据的，工业和电信数据处理者应当建立覆盖本单位相关部门的数据安全工作体系，设置专门的数据安全管理责任部门，本单位党委（党组）或领导班子对数据安全负主体责任，主要负责人是数据安全第一责任人，分管数据安全的负责人是直接责任人，明确各部门数据安全职责及人员，建立常态化沟通与协作机制。</p>	<p>第十四条【工作体系】涉及重要数据和核心数据的，工业和电信数据处理者应当建立覆盖本单位相关部门的数据安全工作体系，设置专门的数据安全管理责任部门，本单位党委（党组）或领导班子对数据安全负主体责任，主要负责人是数据安全第一责任人，分管数据安全的负责人是直接责任人，明确各部门数据安全职责及人员，建立常态化沟通与协作机制。</p>
<p>第十五条【关键岗位管理】工业和电信数据处理者应当确认数据处理关键岗位及人员，签署数据安全责任书，记录数据处理活动。</p>	<p>第十五条【关键岗位管理】工业和电信数据处理者应当确认数据处理关键岗位及人员，签署数据安全责任书，记录数据处理活动。</p>
<p>第十六条【安全同步】工业和电信数据处理者应当确保数据安全管理和技术保护手段与生产运营、业务发展同步规划、同步建设、同步运行。</p>	<p>第十六条【安全同步】工业和电信数据处理者应当确保数据安全管理和技术保护手段与生产运营、业务发展同步规划、同步建设、同步运行。</p>
<p>第十七条【数据收集】工业和电信数据处理者收集数据应当遵循合法、正当、必要的原则，不得窃取或者以其他非法方式收集数据。</p> <p>数据收集过程中，应当采取配备技术手段、签署安全协议等措施加强对数据收集人员、设备的管理，并对数据收集的时间、类型、数量、频度、流向等进行记录。</p>	<p>第十七条<u>第十四条【数据收集】工业和电信数据处理者收集数据应当遵循合法、正当、必要的原则</u>工业和<u>信息化领域</u>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。</p> <p>数据收集过程中，<u>应当采取配备技术手段、签署安全协议等措施加强对数据收集人员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</u></p>

	工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）
<p>通过间接途径获取数据的，应当要求数据提供方做出数据源合法性的书面承诺，并承担相应的法律责任。</p>	<p><u>数据收集人员</u>、设备的管理，<u>并对数据收集的时间、类型、数量、频度、流向等进行记录。</u></p> <p>通过间接途径获取<u>重要数据和核心数据的</u>，<u>工业和信息化领域数据处理器应当要求数据提供方做出数据源合法性的书面承诺，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。</u></p>
<p>第十八条【数据存储】工业和电信数据处理器应当依据法律规定或者与用户约定的方式和期限存储数据。存储重要数据的，还应当采用校验技术、密码技术等措施进行安全存储，不得直接提供存储系统的公共信息网络访问，并实施数据容灾备份和存储介质安全管理。存储核心数据的，还应当实施异地容灾备份。</p>	<p><u>第十八条第十五条</u>【数据存储】<u>工业和信息化领域数据处理器</u>应当依据法律规定或者与用户约定的方式和期限存储数据。存储重要数据和<u>核心数据的</u>，应当采用校验技术、密码技术等措施进安全存储，不得直接提供存储系统的公共信息网络访问，并实施数据容灾备份和存储介质安全管理，<u>定期开展数据恢复测试。</u>存储核心数据的，还应当实施异地容灾备份。</p>
<p>第十九条【数据使用加工】工业和电信数据处理器未经个人、单位等同意，不得使用数据挖掘、关联分析等技术手段针对特定主体进行精准画像、数据复原等加工处理活动。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，建立登记、审批机制并留存记录。</p> <p>工业和电信数据处理器提供数据处理服务，涉及经营电信业务的，应当按照相关法律、行政法规规定取得电信业务经营许可。</p>	<p><u>第十九条第十六条</u>【数据使用加工】<u>未经个人、单位等同意，不得使用数据挖掘、关联分析等技术手段针对特定主体进行精准画像、数据复原等加工处理活动。工业和电信数据处理器</u><u>工业和信息化领域数据处理器</u>利用数据进行自动化决策<u>分析的</u>，应当保证决策<u>分析</u>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，<u>建立登记、审批机制并留存记录。</u></p> <p><u>工业和电信数据处理器提供数据处理服务</u><u>工业和信息化领域</u>数据处理器提供数据处理服务，涉及经营电信业务的，应当按照相关法律、行政法规规定取得电信业务经营许可。</p>
