

## “数据分类分级保护”背景下的企业合规

### 以国家和公共利益为视角依法合规运用数据

本报记者 任文岱

数据分类分级保护制度是开展数据安全治理的基础，也是促进数据充分利用、有序流动和安全共享的重要前提。企业应严格按照国家重要数据目录和本地区、行业监管部门制定的重要数据具体目录对重要数据加强保护。其他数据，可参考既有法律法规，开展适合自身的、行之有效的数据分类分级。

《中华人民共和国数据安全法》第二十一条明确规定，“国家建立数据分类分级保护制度”。2022年1月，国务院办公厅印发《要素市场化配置综合改革试点总体方案》提出，探索建立数据要素流通规则，要探索“原始数据不出域、数据可用不可见”的交易范式，在保护个人隐私和确保数据安全的前提下，分级分类、分步有序推动部分领域数据流通应用；要强化网络安全等级保护，推动完善数据分级分类安全保护制度。

2021年底，全国信息安全标准化技术委员会发布《网络安全标准实践指南——网络数据分类分级指引》（以下简称《指引》），明确了网络数据分类分级的原则、框架和方法，用于指导数据处理者开展数据分类分级工作。

当前，已有不少部门、地方政府出台了相关领域、行业数据分类分级保护规定。比如，今年2月1日起，根据《江苏省公共数据管理办法》，江苏对公共数据将依法实行分类分级保护。上海、浙江、福建、重庆等地也出台了公共数据开放分级分类试行指南。此外，中国人民银行于2020年9月发布《金融数据安全 数据安全分级指南》；工业和信息化部于2021年9月发布《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》，在第二章专门规定“数据分类分级管理”。

近两年来，“数据分类分级保护”已成为数据安全领域的高频词。数据分类分级保护对数据安全有何影响？企业如何才能让数据分类分级合规有序落地？近日，民主与法制社记者就此采访了相关专家学者。

#### 开展数据安全治理的基础

数据安全法第三章“数据安全制度”部分规定，国家建立数据分类分级保护制度、数据安全审查制度、数据安全应急处置机制等。上海大学法学院大数据与人工智能法治研究中心执行主任陈吉栋认为，数据分类分级保护制度是开展数据安全治理的基础，也是促进数据充分利用、有序流动和安全共享的重要前提。

陈吉栋表示，从数字经济发展角度看，数据的流通利用是实现数据资源价值的必然路径，由此才能形成数字经济。“复杂多样的业务场景，使工业数据呈现出时序、非时序、结构化、非结构化等多种形式，这些数据在承载信息、应用领域、重要程度等方面各不相同。可以说，数据流通过程复杂，且涉及主体多样。”

陈吉栋进一步解释，具体来讲，工业数据在企业内部研发、生产、运营维护、管理等环节之间互通，在上下游企业间、平台间流转，涉及设备厂商、工业企业、平台企业、服务商等相关方。因此，在数据流向跟踪、风险定位、责任追溯等方面，数据管理者面临着不小的压力。

数据流通包括数据的开放、共享、互换、交易。因为数据的形态种类繁多，数据的价值各不相同，所以只有通过合理安排不同数据的流通方式和规则，为数据开发利用主体提供开展合规数据流通的行动依据，对数据进行分类分级，才能最大限度地释放数据的价值。

中央财经大学法学院副教授刘权表示，对数据进行科学合理分类分级，有利于保障数据要素有序自由流动，实现数据要素市场有效配置，发展壮大数字经济。

“不同类型和级别的数据在不同场景下，安全级别不同，安全防护措施也应当不同。数据分类分级的目的是为了保护数据安全，不同类型和级别的数据应采取不同的保护措施。对数据进行分类分级，有利于更好地保护数据。”刘权说。

陈吉栋以数据交易为例称，数据交易应当在充分衡量数据安全级别基础上进行。只有充分考虑数据本身的复杂性、多样性及其可能的影响范围和影响程度，并结合不同行业数据安全治理现状及其在具体业务层面的数据安全分级指南，才能依法有序进行合规的数据交易实践。

#### 数据分类分级保护的标准

数据安全法第二十一条对数据分类分级提出了具体要求。刘权表示，该条提出了数据分类分级的两大标准：一是根据数据在经济社会发展中的重要程度进行分类分级；二是根据一旦遭到篡改、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分类分级。简而言之，我国根据数据“重要程度”和受侵犯后的“危害程度”，对数据进行分类分级。

