《零售企业数据安全合规指南》

数据安全作为《基于数字化运营的CRM 3.0系统需求指南》重要的一部分，协会联合知名律所北京市盈科律师事务所，以及其它相关专家，在《CRM需求指南》中增加了《合规指南》的内容，专家们结合司法实践，系统阐述了数据安全合规的相关要求，为企业开展数据应用相关工作提供了可靠的指引。在CRM系统需求中，加入数据安全合规的内容，是一项具有创新性的实践，将与数据相关的技术开发、业务运营和法规要求进行有机结合。

《零售企业数据安全合规指南》作为《基于数字化运营的CRM 3.0系统需求指南》的一部分于2023年2月10日发布，其他部分将于近期发布，敬请关注。

1 数据安全发展趋势

1.1 数据要素市场发展趋势

数据要素市场化是数字经济的新现象。由于大数据与人工智能技术的结合，数据已经成为第一生产要素，数据及其运行机制成为支撑算法算力切实有效发挥作用的关键要素，是数字经济高质量发展的基础原料和逻辑基点。数据正在成为企业进行决策、生产、营销、交易、配送、服务等商务活动所必不可少的投入品和重要的战略性资产，成为促进经济高质量增长的重要驱动力。协同推进技术、 模式、业态和制度创新，切实用好数据要素，将为经济社会数字化发展带来强劲动力。

1）国家层面的顶层设计

2020 年 4 月 9 日，中共中央、国务院印发《关于构建更加完善的要素市场化配置体制机制的意见》，进一步强调数据要素的重要地位，将数据与土地、资本、技术、劳动并列为五大生产要素。提出加快培育数据要素市场，包括推进政府数据开放共享、提升社会数据资源价值、加强数据资源整合和安全保护三项具体内容。

2021年3月，中央在“十四五”规划中作出了“建设高标准市场体系；推进土地、劳动力、资本、技术、数据等要素市场化改革”的战略部署，要求建立数据资源产权、交易流通、跨境传输和安全保护等基础制度和标准规范，推动数据资源开发利用。

2021 年 12 月 12 日，国务院印发《“十四五”数字经济发展规划》，提出在2025 年初步建立数据要素市场体系，充分发挥数据要素作用。

2）各地陆续出台数字经济促进条例

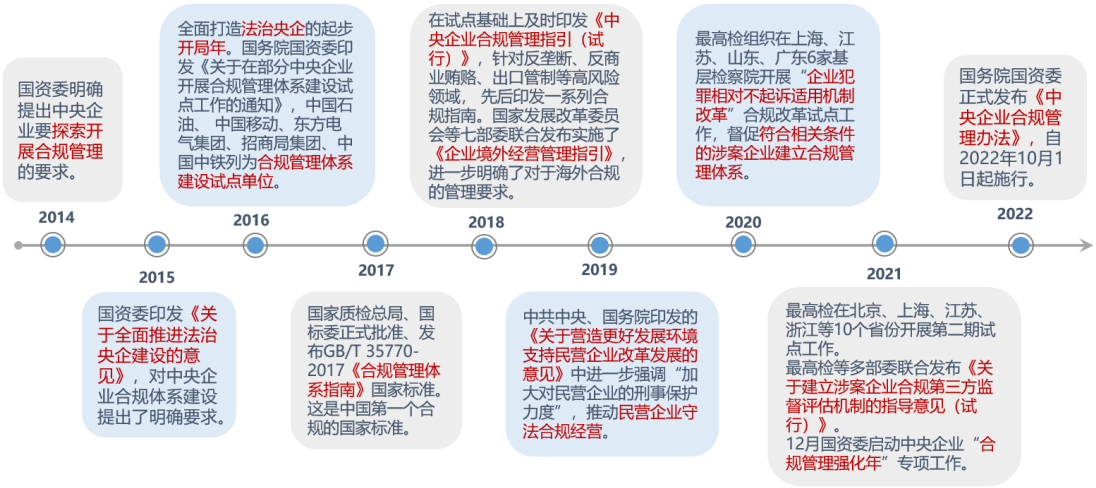
2021-2022年，全国各省市陆续出台了数字经济促进条例，以培育数据要素市场。例如，自2022年6月1日起施行的《广州市数字经济促进条例》第四条规定：“数字经济发展应当以数字产业化和产业数字化为核心，推进数字基础设施建设，实现数据资源价值化，提升城市治理数字化水平，营造良好发展环境，构建数字经济全要素发展体系。”自2022年11月1日起施行的《深圳经济特区数字经济产业促进条例》第二十三条规定：“鼓励市场主体加强数据开放和数据流动，推动数据要素资源化、资产化、资本化发展。” 即将于2023年1月1日起施行的《北京市数字经济促进条例》第一条明确：“为了加强数字基础设施建设，培育数据要素市场，推进数字产业化和产业数字化，完善数字经济治理，促进数字经济发展，建设全球数字经济标杆城市，根据有关法律、行政法规，结合本市实际情况，制定本条例。”