<p>第二十条【数据传输】工业和电信数据处理器应当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。传输重要数据的，还应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施，涉及跨组织机构或者使用公共信息网络进行数据传输的，应当建立登记、审批机制。跨不同数据处理主体传输核心数据的，还应当通过国家数据安全协调机制审批。</p>	<p><u>第二十条第十七条</u>【数据传输】<u>工业和电信数据处理器</u><u>工业和信息化领域数据处理器</u>应当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<u>核心数据的</u>，应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施，<u>涉及跨组织机构或者使用公共信息网络进行数据传输的，应当建立登记、审批机制。跨不同数据处理主体传输核心数据的，还应当通过国家数据安全协调机制审批。</u></p>
<p>第二十一条【数据提供】工业和电信数据处理器应当依据行业数据分类分级管理要求，明确数据提供的范围、数量、条件、程序等。提供重要数据的，还应</p>	<p><u>第十八条</u>【数据提供】<u>工业和电信数据处理器</u><u>工业和信息化领域数据处理器</u>提供数据，<u>应当依据行业数据分类分级管理要求</u>，应当明确提供的范围、类</p>

	<p>工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）</p>
<p>当采取数据脱敏等措施，建立审批机制。提供核心数据的，还应当通过国家数据安全工作协调机制审批。工业和电信数据处理者应当事先对数据接收方的数据安全保护能力进行核实，并与数据接收方签订数据安全协议，明确数据提供的范围、使用方式、时限、用途以及相应的安全保护措施、违约责任，并督促数据接收方予以落实。</p>	<p>别、条件、程序等，<u>应当事先对数据接收方的数据安全保护能力进行核实</u>，并与数据获取方签订数据安全协议，<u>明确数据提供的范围、使用方式、时限、用途以及相应的安全保护措施、违约责任，并督促数据接收方予以落实。</u><u>提供重要数据和核心数据的，应当对数据获取方数据安全保护能力进行评估或核实，采取必要的安全保护措施。</u></p>
<p>第二十二條【数据公开】工业和电信数据处理者公开数据应当真实、准确，并在公开前开展安全评估，对涉及个人隐私、个人信息、商业秘密、保密商务信息以及可能对公共利益及国家安全产生重大影响的，不得公开。</p>	<p><u>第十九条【数据公开】工业和电信数据处理者工业和信息化领域数据处理者公开数据应当真实、准确，并在公开前开展安全评估，对涉及个人隐私、个人信息、商业秘密、保密商务信息不得公开。</u><u>应当在数据公开前分析研判</u>可能对公共利益、国家安全产生的影响，存在重大影响的<u>不得公开。</u></p>
<p>第二十三條【数据销毁】工业和电信数据处理者应当建立数据销毁策略和管理制度，明确销毁对象、流程和技术等要求，对销毁活动进行记录和留存。销毁重要数据和核心数据的，不得以任何理由、任何方式对销毁数据进行恢复。</p> <p>符合以下情况之一的，工业和电信数据处理者应当销毁相应数据：</p> <p>（一）因业务约定，需要销毁的；</p> <p>（二）个人依据其合法权益请求销毁的；</p> <p>（三）组织基于保护国家安全、社会公共利益目的，且有第三方机构提供证明，请求销毁的。</p>	<p><u>第二十三條第二十条【数据销毁】工业和电信数据处理者工业和信息化领域数据处理者应当建立数据销毁制度策略和管理制度</u>，明确销毁对象、<u>规则、流程和技术等要求</u>，对销毁活动进行记录和留存。