数据安全法解读系列（三）
数据分类分级迫在眉睫

（来源：安永微信公众号，2021-07-21）

序言

2021 年 6 月 10 日，《中华人民共和国数据安全法》已由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议正式通过，并将于 2021 年 9 月 1 日正式施行。

一、数据安全法核心内容解读

《中华人民共和国数据安全法》是我国继《中华人民共和国网络安全法》之后，在数据安全领域又一基础性法律，对于国家数据安全和数字经济的发展具有举足轻重的意义。纵观《数据安全法》全文，以下十大核心内容尤其值得企业关注：

1.域外适用性

《数据安全法》第二条指出对于在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

2.明确各方数据安全职责

《数据安全法》第六条明确了国家各个层级对数据安全的职责定位，建立起数据安全协同治理体系，加强为推动各地区、各部门开展数据安全工作奠定基础。同时，《数据安全法》明确指出各行业监管、公安机关、国家安全机关、国家网信部门在各自职责范围内，承担数据安全监管职责，统筹协调网络数据安全和相关监管工作。

3.鼓励数据开发与利用

国家实施大数据战略，鼓励和支持数据在各行业、各领域的创新应用，将数字经济发展纳入国民经济和社会发展规划，并根据需要制定数字经济发展规划。根据《数据安全法》第十三至十七条，国家提倡数据的开发和利用旨在提升公共服务的智能化水平，充分考虑老年人、残疾人的需求，鼓励技术推广和商业创新、国家相关组织制定并适时修订有关数据开发利用技术、产品和数据安全的相关标准。

4.开展数据安全检测评估工作

国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制，并对影响或者可能影响国家安全的数据处理活动进行国家安全审查。（第十八条、第二十二条、第二十四条）

5.建立数据安全应急处置机制

根据《数据安全法》第二十三条，国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

6.健全和维护数据交易管理秩序

《数据安全法》第十九条指出，国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。可以预见今后国家会陆续出台更多数据交易相关管理要求，规范数据交易市场秩序。

7.建立数据分类分级保护制度

根据《数据安全法》第二十一条，国家建立数据分类分级保护制

度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏或者非法获取、非法利用，对国家安全、公共利益或者公民、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护，各地区、各部门按照数据分类分级保护制度，对本地区、本部门及相关行业、领域的重要数据开展重点保护工作。对于关系国家安全、国民经济命脉、重要民生、重大公共利益等核心数据，实行更加严格的管理制度。

8.开展数据出口管制和反制裁措施

根据《数据安全法》第二十五条、第二十六条国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制，对任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，将根据实际情况对该国家或者地区对等采取措施。

9.履行数据安全保护的义务

企业开展数据处理活动应当依照法律、法规的规定健全数据安全管理制度、开展数据安全教育培训、采取必要的数据安全保障技术措施、加强数据风险监测和评估、及时应对和上报数据安全事件、合法正当收集和使用数据，不得超过必要限度、在网络安全等级保护制度基础上履行数据安全保护义务等。（第二十七条至第三十二条）

10.更加严苛的法律责任惩戒力度

基于不同违反数据安全法的场景，《数据安全法》细化了违法责任，其中针对最为严重情节，将由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关

业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。（第四十四条至第五十二条）

二、数据分类分级工作是基础和核心

《数据安全法》中不仅强调了国家各个层级关于数据安全的职责定位、战略方针和审查要求，同时也鼓励各行业企业依法开展包括数据分类分级、数据出口管制、应急处置机制、安全事件上报、风险监测评估、系统等级保护等数据安全保障工作。

而《数据安全法》第二十一条中提出的国家建立数据分类分级保护制度，作为《数据安全法》第三章的国家数据安全基本制度的总起段落，首先提出了对数据进行分类分级的要求，并紧接着定义了重要数据保护目录以及国家核心数据两大重要概念，不难看出我国推行的数据安全制度将围绕着数据分类分级制度展开，或者说建立数据分类分级保护制度是我国整个数据安全制度的基础和首要工作。

《数据安全法》中重要数据目录的制定是根据其在经济社会发展中的重要程度，以及一旦遭到篡改、破坏或者非法获取、非法利用，对国家安全、公共利益或者公民、组织合法权益造成的危害程度，由国家数据安全工作协调机制统筹协调有关部门制定重要数据目录；关系国家安全、国民经济命脉、重要民生、重大公共利益的数据则被认定为国家核心数据。国家核心数据这一概念是《数据安全法》首次提出的数据类型，也是从国家法律法规层面对数据分类的进一步细分。