国家和地方相关政策文件的密集出台，为数据作为生产要素在市场中进行配置，提供了政策土壤，也推动了我国大数据产业不断发展，技术不断进步，基础设施不断完善，融合应用不断深入。

1.2 企业合规管理发展趋势

习近平总书记强调，守法经营是任何企业都必须遵守的一个大原则,企业只有依法合规经营才能行稳致远。党的十九大后，党中央明确提出习近平法治思想，把全面依法治国提升到前所未有的新高度。《法治中国建设规划（2020 - 2025年）》《法治社会建设实施纲要（2020-2025年）》等中央文件对企业依法合规经营提出明确要求。在当前国际竞争越来越体现为规则之争、法律之争的大背景下，我国企业面临的国内外环境和风险挑战日趋复杂严峻,必须加快提升依法合规经营管理水平,确保改革发展各项任务在法治轨道上稳步推进。自2022年10月1日起施行的《中央企业合规管理办法》第三条规定对企业“合规”的定义，作出了明确规定：“本办法所称合规，是指企业经营管理行为和员工履职行为符合国家法律法规、监管规定、行业准则和国际条约、规则，以及公司章程、相关规章制度等要求。”合规管理成为企业做大做强的必经之道。

1）我国企业合规管理政策的发展历程



2）合规成为企业管理必选项

为推进合规管理，《中央企业合规管理办法》制定了一系列保障措施，例如，在组织和职责方面，将中央企业主要负责人作为推进法治建设第一责任人，设立合规委员会，由总法律顾问兼任首席合规官等；在运行机制方面，应当建立合规风险识别评估预警机制，将合规审查作为必经程序嵌入经营管理流程，并应建立违规问题整改机制、设立违规举报平台、完善违规行为追责问责机制等。

1.3 网络安全与数据安全发展趋势

当前，以数字经济为代表的新经济成为经济增长新引擎，数据作为核心生产 要素成为了基础战略资源，数据安全的基础保障作用也日益凸显。伴随而来的数 据安全风险与日俱增，数据泄露、数据滥用等安全事件频发，为个人隐私、企业 商业秘密、国家重要数据等带来了严重的安全隐患。为了规范数据处理活动，保障数据安全，促进数据开发利用，近两年来，国家对数据安全与个人信息保护进行了前瞻性战略部署，开展了系统性的顶层设计。《中华人民共和国数据安全法》于2021年9月1日正式施行，《中华人民共和国个人信息保护法》于2021年11月1日正式施行。这两部法律与2017年的《中华人民共和国网络安全法》共同构建了中国数据合规及隐私保护的基础法律框架，对网络安全、数据安全和个人信息保护提出了方向性和基础性指引及监管要求。

“工欲善其事，必先利其器”，在数字经济快速发展的背景下，我们更需要深刻认识到数据安全建设的重要性，不仅需要在技术上重点布局、勇于创新，更需要在安全意识和安全管理水平上大幅提升。

2 安全合规指南

2.1 数据资产盘点

2.1.1 数据流向测绘

首先，要做数据安全管控，我们需要知道企业目前有哪些数据，数据是如何分布的，哪些是敏感数据，敏感数据分布在哪里。为了解决这些问题，我们需要做的是数据资产的梳理、数据分类分级。

其次，要做好敏感数据的安全管控，我们需要知道敏感数据是如何产生的，敏感数据是如何存储的，敏感数据是如何使用的，如谁有权访问敏感数据。为了解决这些问题，我们需要做的是“根据数据分类分级结果，针对敏感数据识别具体的使用场景，绘制出数据流转图。

再次，根据上述绘制的数据流转图，基于整个业务场景识别敏感数据可能存在的安全风险，开展风险评估。同时，识别敏感数据现有的安全控制措施，分析当前存在的不足。

最后，根据风险评估结果，设计差异化、可落地的安全管控措施，包括管理措施、技术措施、监控审计类措施，目的是为了确保数据安全的“可感、可控、可审、可视”。

2.1.2 资产盘点

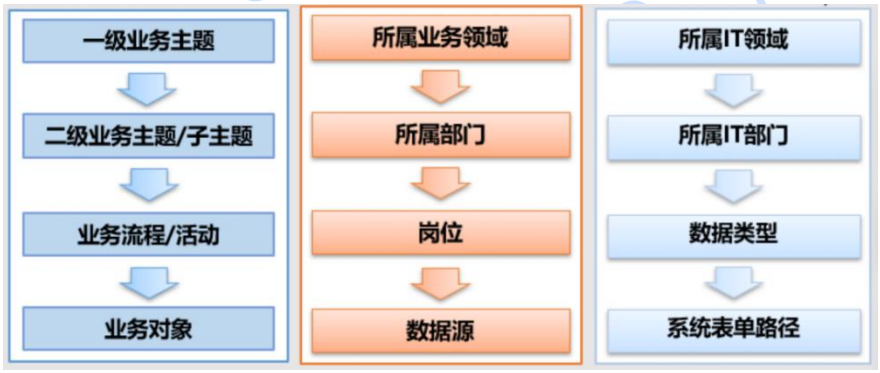
企业开展数据资产盘点的过程中，需要结合所盘点的业务情况，划定业务过程中需要进行盘点的数据范围，即对“企业在运营活动中形成的，由企业拥有、全过程可控，并能给企业带来价值的数据”开展盘点，当拥有、可控、具有价值三个条件全部满足时，即可识别为数据资产盘点的对象范畴。