<u>个人、组织依据法律规定、合同约定等请求销毁的，工业和信息化领域数据处理者应当销毁相应数据。</u></p> <p>销毁重要数据和核心数据的，<u>应当及时向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）更新备案</u>，不得以任何理由、任何方式对销毁数据进行恢复。</p> <p><u>符合以下情况之一的，工业和电信数据处理者应当销毁相应数据：</u></p> <p>（一）<u>因业务约定，需要销毁的； -</u></p> <p>（二）<u>个人依据其合法权益请求销毁的； -</u></p> <p>（三）<u>组织基于保护国家安全、社会公共利益目的，且有第三方机构提供证明，请求销毁的。</u></p>
<p>第二十四條【数据出境】工业和电信数据处理者在中华人民共和国境内收集和产生的重要数据，应当依照法律、行政法规要求在境内存储，确需向境外提供的，应当依法依规进行数据出境安全评估，在确保安全的前提下进行数据出境，并加强对数据出境后的跟踪掌握。核心数据不得出境。</p>	<p><u>第二十四條第二十一条【数据出境】工业和电信数据处理者工业和信息化领域数据处理者在中华人民共和国境内收集和产生的重要数据和核心数据</u>，法律、行政法规<u>要求在境内存储有境内存储要求的，应当在境内存储</u>，确需向境外提供的，应当依法依规进行数据出境安全评估，<u>在确保安全的前提下进行数据出境，并加强对数据出境后的跟踪掌握。</u>核</p>

	<p>工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）</p>
	<p><u>心数据不得出境。</u></p> <p><u>工业和信息化部根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国工业、电信、无线电执法机构关于提供工业和信息化领域数据的请求。非经工业和信息化部批准，工业和信息化领域数据处理者不得向外国工业、电信、无线电执法机构提供存储于中华人民共和国境内的工业和信息化领域数据。</u></p>
<p>第二十五条【数据承接】工业和电信数据处理者因兼并、重组、破产等原因需要转移数据的，应当明确数据承接方案，并通过电话、短信、邮件、公告等方式通知受影响用户。涉及重要数据和核心数据的，应当及时向所在地工业和信息化主管部门或通信管理局备案。</p> <p>作为数据承接方的工业和电信数据处理者，应当及时向所在地工业和信息化主管部门或通信管理局备案，承担数据安全责任和保护义务，不得违反国家有关规定及原数据处理者与用户的约定。</p> <p>重要数据和核心数据没有承接方且符合销毁条件的，工业和电信数据处理者应当依法进行数据销毁。重要数据和核心数据没有数据承接方且不符合销毁条件的，工业和电信数据处理者应当及时上报所在地工业和信息化主管部门或通信管理局，将数据移交至行业监管部门指定的机构进行保存。</p>	<p>第二十五条【数据承接】<u>第二十二条【数据转移】</u> <u>工业和电信数据处理者</u><u>工业和信息化领域数据处理者</u>因兼并、重组、破产等原因需要转移数据的，应当明确<u>数据承接方案</u><u>数据转移方案</u>，并通过电话、短信、邮件、公告等方式通知受影响用户。</p> <p>涉及重要数据和核心数据的，应当及时向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）<u>或无线电管理机构（无线电领域）</u>更新备案。作为数据承接方的工业和电信数据处理者，应当及时向所在地工业和信息化主管部门或通信管理局备案，承担数据安全责任和保护义务，不得违反国家有关规定及原数据处理者与用户的约定。</p> <p>重要数据和核心数据没有承接方且符合销毁条件的，工业和电信数据处理者应当依法进行数据销毁。重要数据和核心数据没有数据承接方且不符合销毁条件的，工业和电信数据处理者应当及时上报所在地工业和信息化主管部门或通信管理局，将数据移交至行业监管部门指定的机构进行保存。</p>