目前国家有关部门还尚未明确重要数据的具体判定标准，重要数据目录也尚未出台，对于大多数的企业而言尚且无法鉴别其业务开展过程中是否包含重要数据和核心数据，缺乏国家明确的数据分类分级保护制度的指引来开展和落实相关工作。其实，数据分类分级这一要求早前已在多项法律法规和行业标准中有所体现：

《网络安全法》第二十一条“（四）采取数据分类、重要数据备份和加密等措施”；

《数据安全管理办法（征求意见稿）》第十九条“网络运营者应当参照国家有关标准，采用数据分类、备份、加密等措施加强对个人信息和重要数据保护”；

《工业数据分类分级指南（试行）》第五条“工业企业结合生产制造模式、平台企业结合服务运营模式，分析梳理业务流程和系统设备，考虑行业要求、业务规模、数据复杂程度等实际情况，对工业数据进行分类梳理和标识，形成企业工业数据分类清单”；

《证券期货业数据分类分级指引》(JR/T 0158—2018)给出了证券期货业数据分类分级方法概述及数据分类分级方法的具体描述，并就数据分类分级中的关键问题处理给出建议；

《金融数据安全数据安全分级指南》（JR/T 0197—2020）提出了金融数据安全分级的目标、原则和范围，明确了数据安全定级的要素、规则和定级过程，并给出了金融业机构典型数据定级规则供实践参考；**《个人金融信息保护技术规范》**（JR/T 0171-2020）将个人金融信息按照敏感程度分为三大类，规定了个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求。

可以看出《网络安全法》《数据安全管理办法》中已明确提出数据分类分级的合规要求，且工业和金融行业监管已经制定了相关的配套法律法规。企业应当根据自身的行业特性，基于企业自身需求，参考上述法律法规要求与行业监管要求，开展企业层面的数据分类分级工作。

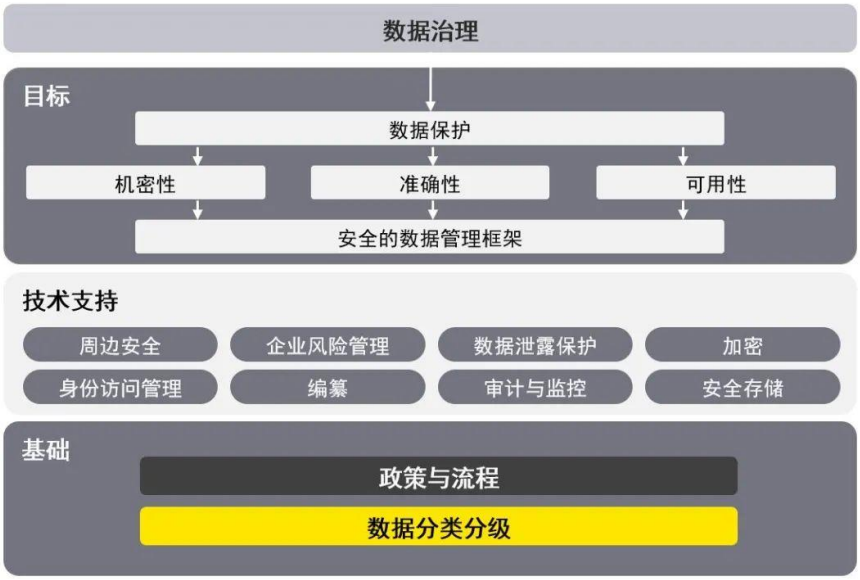
三、企业数据分类分级合规实践

安永观点

随着《数据安全法》的出台，我国的数据安全体系将以数据分类分级为基础展开。事实上，许多大型的跨国组织在企业内部已经基于ISO信息安全体系框架建立了一套数据分类分级制度。

那么，开展企业内部的数据分类分级，对企业信息安全与数据安全有什么基础性的帮助呢？首先，数据分类是数据治理和信息生命周期管理的基础，通过对企业内部的数据全生命周期的盘点梳理，可以帮助确定企业数据所有权的适当分配和建立完善的问责制度，满足监管及合规要求；其次，根据梳理的数据资产对企业的重要程度（比如敏感性和关键性），为数据打上不同的标签，对敏感数据进行分级，根据数据所属的级别，一目了然哪些数据可以使用、哪些不可以使用、哪些能对外开放、哪些不能开放、不同等级的数据在不同场景使用哪

种安全策略，可以考虑采取技术方法（比如数据泄露防护、加密、企业权限管理等），对机密信息提供进一步的保护，从而降低数据泄露带来的风险；不仅如此，企业内部建立完善的数据分类分级制度，还可以帮助员工增强数据安全意识，从而降低未经授权使用信息资产的风险。



