零售企业数据安全合规管理指南
（意见征求稿）

中国百货商业协会

2023 年 07 月

版权声明

起草专家

刘知函，北京市盈科律师事务所高级合伙人

张　良，北京市盈科律师事务所律师

王秋杨，北京市盈科律师事务所律师

前言

数据作为新型生产要素，已成为国家重要资产和我国数字经济发展的基础战略资源。2021 年以来，国家、行业、地方相继颁布了大量数据安全政策文件。作为数字经济健康发展的重要基石，数据安全的重要性愈发突出，数据安全合规管理需求愈加明显。

零售企业的消费者数据、交易数据、商品数据规模庞大，近年来，消费者法律意识不断提升，国家相关监管机制也在不断完善，对零售企业存储、使用现有数据提出了很高的要求。与此同时，零售企业的数据治理理念和架构又相对传统，形成了数据量大、高要求和低治理水平之间的矛盾，处理不好可能会上升到司法层面的问题。

为此，中国百货商业协会联合知名律所北京市盈科律师事务所，结合企业反馈，起草《零售企业数据安全合规指南（征求意见稿）》，围绕数据合规目标、治理框架、治理实践路径展开论述。本指南结合司法实践，系统阐述了数据安全合规的相关管理要求，拟为企业开展数据相关工作提供有效指引。

目录

1.总则

1.1 为推动零售企业全面加强数据安全合规管理，规范零售企业数据处理活动，保障企业数据安全，促进企业健康发展，保护个人、组织的合法权益，维护国家经济安全和社会稳定，提升零售企业数据治理能力及数据安全保护水平，根据《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》《中华人民共和国电子商务法》《中华人民共和国消费者权益保护法》《数据出境安全评估办法》《网络交易监督管理办法》《中央企业合规管理办法》等有关法律法规规定，制定本指南。

1.2 本指南适用于百货商店、购物中心、奥特莱斯、大型超市、专卖店，日用工业品的零售、批发和生产企业等，以及上述企业的线上业态（以下称“零售企业”）。

1.3 中国百货商业协会负责协同其他监管单位，监督指导零售企业数据安全合规管理工作。

1.4 零售企业应当对本企业工作中收集和产生的数据和数据安全承担主体责任。

数据安全合规管理是合规管理体系的专项重点领域，已建立合规管理体系的零售企业，应在现有合规管理体系的基础上，进行专项深化管理。

数据安全风险较高的零售企业，必须将数据安全合规作为重点领域进行专项管理。达到以下条件之一的，视为数据安全风险较高：

A. 主要业务涉及个人信息处理，且从业人员规模大于 200 人；

B. 处理超过 100 万人的个人信息，或预计在 12 个月内处理超过 100 万人的个人信息；

C. 处理超过 10 万人的个人敏感信息的；

D. 自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的；

E. 法律法规规定的其他情形。

1.5 零售企业应当按照以下原则提升数据安全合规管理：

A. 高度重视。数据是重要的战略性资源，零售企业要将数据安全合规管理提升到事关国家安全、经济安全、社会稳定和人民群众切实合法权益的高度，始终把国家主权、安全、发展利益放在首位，加强安全能力建设，重视企业、员工、股东及合作方数据安全及个人信息保护，以发展促安全、以安全保发展。

B. 推进落实。零售企业要坚持将数据安全合规要求逐步覆盖各业务领域，各部门，各级全资、控股或实际控制的子企业、分支机构及其员工。数据应当全面包括电子或其他方式对信息的记录。数据安全合规管控措施及技术应用覆盖所有数据资产及数据处理全流程。

C. 强化责任。零售企业要切实加强对数据安全合规管理的组织领导，明确职责，建立健全分工负责、协作配合的工作机制，明确管理人员和各岗位员工的数据合规责任并督促有效落实。

D. 协同融合。零售企业认真贯彻落实数据安全合规的相关要求，将数据安全合规工作纳入企业数字化转型整体布局中，将数据安全合规管理通过企业数字化技术的应用及升级进行有效落地。

1.6 零售企业的数据安全合规管理建设应达到以下目标：

A. 满足合规要求。及时发现合规差距，全面履行数据安全责任义务，为业务的稳定运行和规范化开展筑牢根基。

B. 有效管理数据安全风险。不断产出的海量数据在动态实时流转过程中，面临着较大的风险暴露面，数据安全威胁及带来的影响与日俱增。叠加数据安全边界较为模糊、数据安全基础不够强韧等问题，零售企业数据安全风险的有效管理必然是数据安全合规管理的重要使命。

C. 逐步实现数据资产化。数字经济的高速发展离不开数据价值的充分释放，数据安全是保障数据价值释放的重要基石。数据安全合规管理通过体系化的建设，完善组织的合规管理和风险管理工作机制，提升数据安全保护水平，促进数据的开发利用，进而实现数据资产化。