数据资产盘点范围应包含18种数据资源，盘点数据资产类型可分为：业务对象、基础表、代码表、报表与指标等。

业务类	1.0 集成产品开发（IPD）
	2.0 从市场到线索（MTL）
	3.0 渠道销售（CS）
	4.0 零售（Retail）

	5.0 从商机到回款（OTC）
	6.0 从问题到解决（ITR）
使能类	7.0 从战略到执行（DSTE）
	8.0 资本运作管理（CIM）
	9.0 集成供应链（ISC）
	10.0 采购管理（PM）
	11.0 客户关系管理（CRM）
支撑类	12.0 人力资源管理（HRM）
	13.0 财务管理（FM）
	14.0 质量管理体系（QMS）
	15.0 流程与IT（BP&IT）
	16.0 品牌与公共关系管理（B&RM）
	17.0 基建管理（CCM）
	18.0 基础支持管理（BSM）

数据资产盘点要围绕企业的全部业务活动展开，包含所有类型数据(线上线下、结构半结构)，真实反映数据资源全貌，并识别出核心的数据资产。盘点的方法和过程包含以下内容：



（1）业务层面盘点

划分业务主题及子主题，梳理业务流程和业务活动，识别业务对象。

（2）组织层面盘点

确定数据所属业务领域、业务部门、岗位及数据来源。

（3）IT层面盘点

数据所属IT架构中具体区域、IT系统、数据类型和系统路径。

（4）成果汇总

业务层面、组织层面和IT层面盘点的成果填充至提前制定好的数据资产盘点模板，形成数据资产盘点清单。

（5）清单内容细化

针对盘点的成果进行内容细化，例如数据量、更新频率、数据重要等级、数据密集等资产认定字段进行完善。

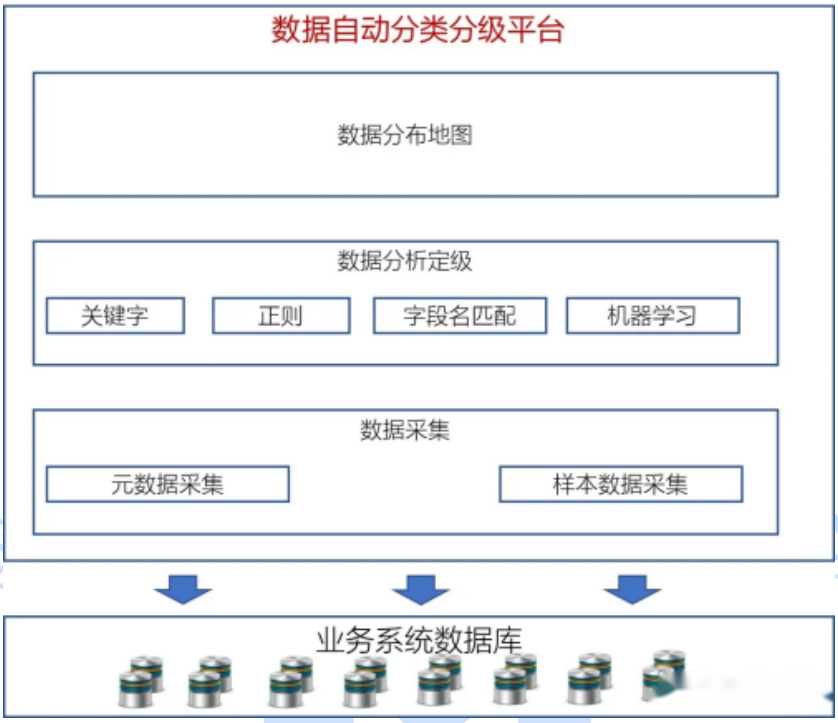
（6）输出数据资产盘点成果

输出数据资产盘点成果，为后续构建数据资产地图、数据安全管理、数据治理提供基础支持。

2.2 数据分类分级

从数据分类而言，建议数据分类遵循有关法律法规及部门规定要求，优先对国家或行业有专门管理要求的数据进行识别和管理，满足相应的数据安全合规管理要求。比如识别是否存在国家核心数据、重要数据、个人信息数据等。根据不同数据分类，匹配不同的法律法规要求，部署相应的落地要求。

借助技术手段可以对结构化数据开展自动分类分级和敏感数据的标志标识，最终输出数据资产分布地图。如下图所示，自动分类分级平台可以通过多种方式采集应用系统中的原始数据，并使用关键字、正则表达式、字段名匹配、表明匹配、机器学习、自然语言识别等多种敏感信息识别算法，识别敏感数据的类型，并按照分级标准完成敏感数据的分级。