那么，企业要想开展数据分类分级工作，具体应该如何开展呢？基于安永多年的行业经验和领先实践，主要分为三个阶段：

1. 数据识别与分类分级

首先，企业应制定数据分类分级的管理制度，其中包括分类分级的规则与标准，以及数据分类分级的填写模板，然后对企业员工进行数据分类分级的相关培训。基于数据在业务场景与运营管理中的处理活动，识别出存储在不同地方的数据信息，以及它们如何被传输与使用的。培训应该针对不同的对象分别开展，一个是针对业务部门员工进行非结构化数据的数据分类分级的培训，另外是对 IT 及系统负责人进行系统的数据分类分级培训。培训完成之后，分发并收集数据分类分级的模板，各部门填写完成后，收集汇总数据清单。

2.数据分类分级安全保护策略梳理

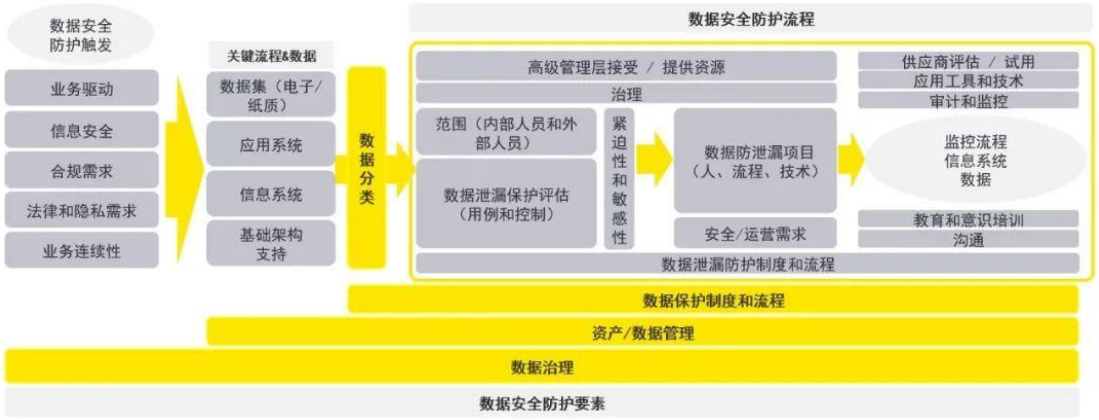
经过梳理和汇总形成数据清单之后，企业应根据数据的属性对数据进行分类，根据数据对企业业务的重要程度对数据进行分级，并按照不同的级别打上相应的标签，如公开、内部、机密、绝密等，标签应明确其格式和适用范围。对于不同级别的数据，企业应制定相应的数据保护要求，如采取不同级别的数据加密手段，以及制定不同的数据备份策略等。对于被判定为机密、绝密数据的信息，企业应厘清其使用及应用场景，并单独制定机密、绝密数据的安全保护策略，明确机密、绝密数据的使用、传输和存储规则及保护要求。

3.数据分类分级保护整体规划设计与速赢措施

根据数据分类分级安全保护策略，企业应对数据分类分级保护制定整体规划设计，建立数据安全防护流程，明确数据安全责任人，落实不同数据分类分级的保护措施，并应通过数据保护管控评估矩阵对数据安全保护的落实情况进行监控。

为了更有效的保护企业机密、绝密数据，企业应针对机密、绝密数据的保护应单独制定培训材料，并定期对员工开展培训以确保员工了解自身在机密、绝密数据保护方面的责任，如机密、绝密数据不允许通过电子邮件发送，打印、传真或者复印不应留下文档，对于生成或者存储机密、绝密信息的硬件设备和软件维护只能由经过授权的员工完成等。同时，企业应制定与之相配套的纪律处分规则，并通过意识宣贯确保员工知悉不遵守企业数据分类分级策略的后果。

企业还应部署数据标签工具，实现数据批量标签管理的自动化，严格管理企业机密、绝密数据使用、传输和存储，及时发现违反企业数据分类分级策略的行为，并提出警告。



综上，参照现在国内的法律法规环境，数据分类分级工作的重要性不言而喻。开展数据分类分级工作，企业除了可以满足合规监管要求，更可以提升自身信息化水平和运营能力。数据分类分级是管理体系合理规划、数据安全合理管控、人员精力及力度合理利用的基础，是迈向数据安全精细化管理的重要一步。

原文链接：https://mp.weixin.qq.com/s/jiEEoD-H_Mjcd6bMXF_gkg ，转载请注明。