2.数据安全合规管理规划

数据安全规划阶段主要确定零售企业数据安全合规管理工作的总体定位和愿景，根据企业整体发展战略内容，结合实际情况进行现状分析，制定数据安全规划，并对规划进行充分论证。

2.1 现状分析

零售企业应通过现状分析找到数据安全合规管理的核心诉求及差距项，以此作为规划设计的依据。可以从安全合规对标、风险现状分析对比入手。

一是数据安全合规对标。数据安全合规是企业履行数据安全相关责任义务的底线要求。零售企业应对企业适用的外部法律法规、监管要求、标准规范等进行梳理，将重要条款与现有情况进行对比，分析其差距，确定合规需求。

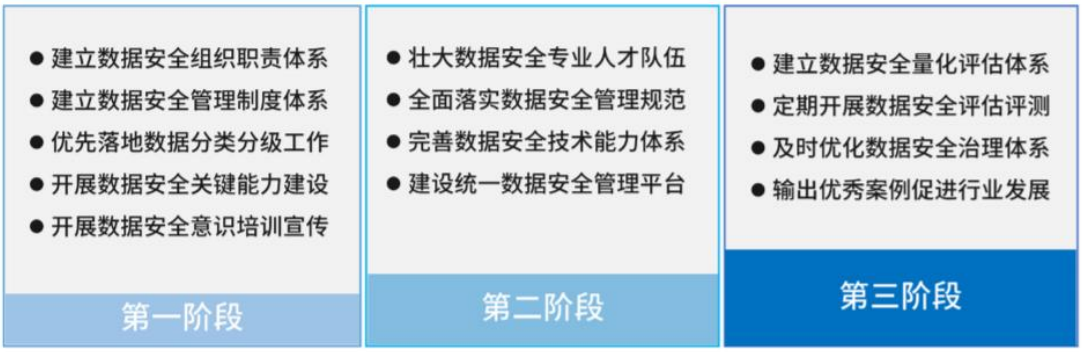
二是数据安全风险现状分析。有效的数据安全风险管理是企业推进业务发展的重要保障。零售企业需结合其业务场景，基于数据全生命周期安全防护要求，通过数据安全风险评估等方式识别数据面临的安全威胁及所在环境的脆弱性，形成风险问题清单，提炼数据安全建设需求点。

2.2 方案规划

零售企业应根据现状分析结果，结合数据安全合规管理目标，给出可落地实施的数据安全合规管理规划方案，并提炼重点目标和任务，分阶段落实到工程实施中。方案规划可以从组织架构、制度流程、技术工具和人员能力四个维度入手，通过不断建设与完善达成建设目标。

以一家数据安全合规管理建设刚起步的零售企业为例，一般来说，可以将数据安全规划分为三个阶段，如图 1 所示。

图 1：数据安全合规管理规划示例



来源：中国信息通信研究院数据安全推进计划

第一阶段，零售企业尚处于数据安全合规管理建设初期，急需在内部明确数据安全合规管理责任分工和管理要求，因而建议主要完成初步的数据安全合规管理体系建设工作，包括数据安全组织机构的建立、数据安全制度体系的编制、数据安全基础能力建设以及数据安全意识培训宣贯。同时数据分类分级作为实施数据安全管理措施和技术措施的前提，是一个需要提前布局且长期推进的工作。

第二阶段，零售企业有了一定的数据安全合规管理基础，可以在这一阶段着重完善数据安全技术能力体系，通过建设统一的管理平台，全面落实数据安全管理规范及策略要求，并通过常态化数据安全运营，实现持续的数据安全保障能力。同时，应加强数据安全能力培训体系的构建，培养复合型数据安全专业人才，壮大数据安全人才队伍。

第三阶段，零售企业已经初步建成数据安全合规管理体系，这一阶段以持续优化为主要目标，重在建立数据安全合规管理的量化评估体系，定期开展数据安全评估评测，监测各项指标的达标情况。再根据评估评测结果及时优化建设内容，最终达到较高的数据安全合规管理水平。同时，通过提炼并输出成功经验，促进行业共同进步。

2.3 方案论证

为保障规划方案在建设过程的顺利实施，应从以下方面进行论证分析。

一是可行性分析，根据组织现状，明确人力、物力、资金的投入与产生的效益对比，协调数据安全管理机制和技术能力建设与业务系统之间的分歧，确保在业务发展与安全保障之间达到平衡。

二是安全性分析，方案在正式实施前，要进行详细的方案论证分析，确保可以在业务稳定运行的前提下实施治理建设，同时要考虑治理过程中可能产生的新风险，避免未知风险的引入。

