三问企业数据分类分级合规

作者：潘永建 | 朱晓阳 | 邓梓珊 | 黄文捷

近期，国家密集颁布有关数据分类分级制度的法规和指导性文件征求意见稿(请见文中表一)。这些法规文件旨在细化之前法规规定的数据分类分级制度，具体指导政府部门和组织实施分类分级制度。从企业合规视角，也有必要借助数据的分类分级管理履行繁杂交织的数据合规义务。通力网安数据合规团队在诸多法规文件中“去芜存菁”，针对企业关心的三个核心实务问题进行简要解析。

(1) 什么是分类分级制度(What)?
(2) 为什么要实施分类分级制度(Why)?
(3) 如何实施分类分级制度(How)?

1. 什么是“数据分类分级”制度(What)

除《数据安全法》规定的重要数据分类分级制度外，各部门、各地区政府也正在逐步制定不同行业、领域的数据分类分级制度或指引，为企业的数据分类分级工作提供参考。

2021 年 9 月 1 日生效的《数据安全法》第二十一条规定，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、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，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。关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。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。

数据分类分级并不仅仅限于重要数据。简而言之，数据分类分级是将企业所掌握的数据根据法律法规及企业自身实际情况进行分类，并在分类的基础上，根据不同类别数据的重要程度及“灾害后果”严重程度，实施不同级别的管理措施。

除重要数据相关的分类分级制度外，若干法规、规范性文件和政策对部分其他类型数据的分类分级设定了具体制度，数据分类分级制度正在逐步构建。

发文机关	法律法规名称
全国人大常委会	《数据安全法》
工业和信息化部	《工业和信息化领域数据安全管理办法(试行)》(征求意见稿)
工业和信息化部	《关于加强车联网网络安全和数据安全工作的通知》
上海市人大常委会	《上海市数据条例(草案)》(征求意见稿)
信息安全标准化技术委员会	《网络安全标准实践指南——数据分类分级指引》(征求意见稿)
贵州省人民代表大会常务委员会	《贵州省大数据安全保障条例》
天津市互联网信息办公室	《天津市数据安全管理办法(暂行)》
国务院办公厅	《科学数据管理办法》
中国证券监督管理委员会	《证券基金经营机构信息技术管理办法》 《证券期货业数据分类分级指引(JRT 0158-2018)》
工业和信息化部	《工业数据分类分级指南(试行)》
中国人民银行	《个人金融信息保护技术规范(JR/T0171-2020)》
中国人民银行	《金融数据安全 数据安全分级指南(JR/T 0197-2020)》

表一： 数据分类分级制度的主要法规和文件

2. 为什么要实施数据分类分级(Why)

从国家监管的角度看，实施数据分类分级制度，是落实管理《网络安全法》《数据安全法》《个人信息保护法》等法规管理重要数据和其他受监管数据的必要措施。同时，数据分类分级也是国家推动数据开放共享、提升数据资源价值的前提。从企业治理的角度看，企业既面临个人信息、重要数据等合规义务，也必须遵守其所在行业、领域的特殊类型数据的合规义务。如果企业没有对自身数据情况进行充分评估，并将数据进行分类分级管理，数据合规义务无疑将成无源之水、无本之木。

作为数据处理者的企业应履行数据分类分级的法定义务。并且，企业为了遵从相关法规，履行个人信息保护、数据收集与使用、数据出境、重要数据等各类数据合规义务，有必要做好数据分类分级工作。按照相关法规，未履行数据分类分级义务的企业可能受到信用惩戒、公开曝光、没收违法所得、罚款、暂停营业、停业整顿、关闭网站、吊销业务许可证或者吊销营业执照等行政处罚；构成犯罪的，依法追究刑事责任。而对于处在特殊行业的企业而言，部分内部经营数据可能直接构成受规制的特殊类

型数据，未能将该类数据进行单独处理和保护的话，亦有可能违反特殊法律法规规定(例如，医药企业收集的人口健康信息、人类遗传资源信息等)。

在相关法规和文件尚在征求意见阶段的情形下，企业普遍感到困惑，是否应等到相关法规文件正式生效后开展数据分类分级工作?结合数据立法和执法实践，我们认为，企业不应抱着“等(立法)”“靠(政府)”态度，而应积极主动实施数据分类。首先，作为新生法律制度，我国数据分类分级制度立法一直“摸着石头过河”，其立法逻辑亦经历从“自下而上”到“自上而下”的转变(请见我们之前的法评文章《能力越大，责任越大——数据分类分级制度评述》)。最新颁布的《网络安全标准实践指南——数据分类分级指引》(征求意见稿)特别指出，数据分类分级原则之一是“自主性”原则，即在国家数据分类分级规则的框架下，根据自身管理需要，行业、领域、地方或组织自主细化确定所管辖数据的类目设置和层级划分。因此，在框架规则基本建成的前提下，企业应考虑自主进行细化工作；其次，如上文所述，企业有必要对其持有的数据“摸家底”，实施数据分类分级制度，并对不同重要和敏感程度的数据采取不同的管控和保护措施，建立、完善数据风险管理内部流程，这将有助于企业履行其他网安数据合规义务。