数据类别千差万别，甚至同样的数据在不同的单位，重要程度的级别可能不一样。“数据处理活动”的主体，可以根据主管部门、监管单位对本行业的数据分类分级标准进行数据分类、分级。若“数据处理活动”主体的主管、监管单位未制定相关标准，则建议按照上图进行分类分级，并建立对应级别的数据保护措施。通过数据映射，将数据的类别和级别，按照法律法规和国家标准、行业标准的保护要求进行保护，并以下列形式进行展现：

数据分类分级映射表

数据分类			数据编码	数据分级				
一级分类	二级分类	三级分类	编码规则	一级	二级	三级	四级	五级
核心数据	——	——	HX001				——	——
重要数据			ZY001			——	——	
个人信息	敏感个人信息	个人健康数据	GX001			——	——	
	一般个人信息	个人手机号码	GX002		——			
业务数据	敏感业务数据	知识产权数据	YW001			——	——	
	重要业务数据	财务数据	YW002		——	——		
	一般业务数据	公开业务数据	YW003	——	——			

2.3 数据安全风险评估

为确保业务合规，企业在开展业务之前需进行相应的风险评估；与此同时，企业开展对个人权益有重大影响的个人信息处理活动时，应当事前进行个人信息保护影响评估，这既是《个人信息保护法》第五十五条规定的法定义务，也是数据合规风险评估的一种。

结合企业业务实际情况，建议在以下场景中增加数据合规评估：

1) 产品/IT方案上线（尤其是涉及用户数据收集的产品/IT）

2) 数据入/出数据湖

3) 涉及个人数据处理的用户活动

4) 流程发布

5) 个人数据采购

6) 对外提供个人数据

为平衡数据合规评审效率和质量，可以分层分级进行风险评审。主要场景如下：

1) 成熟场景：成熟场景风险相对可控，可基于业务部门数据合规BP的能力交由数据合规BP负责评审。成熟场景的定义可以采用白名单管理，成熟一个授权一个。

2) 新场景（新业务、新产品）：新场景涉及的法律不清晰、业务场景不清晰，需由专业团队把关，建议由数据合规专家（能力小组）进行评审。

3) 升级机制：当遇到数据合规BP无法判断的场景时，可将评审工作升级，由数据合规专家（能力小组）进行把关。

2.4 数据全生命周期保护框架

2.4.1 管理体系的重要角色部门

1) 数据合规负责人

2) 《个人信息保护法》第52条规定，“处理个人信息处理数量达到网信部门规定数量的个人信息处理者应当指定个人信息保护负责人。”《数据安全法》第27条也规定，重要数据的处理者应当明确数据安全负责人和管理机构

3) 数据合规负责人的级别如何设置。个人信息保护负责人具体如何设置、级别如何安排，属于企业自治内容，但应与企业重要数据/个人信息的数量、重要程度等相匹配。

4) 数据合规组织机构

5) 数据合规组织机构是指明确配合个人信息保护负责人开展工作的工作机构。《数据安全法》第27条规定，重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。《个人信息保护法》虽然没有直接规定企业应当设立个人信息保护工作机构，但其对企业处理个人信息规定了各方面义务，履行这些义务显然需要专门工作机构的支持。

6) 成熟的数据合规管理体系一般围绕以下骨架搭建：数据合规工作组可分领导小组、能力小组、实施小组。领导小组由主要由公司重量级领导做组长，各业务部门主管为成员，负责制定整体策略，决策数据合规方案；能力小组由法务合规专家、技术专家组成，负责制定数据合规要求，跨部门统筹协调等；实施小组主要由各BG/BU的数据合规人员组成，负责数据合规的具体落实。

7) 独立监督机构

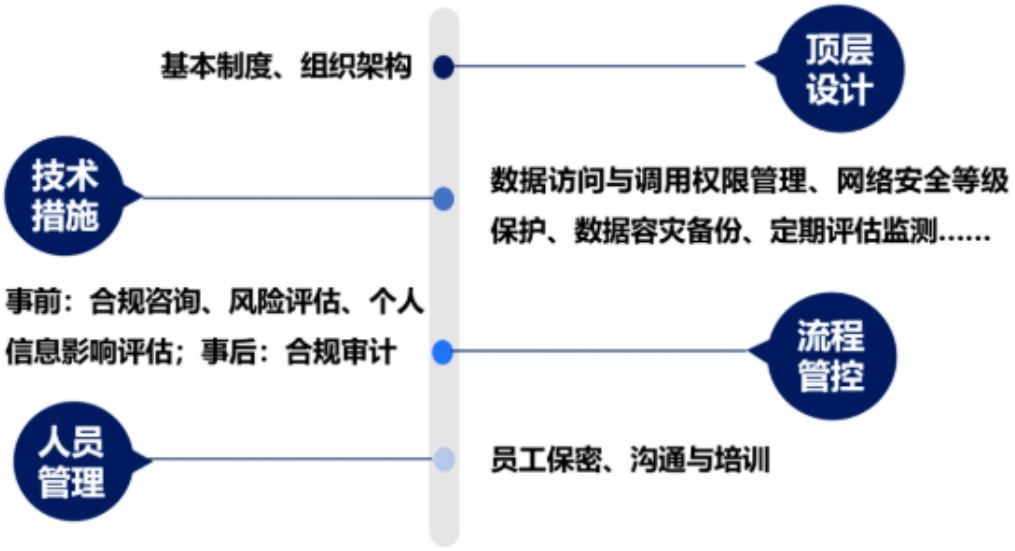
8) 《个人信息保护法》第58条规定，提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当成立主要由外部成员组成的独立机构对个人信息保护情况进行监督。