三是可持续性分析，数据安全合规管理是持续性过程，随着业务拓展和技术进步，规划方案在保证与当前组织现有体系兼容的同时，也要考虑与后续的发展相适应。因此数据安全合规管理方案不仅要考虑当下，还要着眼于未来。在满足当前数据安全需求的同时，还要适应后续的持续发展。

3.数据安全合规管理实践

3.1 零售企业涉及的消费者个人信息保护

3.1.1 通用要求

1) 处理消费者个人信息应遵循合法、正当、必要和诚信原则，具有明确、合理的目的并公开处理规则。
2) 收集个人信息，应先取得个人的同意，且限于实现处理目的的最小范围，不得过度收集个人信息。
3) 应采取必要措施保障所处理的个人信息的安全。
4) 不得以任何理由强制要求消费者同意个人信息处理行为，不得因消费者不同意提供非必要个人信息，而拒绝消费者使用其基本功能服务。
5) 应提供便捷的支持个人复制、更正、补充、限制处理、删除其个人信息、撤回授权同意以及注销账号的功能，且不得设置不合理条件。
6) 应该保证个人信息的遗忘权和修改权，个人有权要求删除相关的所有个人信息和更改个人的信息。如果因为技术限制不能删除，应该确认只应该存储个人信息而不能做任何其他用途。
7) 移动互联网应用程序（APP）使用第三方组件或 SDK 时，应避免其未经授权收集个人身份信息。

3.1.2 敏感个人信息的处理

敏感个人信息指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇的个人信息，包括消费者的银行账户、交易和消费记录、指纹/声纹/人脸等生物识别信息、身份证、通信记录和内容、通讯录、好友列表、群组列表、精准定位信息等。此外，14 岁以下（含）儿童的个人信息亦属于个人敏感信息。

3.1.2.1 敏感个人信息的收集

1) 应对处理敏感个人信息的合法性、必要性及正当性进行审查，重点排除非必要收集敏感个人信息的场景。原则上不应以改善服务质量、提升消费者体验以及研发新产品等为目的处理敏感个人信息。
2) 对于人脸、声纹或指纹等生物识别信息，应评估是否具有增加消费者利益的目的和充分的必要性，并应满足国家标准《信息安全技术 生物特征识别信息保护基本要求》（GB/T 40660-2021）。
3) 除 3.1.1 所列通用要求外，还应向消费者告知处理敏感个人信息的必要性以及对个人权益的影响。
4) 应对每项敏感个人信息取得消费者单独同意，不应一次性针对多项敏感个人信息或多种处理活动取得同意。取得单独同意时，不得将处理敏感个人信息的同意期限设置为“始终允许”或“永久”。
5) 使用人脸、声纹、指纹等生物识别或辨识技术时，应同时提供非生物识别的身份识别方式，不得因消费者不同意收集生物识别数据而拒绝其使用其基本业务功能。
6) 收集不满十四周岁未成年人个人信息的，应取得未成年人的父母或者其他监护人的同意。

3.1.2.2 敏感个人信息的存储

1) 敏感个人信息应依法在中国境内存储。
2) 应采取安全措施存储和传输敏感个人信息，包括但不限于加密存储和传输、采用物理或逻辑隔离方式分别存储敏感个人信息和其他数据等。

3.1.2.3 敏感个人信息的使用、加工

1) 建议对敏感个人信息进行匿名化或去标识化后，再进行处理。
2) 处理完成后，应立即删除过程数据。

3.1.3 个人信息处理规则（隐私政策）的制定

1) 零售企业处理消费者的个人信息，应当制定个人信息处理规则并严格遵守。个人信息处理规则的内容应明确具体、简明通俗，系统全面地向个人说明个人信息处理情况。
2) 个人信息处理规则应当集中公开展示、易于访问并置于醒目位置。如零售企业开发了 APP，则在进入 APP 主功能界面后，通过 4 次以内的点击，能够访问到个人信息处理规则，且链接位置突出、无遮挡。
3) 应制定专门的未成年人个人信息处理规则。

3.1.4 定期进行合规审计

零售企业作为个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

3.1.5 特定情形下需进行个人信息保护影响评估

当出现下列情形之一的，零售企业应当事前进行个人信息保护影响评估，并对处理情况进行记录，留存相关记录至少三年：

A. 处理敏感个人信息；
B. 利用个人信息进行自动化决策；
C. 委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；
D. 向境外提供个人信息（主要包括两种情形：一是运营者将在境内收集和产生的数据传输、存储至境外；二是运营者收集和产生的数据存储在境内，境外的机构、组织或者个人可以访问或者调用）；
E. 其他对个人权益有重大影响的个人信息处理活动。