<p>第二十六条【委托处理】工业和电信数据处理者委托他人开展数据处理活动的，应当对被委托方的数据安全保护能力、资质进行核实，确保符合国家、行业主管部门的相关要求，并通过合同约定、现场核查等方式对被委托方落实数据安全保护措施的情况进行监督管理。委托处理重要数据和核心数据的，还应当委托取得相应认证资质的检测评估机构对被委托方进行安全评估。除法律、行政法规另有规定外，未经委托方同意，被委托方不得将数据提供给第三方。</p>	<p>第二十六条<u>第二十三条【委托处理】</u><u>工业和电信数据处理者</u><u>工业和信息化领域数据处理者</u>委托他人开展数据处理活动的，<u>应当通过签订合同协议等方式，明确委托方与被委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，应当对被委托方的数据安全保护能力、资质进行评估或核实。确保符合国家、行业主管部门的相关要求，并通过合同约定、现场核查等方式对被委托方落实数据安全保护措施的情况进行监督管理。委托处理重要数据和核心数据的，还应当委托取得相应认证资质的检测评估机构对</u>被委托方进行安全评估。</p> <p>除法律、<u>行政法规另有规定外</u><u>行政法规等另有规定</u></p>

	<p>工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）</p>
	<p>外，未经委托方同意，被委托方不得将数据提供给第三方。</p>
	<p><u>第二十四条【核心数据跨主体处理】跨主体提供、转移、委托处理核心数据的，应当评估安全风险，采取必要的安全保护措施，并经由地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报工业和信息化部。工业和信息化部按照有关规定进行审查。</u></p>
<p>第二十七条【安全审计】工业和电信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。日志留存时间不少于六个月，定期进行安全审计，并形成审计报告，涉及重要数据和核心数据的，应当至少每半年进行一次。</p>	<p><u>第二十七条【安全审计】第二十五条【日志留存】工业和电信数据处理者工业和电信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。日志留存时间不少于六个月，定期进行安全审计，并形成审计报告，涉及重要数据和核心数据的，应当至少每半年进行一次。</u></p>
<p>第四章 数据安全监测预警与应急管理</p>	<p>第四章 数据安全监测预警与应急管理</p>
<p>第二十八条【监测预警机制】工业和信息化部统筹建立工业和信息化领域数据安全风险监测机制，建设数据安全监测预警平台，对数据泄露、违规传输、流量异常等安全风险进行监测和预警，及时组织研判重要数据和核心数据安全风险并进行预警。</p> <p>地方工业和信息化主管部门、通信管理局建设数据安全监测预警平台，组织开展本地区工业、电信行业数据安全风险监测，按照有关规定及时发布预警信息，通知本地区工业和电信数据处理者及时采取应对措施。</p> <p>工业和电信数据处理者应当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。</p>	<p><u>第二十八条第二十六条【监测预警机制】工业和信息化部统筹建立工业和信息化领域数据安全风险监测机制，对数据泄露、违规传输、流量异常等安全风险进行监测和预警，及时组织研判重要数据和核心数据安全风险并进行预警。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、溯源、预警、处置等能力，与相关部门加强信息共享。</u></p> <p>地方工业和信息化主管部门、<u>通信管理局和无线电管理机构建设数据安全监测预警平台建设本地区数据安全监测预警机制</u>，组织开展本地区工业、电信行业<u>和无线电</u>数据安全风险监测，按照有关规定及时发布预警信息，通知本地区工业和<u>电信数据信息化领域数据</u>处理者及时采取应对措施。</p> <p><u>工业和电信数据工业和电信数据</u>工业和电信领域数据工业和电信领域数据处理者应当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。</p>
<p>第二十九条【信息上报和共享】工业和信息化部统一汇集、分析、通报工业和信息化领域数据安全风险信息，鼓励安全服务机构、行业组织、科研机构等开展数据安全风险和事件等相关信息上报和共享。</p>	<p><u>第二十九条第二十七条【信息上报和共享】工业和信息化部统一汇集建立数据安全风险信息上报和共享机制，统一汇集、分析、研判、通报工业和电信领域数据安全风险信息</u>，鼓励安全服务机构、行</p>