9) 在落实《个人信息保护法》该项规定的过程中，涉案企业合规第三方监督评估制度和上市公司独立董事制度可能会成为参考。因此，建议企业在制定未来规划时，可以尽早考虑成立独立监督机构，占据主动优势。

2.4.2 数据合规 BP 的“能力模型”

数据合规BP是整个数据合规责任体系的关键，一个合规的数据合规BP才能帮助业务主管履行好数据合规管理第一责任人的职责。数据合规BP（Business Partner） 能力模型包含三个方面——法律、技术、业务。

2.5 数据安全管理体系建设



通过对企业数据安全管理现状的梳理，对于企业在数据安全合规体系方面需要整改或调整的方向和重点事项有了基本判断，进而进入整改环节。

企业在数据安全合规体系建设将涉及企业内部机构的机构设置、职能安排和编制管理，需要综合企业整体合规规划、业务发展、组织结构、信息安全能力、资源和成本等多方面情况考虑。企业数据安全合规体系建设工作可以分解为以下几个方面：

1）制定行动计划

企业的数据安全合规体系建设方案，法律人员可以与企业其他相关人员基于企业数据合规现状、围绕企业开展本次数据合规的目标制定数据合规整改行动计划，对企业应当在什么时限内、按照何种优先顺序、采取何种具体措施以满足特定的数据合规要求作出安排，作为后续工作的操作指引。

2）落实数据安全合规体系建设方案

数据安全合规体系建设的实施主体主要是企业的相关管理和业务部门。法律人员可以在组织架构搭建的合法合规性、相关制度文本内容的规范性、合法性和有效性，以及数据安全合规管理措施的合法性等方面提供专业支撑。

例如，根据《个人信息保护法》，企业处理个人信息达到一定数量或者处理重要数据的，应当设置数据合规管理机构、指定数据合规负责人。就企业数据合规组织架构搭建，法律人员根据法律规定、企业公司章程规定、企业合规管理组织架构现状及企业实际情况，提出相应的建议方案。

又如，法律人员协助起草和审查相关数据安全管理制度文本的规范性、合法性和有效性。企业的数据合规管理制度体系可以从三个层次考虑：

确定企业、全体成员和业务伙伴共同遵守的数据合规行为准则，列明数据合规底线。

企业数据安全管理的纲领性文件，明确公司数据合规管理总体要求、管理机构及职责、基本制度、网络及数据安全技术措施、信息系统安全保护等事项。

相关具体制度，确定包括管理流程、管理标准、管理措施等具体数据合规管理细则。法律人员通常需要协助企业对照数据安全相关法律规定，起草、修改、审阅相关制度文本。

企业建立数据安全合规体系后，需要在日常运营和管理中落实运行。法律人员在数据合规咨询、数据合规审查评估、数据合规审计、人员培训等方面提供持续的法律服务支撑，是企业数据安全管理的重要方面。

2.6 营销/算法推荐合规管理体系

《个人信息保护法》第24条对利用个人信息进行自动化决策行为进行规定，算法推荐是自动化决策的方式之一，因此，对算法推荐的法律规制也要依次为依据，《互联网信息服务算法推荐管理规定》则是对算法推荐的规制作了详细规定，更具有可操作性。结合出台的相关法律法规，梳理了算法推荐合规义务清单如下：

“算法推荐”合规义务清单

序号	义务内容	风险行为	义务来源	法规要求
1.算法推荐规制的原则性规定				
1.1	算法推荐规制的总体要求	公司是否存在违法行为，是否遵守科学伦理?	《互联网信息服务算法推荐管理规定（征求意见稿）》第4条	应当遵守法律法规，尊重社会公德和伦理，遵守商业道德和职业道德，遵循公正公平、公开透明、科学合理和诚实信用的原则。
1.2	坚持主流价值导向，促进算法应用向上向善	公司提供算法推荐服务未树立正确价值观	《互联网信息服务算法推荐管理规定（征求意见稿）》第6条	应当坚持主流价值导向，优化算法推荐服务机制，积极传播正能量，促进算法应用向上向善。
1.3	禁止利用算法推荐从事违法活动、发布违禁信息	公司利用算法推荐发布信息未经审查		不得利用算法推荐服务从事危害国家安全、扰乱经济秩序和社会秩序、侵犯他人合法权益等法律、行政法规禁止的活动， 不得利用算法推荐服务传播法律、行政法规禁止的信息。
1.4	应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。	公司利用个人信息进行自动化决策是否针对个人实现不合理的差别待遇	《个人信息保护法》第24条第1款	个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。