3.2 数据安全组织建设

3.2.1 组织架构

1） 零售企业承担数据管理、信息系统管理或 IT 技术等部门和其他各职能部门分别作为各业务范围内数据安全合规管理的责任部门，作为数据安全合规管理的第一道防线，主要职责包括：

A. 制定企业数据管理的相关标准，包括数据分类分级、权限管理等工作；

B. 制定企业数据管理的相关制度及规范，包括数据全生命周期管理的相关制度；

C. 负责统一规范企业数据收集、存储、使用、加工、传输、提供、公开等工作机制；

D. 负责数据安全技术的应用及更新；

E. 负责数据管理能力建设；

F. 其他规章制度规定的数据管理工作。

2） 零售企业各职能部门负责本领域的日常数据安全合规管理工作，规范数据收集、存储、使用、加工、传输、提供、公开等工作，妥善应对数据安全合规风险事件，组织或配合进行违规问题调查并及时整改。

3） 零售企业合规管理牵头部门作为数据合规管理第二道防线，在数据安全合规管理方面的职责包括：

A. 参与对企业涉及数据安全事项的合规审查；

B. 对数据安全合规管理的情况进行评估与检查；

C. 组织或协助数据安全合规责任部门、人事部门开展数据安全合规培训，为公司其他部门提供数据安全合规咨询与支持；

D. 合规委员会或合规管理负责人交办的其他工作。

4）零售企业可视情况通过建立联合的数据合规管理办公室或工作组，开展数据安全合规管理标准、制度及规范的建立工作，可由相关业务、信息系统、技术、合规、风险管理、内部审计等部门人员组成，在经理层及合规管理负责人的领导下，有效推动数据安全合规管理工作的开展及实施。

5） 内部审计部门负责定期对数据安全进行审计，可根据风险评估和审计资源铺排，在审计工作中涵盖数据安全合规的内容，并出具相关审计报告，为企业数据安全风险管理的有效性提供合理保障。

3.2.2 授权和审批

零售企业在运营过程中，涉及账号、权限、介质、系统、软硬件等的申请、变更、新增、删除等重要行为时，应通过相关授权和审批过程进行：

A. 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；

B. 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程；

C. 应针对数据处理的权限管理，建立适当的用户权限管理机制，根据岗位设置相关账户权限，明确相关数据所涉及的账户管理流程，减少数据滥用情况；

D. 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

3.2.3 数据安全管理人员

1） 应对安全管理机构的负责人和关键岗位的人员进行安全背景审查和安全技能考核，符合要求的人员方能录用。关键岗位的范围由安全管理机构明确，通常包括与关键业务系统直接相关的系统管理、网络管理、数据管理等岗位。关键岗位应配备专人，并配备 2 人以上共同管理。