	<p>工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）</p>
<p>地方工业和信息化主管部门、通信管理局汇总分析本地区工业、电信行业数据安全风险和事件信息，及时将涉及重要数据和核心数据的安全风险上报工业和信息化部。</p> <p>工业和电信数据处理者应当及时将自身数据安全风险情况向所在地工业和信息化主管部门或通信管理局报告。</p>	<p>业组织、科研机构等开展数据安全风险和事件等相关信息上报和共享。</p> <p>地方工业和信息化主管部门、通信管理局和无线电管理机构汇总分析本地区工业、电信行业和无线电数据安全风险和事件信息，及时将涉及重要数据和核心数据的安全风险可能造成重大及以上安全事件的风险上报工业和信息化部。</p> <p>工业和电信工业和信息化领域数据处理者应当及时将自身数据安全风险情况可能造成较大及以上安全事件的风险向所在地地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报告。</p>
<p>第三十条【应急处置】工业和信息化部制定工业和信息化领域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。</p> <p>地方工业和信息化主管部门、通信管理局组织开展本地区工业、电信行业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，应当立即上报工业和信息化部，并及时报告事件发展和处置情况。</p> <p>工业和电信数据处理者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，应当第一时间向所在地工业和信息化主管部门或通信管理局报告。事件处置完成后应当在规定的期限内形成总结报告，每年向所在地工业和信息化主管部门或通信管理局报告数据安全事件处置情况。</p> <p>工业和电信数据处理者对可能损害用户合法权益的数据安全事件，应当及时告知用户，并提供减轻危害措施。</p>	<p>第三十条第二十八条【应急处置】工业和信息化部制定工业和信息化领域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。</p> <p>地方工业和信息化主管部门、通信管理局和无线电管理机构组织开展本地区工业、电信行业和无线电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，应当立即上报工业和信息化部，并及时报告事件发展和处置情况。</p> <p>工业和电信工业和信息化领域数据处理者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，应当第一时间向所在地地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报告。事件处置完成后应当在规定的期限内形成总结报告，</p> <p>每年向所在地地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报告数据安全事件处置情况。工业和电信工业和信息化领域数据处理者对可能损害用户合法权益的数据安全事件，应当及时告知用户，并提供减轻危害措施。</p>
<p>第三十一条【举报投诉处理】工业和信息化部委托相关行业组织建立工业和信息化领域数据安全违法行为投诉举报渠道，及时向地方工业和信息化主管部门、通信管理局、工业和电信数据处理者下发相关投</p>	<p>第三十一条第二十九条【举报投诉处理】工业和信息化部委托相关行业组织建立工业和信息化领域数据安全违法行为投诉举报渠道，及时向地方工业和信息化主管部门、通信管理局、工业和电信数据处</p>

	<p>工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）</p>