	理的差别待遇。			理的差别待遇。
2.落实算法安全主体责任				
2.1	建立健全内部管理制度： （1）用户注册； （2）信息发布审核； （3）算法机制机理审核； （4）安全评估监测； （5）安全事件应急处置； （6）数据安全保护和个人信息保护。	公司未建立有效的管理制度和操作规程	《互联网信息服务算法推荐管理规定（征求意见稿）》第7条	算法推荐服务提供者应当落实算法安全主体责任，建立健全用户注册、信息发布审核、算法机制机理审核、安全评估监测、安全事件应急处置、数据安全保护和个人信息保护等管理制度，制定并公开算法推荐相关服务规则，配备与算法推荐服务规模相适应的专业人员和技术支撑。
2.2	制定并公开算法推荐相关服务规则	公司未按规定制定和公开算法推荐相关服务规则		
2.3	配备与算法推荐服务规模相适应的专业人员和技术支撑	公司未配备专业人员和提供相应的技术支撑来保障算法安全		
2.4	完善算法推荐服务管理机制	公司未落实管理机制，对服务日志进行留存	《互联网信息服务算法推荐管理规定（征求意见稿）》第23条	应当完善算法推荐服务管理机制，对算法推荐服务日志等信息进行留存，留存期限不少于六个月，并在相关执法部门依法查询时予以提供。
2.5	安全评估	作为具有舆论属性或者社会动员能力的算法推荐服务提供者未按规定履行安全评估义务		具有舆论属性或者社会动员能力的算法推荐服务提供者应当按照国家有关规定开展安全评估。
3.加强算法推荐				
3.1	定期审核、评估、验算算法机制机理、模型、数据和应用结果等	公司未定期开展审核、评估、验算工作	《互联网信息服务算法推荐管理规定（征求意见稿）》第8条	应当定期审核、评估、验证算法机制机理、模型、数据和应用结果等。
3.2	算法模型不得违背公序良俗	公司的算法模型未进行伦理审查		不得设置诱导用户沉迷或者高额消费等违背公序良俗的算法模型。
4.加强信息内容管理				
4.1	建立健全用于识别违法和不良信息的特征库及入库标准、规则和程序	公司未建立识别违法和不良信息的特征库	《互联网信息服务算法推荐管理规定（征求意见稿）》第9条	建立健全用于识别违法和不良信息的特征库，完善入库标准、规则和程序。
4.2	只有作出显著标识的算法生成的合成信息方可继续传输	未作显著标识的算法生成合成信息不得继续传输		发现未作显著标识的算法生成合成信息的，应当作出显著标识后，方可继续传输。
4.3	发现违法信息的处置方案	公司发现违法信息未采取相应处置措施		发现违法信息的，应当立即停止传输，采取消除等处置措施，防止信息扩散，保存有关记录，并向网信部门报告。发现不良信息的，应当按照网络信息内容生态治理有关规定予以处置。
5.加强用户模型和用户标签管理				
5.1	完善记入用户模型的兴趣点规则	公司未制定或制定不完善的兴趣点规则	《互联网信息服务算法推荐管理规定（征求意见稿）》第10条	完善记入用户模型的兴趣点规则，不得将违法和不良信息关键词记入用户兴趣点或者作为用户标签并据以推送信息内容，不得设置歧视性或者偏见性用户标签。
5. 2	不得将违法和不良信息关键词记入用户兴趣点或者作为用户标签并据以推送信息内容	公司用户兴趣点或用户标准成在违法和不良信息关键词		
5. 3	不得设置歧视性或者偏见性用户标签	公司违反规定设置歧视性或者偏见性用户标签		
6.加强算法推荐服务版面页面生态管理				
6.1	建立完善人工干预和用户自主选择机制	公司未建立相关干预和选择机制	《互联网信息服务算法推荐管理规定（征求意见稿）》第11条	算法推荐服务提供者应当加强算法推荐服务版面页面生态管理，建立完善人工干预和用户自主选择机制，在首页首屏、热搜、精选、榜单类、弹窗等重点环节积极呈现符
6.2	在重点环节呈现符合主流价值导向的信息内容	公司未在重点环节呈现符合主流价值导向的信息内容		
7.保障用户知情权				
7.1	综合运用相应策略和规则来增强算法的透明度和可解释性	公司是否采取相关策略和规则增加算法的透明度和可解释性	《互联网信息服务算法推荐管理规定（征求意见稿）》第12条	算法推荐服务提供者应当综合运用内容去重、打散干预等策略，并优化检索、排序、选择、推送、展示等规则的透明度和可解释性，避免对用户产生不良影响、引发争议纠纷。
7.2	以显著方式告知用户情况，并以适当方式公示算法推荐服务的原理/目的/运行机制	公司未设置显著方式告知用户的方案和未以适当方式公示算法推荐原理/目的/运行机制	《互联网信息服务算法推荐管理规定（征求意见稿）》第14条	应当以显著方式告知用户其提供算法推荐服务的情况，并以适当方式公示算法推荐服务的基本原理、目的意图、运行机制等。
7.3	不得利用算法实施流量造假行为	公司应核查是否实施流量造假等行为	《互联网信息服务算法推荐管理规定（征求意见稿）》第13条	不得利用算法虚假注册账号、非法交易账号、操纵用户账号，或者虚假点赞、评论、转发、网页导航等，实施流量造假、流量劫持；
7.4	不得利用算法干预信息呈现，实施自我优待、不正当竞争、影响网络舆论或者规避监管	公司是否为达到非法目的存在利用算法干预信息呈现的行为		不得利用算法屏蔽信息、过度推荐、操纵榜单或者检索结果排序、控制热搜或者精选等干预信息呈现，实施自我优待、不正当竞争、影响网络舆论或者规避监管。
8.保障用户自主选择权				
8.1	提供不针对个人信息的选项或便捷关闭选项	公司提供算法推荐服务是否设置针对个人信息的选项，是否提供便捷关闭选项	《互联网信息服务算法推荐管理规定（征求意见稿）》第15条、《个人信息保护法》第24条第2款	应当向用户提供不针对其个人特征的选项，或者向用户提供便捷的关闭算法推荐服务的选项。用户选择关闭算法推荐服务的，算法推荐服务提供者应当立即停止提供相关服