2） 应与被录用人员签署劳动合同、保密协议，与关键岗位人员应另签署岗位责任协议。

3） 应制定网络与数据安全管理相关岗位人员培训计划，进行安全意识教育和岗位技能培训，并告知相关的安全责任和问责机制。

4） 建立人力资源考核制度，明确网络与数据安全管理考核指标和问责机制，对相关人员特别是关键岗位人员的履职情况进行考核。

5） 出现网络与数据安全重大事件时，对直接负责的主管人员和其他直接责任人员进行问责。

6） 应在安全管理人员调岗时，及时修改访问权限并通知相关人员或角色。应在

人员离岗时，及时终止其所有访问权限，收回与身份鉴别相关的软硬件设备，进行面谈并通知相关人员或角色。

3.3 数据安全管理制度

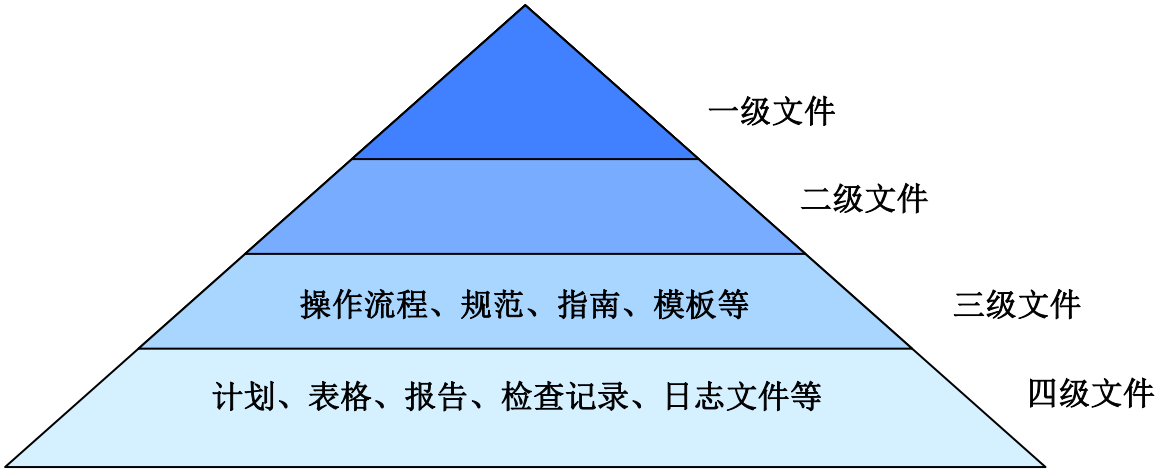
3.3.1 制定安全策略

应制定数据安全工作的总体方针和安全策略，阐明安全工作的总体目标、范围、原则和安全框架等。

3.3.2 建立数据安全管理制度体系

1) 应对安全管理活动中的各类管理内容建立安全管理制度。
2) 对管理人员或操作人员执行的日常管理操作建立操作规程。
3) 形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。常见的制度体系如图 2 所示：

图 2 数据安全制度体系层级



3.3.3 制定和发布

1) 指定或授权专门的部门或人员负责安全管理制度的制定。
2) 由零售企业的数据安全领导小组签署并发布相关文件。

3） 文件发布后应组织宣贯与教育。

3.3.4 评审和修订

1） 文件应定期（建议 1 年）或当组织发生重大变更时，执行修订工作。

2） 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

3） 在修订完成后，应通过文件控制程序，记录版本变更。

3.4 数据资产盘点

数据资产盘点是数据分类分级的基础，本阶段需要对零售企业内的全部数据资源进行识别、梳理，明确当前企业内部存储了哪些数据、数据存储的格式、数据范围、数据流转形式、数据访问控制方式、数据价值高低等问题，并形成数据资源清单。

3.4.1 盘点范畴

零售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。

示例：数据资产盘点范围涵括 18 类数据资源，如表 1。

表 1：数据资产盘点范围示例

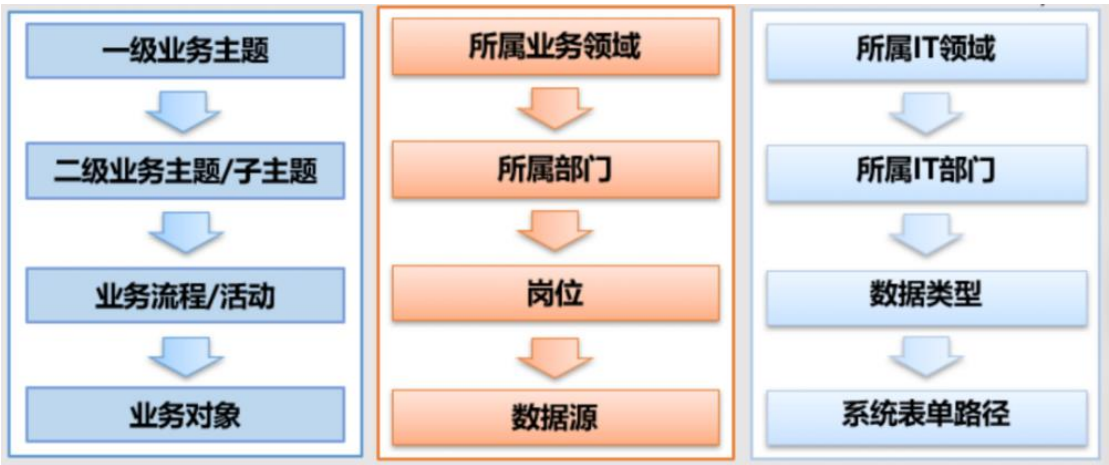
业务类	1.0 集成产品开发（IPD）
	2.0 从市场到线索（MTL）
	3.0 渠道销售（CS）
	4.0 零售（Retail）
	5.0 从商机到回款（OTC）
	6.0 从问题到解决（ITR）
使能类	7.0 从战略到执行（DSTE）
	8.0 资本运作管理（CIM）
	9.0 集成供应链（ISC）
	10.0 采购管理（PM）