<p>诉举报信息。地方工业和信息化主管部门、通信管理局组织工业和电信数据处理器对举报信息进行核实和依法处理，对涉及重要数据和核心数据安全问题的，开展执法调查。</p> <p>工业和电信数据处理器应当建立用户投诉处理机制，公布电子邮件、电话、传真、在线客服等便捷有效的联系方式，配备受理用户投诉的人员接收数据安全相关投诉，并自接到投诉之日起 15 个工作日内答复投诉人。</p>	<p>理者下发相关投诉举报信息。地方工业和信息化主管部门、通信管理局、<u>无线电管理机构建立本地区工业、电信行业和无线电数据安全违法行为投诉举报机制或渠道，依法接收、处理投诉举报，根据工作需要开展执法调查</u>组织工业和电信数据处理器对举报信息进行核实和依法处理，对涉及重要数据和核心数据安全问题的，开展执法调查。<u>鼓励工业和</u>信息化领域数据处理器建立用户投诉处理机制。工业和电信数据处理器应当建立用户投诉处理机制，公布电子邮件、电话、传真、在线客服等便捷有效的联系方式，配备受理用户投诉的人员接收数据安全相关投诉，并自接到投诉之日起 15 个工作日内答复投诉人。</p>
<p>第五章 数据安全检测、评估与认证管理</p>	<p>第五章 数据安全检测、评估与认证管理<u>认证、评估管理</u></p>
<p>第三十二条【安全能力认证】工业和信息化部建立数据安全检测、评估与认证机构管理制度，制定机构认定标准，开展机构选拔认定、资质授权、日常管理和推荐目录发布等工作。地方工业和信息化主管部门、通信管理局依据管理制度和认定标准，开展本地区工业、电信行业数据安全检测、评估与认证机构选拔认定、资质授权和管理等工作。</p>	<p>第三十二条【安全能力认证】<u>第三十条【安全检测与认证】</u>工业和信息化部<u>鼓励、引导具备相应资质的机构，依据相关标准开展行业数据安全检测、认证工作。</u>建立数据安全检测、评估与认证机构管理制度，制定机构认定标准，开展机构选拔认定、资质授权、日常管理和推荐目录发布等工作。地方工业和信息化主管部门、通信管理局依据管理制度和认定标准，开展本地区工业、电信行业数据安全检测、评估与认证机构选拔认定、资质授权和管理等工作。</p>
<p>第三十三条【安全评估】工业和信息化部制定工业和信息化领域数据安全评估规范，指导检测评估机构开展数据安全风险评估、合规评估等工作。地方工业和信息化主管部门、通信管理局负责组织开展本地区工业、电信行业数据安全评估。</p> <p>工业和电信数据处理器应当依据数据安全评估规范，开展数据安全评估及整改。</p> <p>（一）对于一般数据，鼓励开展数据安全自评估，对发现的数据安全风险问题进行及时整改；</p> <p>（二）对于重要数据和核心数据，应当至少每年自行或者委托推荐目录中的检测评估机构开展一次安全评估，并向所在地工业和信息化主管部门或通信管理局报告。</p>	<p>第三十三条<u>第三十一条【安全评估】</u>工业和信息化部制定<u>行业数据安全评估机构管理制度</u>，开展评估机构管理工作。制定行业数据安全评估规范，指导评估机构开展数据安全风险评估、合规评估、能力评估、<u>出境评估</u>等工作。</p> <p>地方工业和信息化主管部门、通信管理局<u>和无线电管理机构</u>负责组织开展本地区工业、电信行业<u>和无线电数据安全评估工作。</u>工业和电信数据处理器应当依据数据安全评估规范，开展数据安全评估及整改。</p> <p>（一）对于一般数据，鼓励开展数据安全自评估，对发现的数据安全风险问题进行及时整改；</p> <p>（二）对于重要数据和核心数据，应当至少每年自</p>

	<p>工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）</p>
	<p>行或者委托推荐目录中的检测评估机构开展一次安全评估，并向所在地工业和信息化主管部门或通信管理局报告。</p> <p><u>工业和信息化领域重要数据和核心数据处理者应当自行或委托第三方评估机构，每年至少开展一次安全评估，及时整改风险问题，并向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报送评估报告。</u></p>
<p>第六章 监督检查</p>	<p>第六章 监督检查</p>
<p>第三十四条【监督检查和协助义务】工业和信息化部组织制定数据安全监测接口标准。行业监管部门对工业和电信数据处理者落实本规定要求的情况进行监督检查。工业和电信数据处理者应当配合行业监管部门依法开展监督检查，并预留检查接口。</p>	<p>第三十四条【监督检查和协助义务】<u>第三十二条【监督检查和协助义务】</u>工业和信息化部组织制定数据安全监测接口标准行业（领域）监管部门对工业和电信工业和电信领域数据处理者落实本规定办法要求的情况进行监督检查。</p> <p><u>工业和电信工业和电信领域数据处理者应当对行业（领域）监管部门监督检查予以配合。数据处理者应当配合行业监管部门依法开展监督检查，并预留检查接口。</u></p>