2.7 数据安全事件应急响应

预防数据泄露是数据合规工作中的重点和难点之一，数据泄露事件一旦发生，企业不仅需要承担高昂的经济损失，还可能承担严重的法律后果。《数据安全法》规定，对造成大量数据泄露等严重后果的数据处理者，将处以较高数额的罚款，责令暂停相关业务、停业整顿、吊销相应业务许可证或营业执照；《个人信息保护法》也规定，违反个人信息保护义务导致信息数据泄露的，将没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务，相关违法行为还会被计入信用档案并公示。企业在数据安全事件发生后应注意采取如下应对措施：

2.7.1 调查、评估与补救措施

接到威胁情报或者监管部门事件通知后，涉事企业应按照本企业的《网络安全应急预案》部署事件处理团队，立即进行事件确认，调查排查数据泄露的原因，识别涉及的数据类型和数量以及数据的敏感程度，确定受影响的个人信息主体的范围，分析所涉数据是否已加密、防控措施是否有效抵御了攻击等，据此评估对个人信息主体的权利和自由的影响程度以及其他可能造成的后果。同时，企业应当立即保护网络系统，修复可能造成数据泄露的漏洞，并防止数据进一步泄露，例如封锁环境、限制访问、监控出入点、关闭受影响的设备、更改秘钥等。在此过程中，企业可以聘请外部法律和技术团队协助电子数据取证并留存证据，以备后续可能发生的调查和争议。

2.7.2 情况上报与通知受影响主体

根据对安全事件的影响与风险的评估以及相关法律法规要求，确定企业是否需要上报监管机构、是否需要通知受影响的个人信息主体。如有必要，企业应迅速确定如下内容：

1）此次安全事件是否受域外法律管辖，且所涉域外法律是否有特殊规定；

2）上报哪个/哪些监管机构，是否包括域外的监管机构；

3）需要通知的数据主体的范围以及通知的方式；

4）上报的内容以及通知的内容。在确定上述内容后，及时根据相关法律法规要求进行上报和通知。

《网络安全法》也在第22和25条规定了网络运营者的通知义务和补救义务。网络运营者发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告；在发生危害网络安全的事件时，应立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

GDPR第33和34条规定了在发生个人数据泄露的情形时，数据控制者的报告和通知义务。除非个人数据泄露不太可能会对自然人的权利和自由造成风险，数据控制者应当在发现数据泄露的72小时内将个人数据泄露的情况报告监管机构。如果数据泄露可能对自然人的权利和自由产生较高风险，数据控制者还应当立即将个人数据泄露的事实告知数据主体。

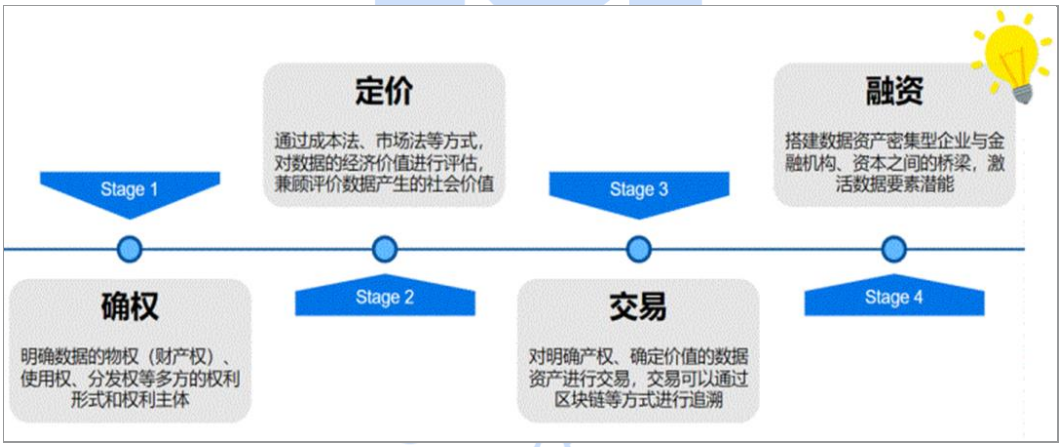
2.7.3 做好安全事件记录

《网络安全法》第21条还要求网络运营者采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。

无论安全事件是否需要上报监管机关或通知受影响的自然人，企业都应当做好安全事件的记录。如果企业根据评估决定不上报和通知，企业应当记录评估的分析过程与结果。企业还应当留存安全事件有关的事实、事件起因、相关影响以及采取的补救措施的相关记录，且相关网络日志至少要留存六个月的时间。这不仅是法律法规的要求，在监管机构介入并可能定性和判罚时，也将成为判罚的重要参考依据。