	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）

3.4.2 盘点方法和过程

数据资产盘点要围绕零售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（图 3）：

图 3 数据资产盘点流程图



A. 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；

B. 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；

C. 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；

D. 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；

E. 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；

F. 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。

3.5 数据分类分级

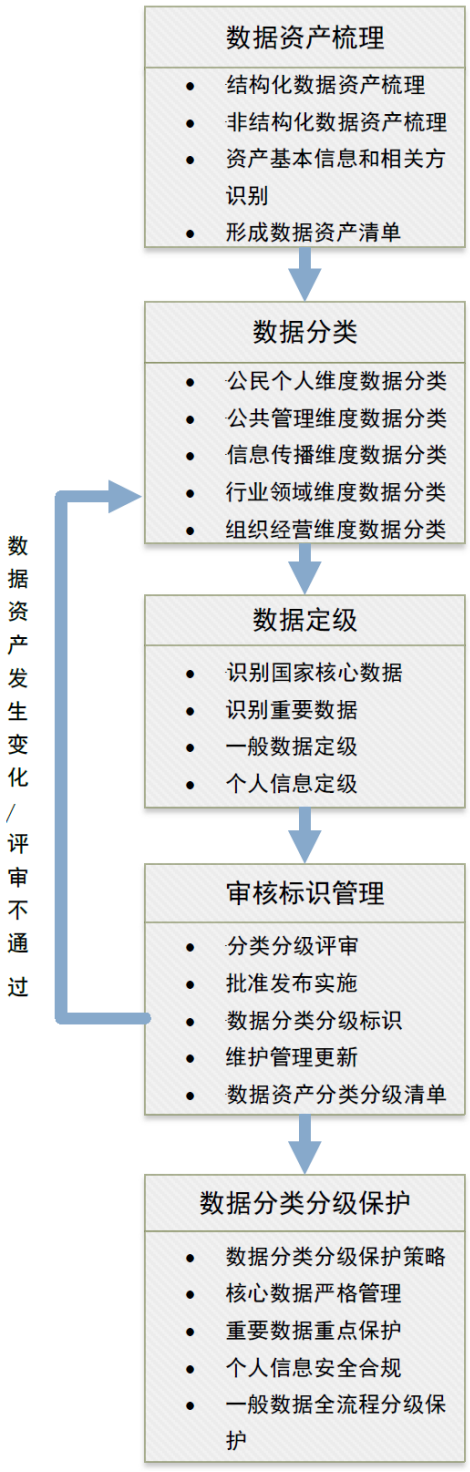
数据分类分级是指从业务领域或数据管理领域的角度出发，将相同属性或特征的数据进行集合并形成不同的数据类别，并在分类的基础上， 根据数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用后对国家安全、公共利益、个人合法权益、组织合法权益的影响及其危害程度将数据分级，最后针对不同级别的数据采取相匹配的保护措施。

由于零售行业尚未发布专门的数据分类分级相关规范，本指南主要参考TC260-PG-2-212A《网络安全标准实践指引——网络数据分类分级指引》的相关内容。

3.5.1 数据分类分级实施流程

按照《网络数据分类分级指引》，数据处理者在开展数据分类分级时，可按照图 4 所示流程实施。

图 4：数据分类分级实施流程



具体到零售企业，数据分类分级的一般流程可分为：

A. 数据资产盘点：详见本指南 3.4 的内容；

B. 数据分类：零售企业主要可以从公民个人维度和组织经营维度等视角给出数据分类框架。公民个人维度即按照数据是否可识别自然人或与自然人关联，将数据分为个人信息和非个人信息两大类。组织经营维度：如可分为用户数

据、业务数据、经营管理数据、系统运行和安全数据等；

C. 数据分级：建立自身的数据分级规则，并对数据进行定级；

D. 审核标识管理：对数据资产分类分级结果进行评审和完善，最后批准发布实施，形成数据资产分类分级清单。并对数据资产和数据分类分级进行维护、管理和定期审核；

E. 数据分类分级保护：依据国家给出的关于核心数据、重要数据、个人信息、公共数据等安全要求，以及行业领域给出的数据分类分级保护要求，建立数据分类分级保护策略，按照核心数据严格管理、重要数据重点保护、个人信息安全合规和一般数据分级保护的思路，对数据实施全流程分类分级管理和保护。

3.5.2 数据分级框架

按照《数据安全法》要求，根据数据一旦遭到篡改、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、组织合法权益造成的危害程度，将数据从低到高分成**一般数据、重要数据、核心数据**共三个级别。

上述三个级别是从国家数据安全角度给出的数据分级**基本框架**。由于一般数据涵盖数据范围较广，采用同一安全级别保护可能无法满足不同数据的安全需求。因此建议零售企业在基本框架定级的基础上，再结合生产经营需求，对一般数据进行细化分级，并给出一般数据分级的参考规则（表 2）。

表 2 一般数据分级规则

安全级别	影响对象	
	个人合法权益	组织合法权益
4 级数据	严重危害	严重危害
3 级数据	一般危害	一般危害
2 级数据	轻微危害	轻微危害
1 级数据	无危害	无危害

来源：《网络安全标准实践指引——网络数据分类分级指引》

1 级数据：数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，不会对个人合法权益、企业合法权益造成危害。1 级数据具有公共传播属性，可对外公开发布、转发传播，但也需考虑公开的数据量及类别，避免由于类别较多或者数量过大被用于关联分析。