<p>第三十五条【数据安全审查】工业和信息化部在国家数据安全工作协调机制指导下，对影响或可能影响国家安全的工业和电信数据处理活动开展数据安全审查。</p>	<p>第三十五条<u>第三十三条</u>【数据安全审查】工业和信息化部在国家数据安全工作协调机制指导下，对影响或可能影响国家安全的工业和电信数据处理活动开展数据安全审查<u>相关工作。</u></p>
<p>第三十六条【保密要求】行业监管部门及其委托的数据安全检测评估机构工作人员对在履行职责中知悉的个人信息和商业秘密等，应当严格保密，不得泄露、出售或者非法向他人提供。</p>	<p>第三十六条<u>第三十四条</u>【保密要求】行业（领域）监管部门及其委托的数据安全检测评估机构工作人员对在履行职责中知悉的个人信息和商业秘密等，应当严格保密，不得泄露、出售或者非法向他人提供。</p>
<p>第三十七条【约谈整改】行业监管部门在履行数据安全监督管理职责中，对未按要求进行重要数据和核心数据备案，或者发现数据处理活动存在重大安全风险或发生安全事件的，可以按照规定权限和程序对工业和电信数据处理者的法定代表人或者主要负责人进行约谈，并要求采取措施进行整改，消除隐患。</p>	<p>第三十七条<u>第三十五条</u>【约谈整改】行业（领域）监管部门在履行数据安全监督管理职责中，对未按要求进行重要数据和核心数据备案，或者发现数据处理活动存在重大安全风险或发生安全事件的，可以按照规定权限和程序对工业和电信工业和电信领域数据处理者的法定代表人或者主要负责人进行约谈，并要求采取措施进行整改，消除隐患。</p>
<p>第七章 法律责任</p>	<p>第七章 法律责任</p>
<p>第三十八条【信用机制】行业监管部门应当将工业和</p>	<p>第三十八条【信用机制】行业监管部门应当将工业</p>

	工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）
电信数据处理者落实数据安全管理工作情况纳入信用管理。对存在数据安全违法违规行为受到行政处罚的数据处理者，按照有关规定将其列入业务经营不良名单或失信名单。	和电信数据处理者落实数据安全管理工作情况纳入信用管理。对存在数据安全违法违规行为受到行政处罚的数据处理者，按照有关规定将其列入业务经营不良名单或失信名单。
第三十九条【法律责任】对于违反本办法的，由行业监管部门依照《数据安全法》《网络安全法》等法律和相关法律法规，根据情节严重程度给予公开曝光、没收违法所得、罚款、暂停业务、停业整顿、关闭网站、吊销业务许可证或吊销营业执照等行政处罚；构成犯罪的，依法追究刑事责任。	第三十九条 第三十六条 【法律责任】有违反本办法规定行为的，由行业（领域）监管部门依照《数据安全法》《网络安全法》等法律和相关法律法规，根据情节严重程度给予公开曝光没收违法所得、罚款、暂停业务、停业整顿、吊销业务许可证关闭网站、或吊销营业执照等行政处罚；构成犯罪的，依法追究刑事责任。
第八章 附则	第八章 附则
	第三十七条 【个人信息保护】 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。
第四十条【涉密排除】涉及国家秘密信息、密码使用等数据处理活动，按照国家有关规定执行。	第四十条 【涉密排除】 第三十八条 【其他规定参照】 涉及军事、国家秘密信息、密码使用等数据处理活动，按照国家有关规定执行。
第四十一条【军事数据排除】涉及军事的数据处理活动，按照国家有关规定执行。	第四十一条 【军事数据排除】 涉及军事的数据处理活动，按照国家有关规定执行。
第四十二条【政务数据排除】工业和信息化领域政务数据处理活动的具体办法，由工业和信息化部另行规定。	第四十二条 第三十九条 【政务数据排除】工业和信息化领域政务数据处理活动的具体办法，由工业和信息化部另行规定。
第四十三条【国防科工、烟草领域】国防科技工业、烟草领域数据安全管理工作由国防科工局、国家烟草专卖局负责，具体制度参照本办法另行制定。	第四十三条 第四十条 【国防科工、烟草领域】国防科技工业、烟草领域数据安全管理工作由国防科工局、国家烟草专卖局负责，具体制度参照本办法另行制定。
第四十四条【施行日期】本规定自 年 月 日起施行。	第四十四条 第四十一条 【施行日期】本规定自 本法 自 2022 年 月 日起施行。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123

Email: kevin.duan@hankunlaw.com