2.8 数据资产化解决方案

要想实现数据资产化，首先要做好数字资产化全生命周期管理。中国通信研究院发布的研究报告将数据资产化生命周期划分为确权—定价—交易—融资四个核心阶段。



定义：

1）确权：明确数据物权（财产权）、使用权、分法权等多方的权利形式和权利主体。

2）定价：通过成本法、市场法等方式，对数据的经济价值进行评估，兼顾评价数据产生的社会价值。

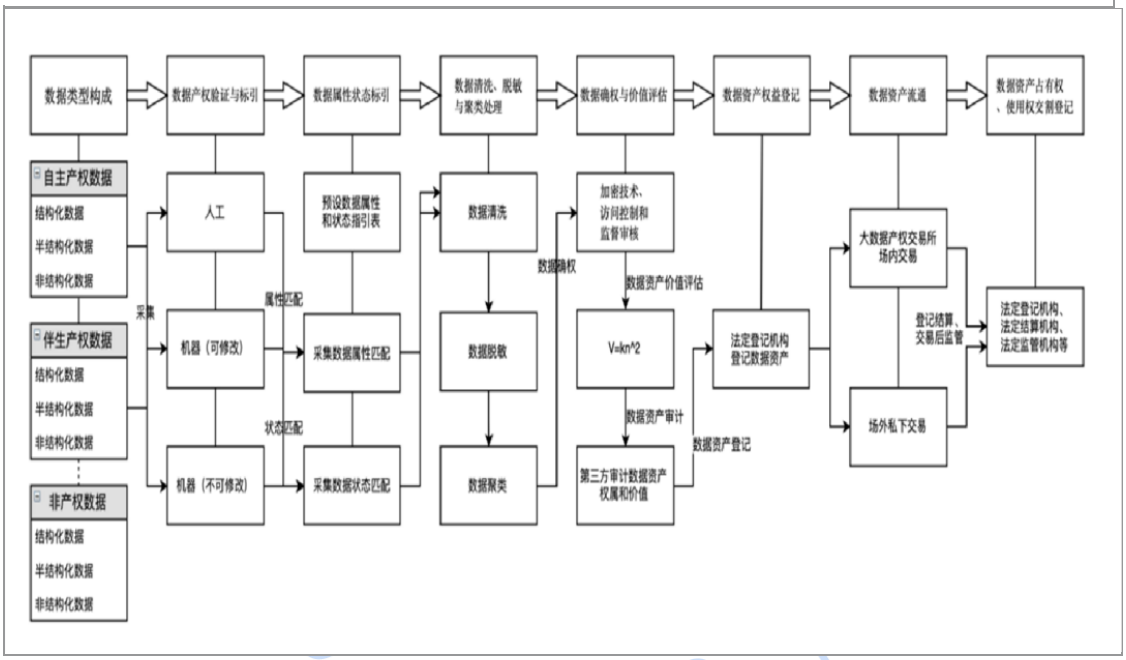
3）交易：对明确产权、确定价值的数据资产进行交易，交易可以通过区块链等方式进行追溯。

4) 融资：搭建数据资产密集型企业与金融机构、资本之间的桥梁，激活数据要素潜能。

企业数据资产化一般步骤：

数据资产化的生命周期划分为六个阶段：业务信息化—数据资源化—数据产品化—数据资产化—资产数据化—资产货币化。

阶段 / 维度	业务信息化	数据资源化	数据产品化	数据资产化	资产数据化	资产货币化
交易价值	/	内部信息	数据/计算能力	数据	资产	潜在收益
交易场所	业务流	内部决策	企业间	交易所	交易所	交易所
客户特征	企业内部	企业内部	上下游企业	所有企业	个人/企业	投资人/企业
交付物	/	数据/信息	产品或服务	数据	数字权益证明	远期收益合约
服务模式	软件 SaaS 技术导入	商业分析 预测与决策	数据租售 信息租售 数据产品 计算/存储等	资产租售 数据代收集 数据代存储	资产租售 资产金融服务 （抵押、担保、拆借等）	期货交易 数据资产租售 数据金融服务



当前数据要素成为推动经济增长和科技创新的重要引擎，赋能经济社会高质量发展的重要作用已经得到充分彰显。如何在厘清法律权属的基础上论证数据资产化，探索合理的数据定价和估值机制，推动数据在市场上进行有序交易，实现其市场化配置并释放价值，实现数据资产的保值和增值，进而实现数据要素的资本化是建设现代化经济体系，推动经济高质量发展的有益和必要的实践和探索。