2 级数据：数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、企业合法权益造成轻微危害。2 级数据通常在企业内部、关联方共享和使用，相关方授权后可向企业外部共享。

3 级数据：数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、企业合法权益造成一般危害。3 级数据仅能由授权的内部机构或人员访问，如果要将数据共享到外部，需要满足相关条件并获得相关方的授权。

4 级数据：数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、企业合法权益造成严重危害，但不会危害国家安全或公共利益。4 级数据按照批准的授权列表严格管理，仅能在受控范围内经过严格审批、评估后才可共享或传播。

3.6 零售企业数据全生命周期保护要求

3.6.1 数据收集安全

1) 明确数据收集过程中个人信息和重要数据的知悉范围和安全管控措施，确保收集数据的合规性、完整性和真实性。
2) 收集的消费者数据应与企业提供的产品或服务直接相关，并与合同协议条款、隐私政策中约定收集的内容保持一致，不应超范围收集数据。
3) 通过系统批量收集数据时，应采用摘要、消息认证码、数字签名等密码技术确保收集过程数据的完整性。
4) 应对数据收集过程进行日志记录，并采取技术措施确保信息来源的可追溯性。

3.6.2 数据传输安全

1) 涉及数据传输的相关人员应记录时间、传输数据、数据接收方等相关信息，以作为数据传输记录备案。
2) 技术手段上应对传输过程的通信双方进行身份认证，确保数据传输双方是可信任的；采用安全、可靠的加密协议，对通信信道进行安全加密；采用密码技术或非密码技术等方式，确保数据的完整性；选用安全的密码算法，确保数据的安全性。

3) 向国家机关、行业主管和监管单位传输数据，应按照国家及行业相关管理要求进行传输。

3.6.3 数据存储安全

1) 应依据最小够用原则存储数据，针对不同类型的数据设定数据存储期，存储时间应为业务必需的最短时间，对于多个不同存储期数据的集合，保存期限选择最长时限为该数据集合的保存期，不应以任何形式存储非业务必需的数据，国家及行业主管部门另有规定的除外，且数据存储不应因其存储形式或存储时效的改变而降低安全保护强度。
2) 相关人员应定期对数据存储过程中可能产生的影响进行风险评估，并采取相应安全防护措施。
3) 应对数据存储区域进行规划，并对不同区域之间的数据流动进行安全管控。
4) 对于高敏感级别数据，应采用密码技术、权限控制等技术措施保证数据完整性，同时应采取加密等技术措施保证数据存储的保密性。
5) 根据数据分类分级和数据对系统运行的影响，制定数据备份策略和恢复策略，备份策略应至少指明备份数据的放置场所、文件命名规则、介质替换频率、备份周期或频率、备份范围等。
6) 应定期开展灾难恢复演练，应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果。
7) 数据备份应基于多冗余策略，可采用磁带、磁盘镜像、磁盘冷备、热备、双活等技术实现，备份频度及保存期限不低于相关监管和业务使用要求。

3.6.4 数据使用、加工安全

1) 梳理数据提供使用的各类场景，明确各类场景的安全要求和责任部门，并建立相应的审核批准机制，对数据使用目的、内容、使用时间、技术防护措施、数据使用后的处置方式等进行审批，并留存相关记录。
2) 应明确原始数据在数据加工过程中的数据获取方式、访问接口、授权机制、逻辑安全、处理结果安全等内容。

3) 在数据加工之前应进行数据安全影响评估，并采用加密、脱敏等技术措施，保证数据加工过程的数据安全性。

4) 应根据数据的不同安全级别，执行数据访问控制过程中的相关安全措施，保障数据在被访问过程中的保密性和完整性，包括但不限于身份认证、多因素认证、二次授权等。

5) 利用自动化工具如代码、脚本、接口、算法模型、软件开发工具包等提供数据时，应通过身份认证、数据加密、反爬虫机制、攻击防护和流量监控等手段，有效防范网络监听、接口滥用等网络攻击，并定期检查和评估自动化工具安全性和可靠性。

3.6.5 数据交换和共享安全

1) 加强数据开放及共享的管理，根据数据使用目的、共享对象，明确数据可进行开放及共享的范围，建立数据共享的申请及授权审批的流程及权限设置，明确数据共享过程的传输方式。

2) 针对企业向外部单位共享数据的情况，零售企业应充分评估相关数据安全风险，涉及重大敏感的数据提供要按审批权限逐级审批。并在相关合同中明确数据安全及保密义务，明确相关违约责任，必要时可单独签订保密协议。相关事项结束后，应进行内部总结汇报，对数据共享情况进行说明，加强数据共享的管理。