陈吉栋认为，目前，我国数据分类分级主要按照数据分类管理、分级保护的思路，遵循自上而下的路径，优先遵循国家、行业的数据分类要求。在此基础上，数据处理者还可按照组织经营维度进行数据分类，包括用户数据、业务数据、经营管理数据、系统运行和安全数据等。

陈吉栋表示，依照数据安全法第二十一条的规定，根据对国家、社会的经济价值以及出现安全事件后造成的危害程度，将数据分为一般数据、重要数据、国家核心数据，并由此对其适配不同程度的安全保护规则。

数据安全法第二十一条还规定，各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。刘权认为，由于数据种类繁多，不同地区、行业的数据差别大，所以我国并没有在国家层面对所有数据进行统一分类分级。

给数据分类分级具体要遵循什么样的标准？全国信息安全标准化技术委员会发布的《指引》明确，数据分类分级应按照数据分类管理、分级保护思路，依据合法合规、分类多维、分级明确、就高从严、动态调整等多项原则进行划分。

陈吉栋表示，在数据分类上，《指引》从国家、行业、组织等多种维度进行划分，同时把一定主动权给予数据处理者，建议再做进一步细分，并给出了具体参考。例如《指引》从公民个人维度划分，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。如果个人信息通过去标识化等处理后，达到无法识别特定自然人且不能复原的匿名化效果，那么处理后的信息不再属于个人信息，这与《中华人民共和国个人信息保护法》第四条的规定一致。

刘权表示，《指引》主要从数据安全保护角度出发，从影响对象、影响程度这两个要素进行分级。影响对象是指，数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用后受到危害影响的对象，包括国家安全、公共利益、个人合法权益、组织合法权益。影响程度是指，数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用后，所造成的危害影响大小。危害程度从低到高可分为轻微危害、一般危害、严重危害。数据从低到高可分成一般数据、重要数据、核心数据三个级别。

陈吉栋说，我国采取的数据分类分级保护的逻辑和路径，本质上是以国家和公共利益为视角，始终站在数据背后的重要价值保护之上。“数据天然具备不同属性和特征，也必然存在不同的管理主体。出于不同的管理目的、基于不同的数据属性或特征对数据采用不同的分类分级方法，便于数据治理，有利于促进数据利用和流通。”

#### 企业如何给数据分类分级

近两年，数据合规问题成为企业重点关注的合规问题之一。在数据分类分级背景下，企业具

体应如何给数据定级分类？

刘权认为，数据定级的具体步骤包括四个方面：一是按照国家和行业领域的核心数据目录、重要数据目录，依次判定是不是核心数据、重要数据，如是，则按照就高从严原则定为核心数据级、重要数据级，其他定为一般数据。二是国家和行业核心数据、重要数据目录不明确时，可参考核心数据、重要数据认定的规定或标准，分析数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用的危害对象和危害程度，参照数据安全基本分级规则进行基本定级，确定核心数据、重要数据和一般数据级别。三是按照一般数据分级规则或者所属行业共识的数据分级规则对一般数据定级，确定一般数据细分级别。四是如果数据属于个人信息，还应识别敏感个人信息、一般个人信息，具体可参考《指引》中对个人信息定级的规定。

在数据分类流程上，《指引》规定数据处理器进行数据分类时，应优先遵循国家、行业的数据分类要求，如果所在行业没有行业数据分类规则，也可从组织经营维度进行数据分类，并给出常见的数据分类维度，包括公民个人维度、公共管理维度、信息传播维度、组织经营维度、行业领域维度。

陈吉栋表示，企业应严格按照国家重要数据目录和本地区、行业监管部门制定的重要数据具体目录对重要数据加强保护。对重要数据以外的其他数据，亦需自主进行分类分级并给予相应程度的保护。企业可以参考既有数据分类分级法律法规等，根据数据安全法等规定和所属行业的数据分类分级要求，结合企业自身实际情况，开展适合自身的、行之有效的数据分类分级。

刘权表示，由于数据的类型级别可能因时间变化、政策变化、安全事件发生、不同业务场景的敏感性变化或相关行业规则不同而发生改变，所以数据处理器需要对数据分类分级进行定期审核并及时调整。