3.6.6 数据出境安全

1) 零售企业应梳理数据出境情况的业务，建立企业内部数据出境合规审查的流程及规范，针对境外并购、赴境外上市等情况，应充分评估数据出境的相关风险，按相关规定进行内部审核审批，并根据法律法规要求，履行监管机构数据出境的审查申报。非经相关部门批准，不得向外国司法或执法机构提供存储于中华人民共和国境内的数据。

2) 零售企业境外分支机构在当地设立服务器，并通过该服务器储存及使用监管企业数据的，应按数据出境的管理要求实施数据安全管理。境外分支机构通

过远程访问使用数据的，应加强访问权限控制及数据传输安全管理，确保数据安全。

3.6.7 数据销毁安全

1) 应制定数据存储介质销毁操作规程，明确数据存储介质销毁场景、销毁技术措施，以及销毁过程的安全管理要求，并对已提供或者已被使用的数据提出有针对性的数据存储介质销毁管控规程。
2) 存储数据的介质如不再使用，应采用不可恢复的方式如消磁、焚烧、粉碎等对介质进行销毁处理。存储介质如需继续使用，不应只采用删除索引、删除文件系统的方式进行数据销毁，应通过多次覆写等方式安全地擦除数据，确保介质中的数据不可再被恢复或者以其他形式被利用。
3) 应定期对数据销毁效果进行抽样认定，通过数据恢复工具或数据发现工具进行数据的尝试恢复及检查，验证结果。

3.7 算法合规管理要求

1) 提供算法推荐服务，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。
2) 应当落实算法安全主体责任，建立健全算法机制机理审核、科技伦理审查、用户注册、信息发布审核、数据安全和个人信息保护、反电信网络诈骗、安全评估监测、安全事件应急处置等管理制度和技术措施，制定并公开算法推荐服务相关规则，配备与算法推荐服务规模相适应的专业人员和技术支撑。
3) 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，不得设置诱导用户沉迷、过度消费等违反法律法规或者违背伦理道德的算法模型。
4) 应当加强用户模型和用户标签管理，完善记入用户模型的兴趣点规则和用户标签管理规则，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。
5) 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。应当保护消费者合法权益，不得根据消费者的

偏好，交易习惯等特征，利用算法在交易价格等交易条件上实行不合理的差别待遇等违法行为。

6) 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。

7) 应当制定并公开算法推荐相关服务规则，以显著方式告知消费者，其提供算法推荐服务的情况，并以适当方式公布算法推荐服务的基本原理、目的意图、运行机制等。

8) 对拥有大量用户以至于具有舆论属性或者社会动员能力的算法推荐服务企业，应当按照国家有关规定开展安全评估。

9) 应当向消费者提供不针对其个人特征的选项，或者向消费者提供便捷的关闭算法推荐服务的选项。消费者选择关闭算法推荐服务的，零售企业应当立即停止提供相关服务。

10) 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 6 个月。

3.8 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。因此，零售企业应当建立数据安全事件应急处置机制，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等，并在发生数据安全事件时，立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

3.8.1 制定应急预案

1）建立应急预案，主要内容包括：启动应急预案的条件；启动应急预案所需的资源，如人员、设备、场所、工具、资金等；应包含非常规时期、遭受大规模攻击时的应急处置流程；事件报告流程；系统恢复流程；事后教育和培训等。

2）配备应急响应所需的资源，确保应急预案能够有效实施。

3）在制定应急预案时，应同所涉及的运营者内部相关计划（如业务持续性计划、灾难备份计划等）以及外部服务提供者的应急计划进行协调，以确保连续性要求得以满足。

4）应对应急预案定期进行评估修订，并持续改进。

3.8.2 制定应急演练计划

每年至少组织一次应急演练。在应急预案发生变化后，应及时组织开展应急演练，检查和完善应急响应机制，提高实战能力。

3.8.3 安全事件的报告

1）发生个人信息和数据泄露、毁损、丢失等安全事件和网络系统遭攻击、入侵、控制等网络安全事件，或者发现网络存在漏洞隐患、网络安全风险明显增大时，零售企业应立即启动应急预案，采取必要的补救和处置措施，及时以电话、短信、邮件或信函等多种方式告知相关主体。

2）零售企业应迅速确定如下内容：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；上报哪个/哪些监管机构，是否包括域外的监管机构；需要通知的数据主体的范围以及通知的方式；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。

3.8.4 事件取证小组及职责

1） 应建立安全事件的取证小组，成员应至少包含安全部门、人力资源部门以及法务部门相关人员，同时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） 事件取证小组负责对安全事件进行定级，分析和描述事件产生的原因，收集证据，记录处理过程，总结经验教训，并确定事件责任方和责任人，按照制度要求实施处罚措施。

3.8.5 做好安全事件记录

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，零售企业都应当做好安全事件的记录，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。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。

——完——