3. 如何实施数据分类分级(How)

参考相关法规和执法实践，我们总结企业实施数据分类分级的工作要点。

(1) 成立由企业法务合规、IT 数据、业务人员等组成的项目组

数据分类分级需要完成识别数据、理解法规要求、甄别数据危害对象和危害程度等工作，而这些工作需要企业法务合规、IT 数据和业务人员合力完成。

举例而言，企业的数据包括结构化数据(RDD、SQL、NOSQL、JSON 等数据)、半结构化数据(日志文件、XML 文档、Email 等)、非结构化数据(办公文档、文本、图片、HTML、报表、图像音频视频资料等)，对于法务合规和业务人员而言，结构化和半结构化数据“不可读”。这些数据的识别需要企业 IT 数据部门的支持；诸多法律合规要求，有赖于法务合规部门的专业解读。即使是看似基础性的法律问题，也需要上述人员共同合作。例如(受法律保护的)个人信息范围亦需要结合法规、司法和行政执法实践作出细致分析；有关数据受篡改、破坏、泄露的后果分析，有赖于业务部门具体说明数据来源、用途、对上下游产业的影响等。

(2) 先分类

根据相关法规，企业宜先分类后分级，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，形成数据分类清单并定期更新。

通常，企业可将其持有的数据分类分为三类：公共数据、个人信息和企业数据。每一数据大类又可以根据法律法规、企业自身需求及实际情况进行进一步细分。

数据类别	数据类别的定义	示例
公共数据	公共管理和服务机构在依法履行公共管理和服务职责过程中收集、产生的数据，及其他组织和个人在提供公共服务中收集、产生的涉及公共利益的数据	如政务数据，以及提供供水、供电、供气、供热、公共交通、养老、教育、医疗健康、邮政等公共服务中涉及公共利益的数据等
个人信息	以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息	如个人身份信息、个人生物识别信息、个人财产信息、个人通信信息、个人位置信息、个人健康生理信息
企业数据	企业在研发设计、生产制造、经营管理、运维服务、平台运营、应用服务、内部管理中收集和产生的数据	如业务数据、经营管理数据、系统运行和安全数据

表二：数据类别

(3) 后分级

企业可参考《网络安全标准实践指南——数据分类分级指引》(征求意见稿)数据定级规则，将各类数据分为一般数据(1到3级)、重要数据(4级)和核心数据(5级)。如果数据集出现"跨级"现象，采取就高从严原则对数据进行定级。

危害对象 危害程度	国家安全	公共利益	组织合法权益	个人合法权益
特别严重危害	核心数据(5级)	核心数据(5级)	重要数据(4级)	重要数据(4级)
严重危害	核心数据(5级)	重要数据(4级)	一般数据(3级)	一般数据(3级)
一般危害	重要数据(4级)	一般数据(3级)	一般数据(2级)	一般数据(2级)
轻微危害	重要数据(4级)	一般数据(2级)	一般数据(1级)	一般数据(1级)

表三：数据定级规则

毋庸置疑，企业判定其持有的数据是否构成核心数据和重要数据至关重要。如果企业持有核心数据及重要数据的，必须按照法律法规的规定予以管理。以医药企业为例，企业可考虑采取以下两步骤加以识别：

第一步：企业是否持有以下数据：

- 与传染病、新型生物技术、实验室生物、国家重要遗传资源和基因数据相关；
- 与突发传染病、重大动植物疫情、微生物耐药性、生物技术环境安全相关；
- 在药品和避孕药具不良反应报告和监测过程中获取的个人隐私、患者和报告者信息；

- 突发公共卫生事件与传染病疫情监测过程中获取的传染病病人及其家属、密切接触者的个人隐私和相关疾病、流行病学信息等;
- 医疗机构和健康管理服务机构保管的个人电子病历、健康档案等各类诊疗、健康数据信息;
- 人体器官移植医疗服务中人体器官捐献者、接受者和人体器官移植手术申请人的个人信息;
- 人类辅助生殖技术服务中精子、卵子捐献者和使用者以及人类辅助生殖技术服务申请人的个人信息;
- 计划生育服务过程中涉及的个人隐私;
- 个人和家族的遗传信息;
- 生命登记信息。

第二步: 分析该等数据如果遭到篡改、破坏、泄露或者非法获取、非法利用, 对国家公共卫生安全与利益、企业及上下游行业业务服务能力、个人合法权益造成的危害程度, 结合表三进行甄别界定。

(4) 分类分级管理

数据分类分级完成后, 企业应按照法规履行对外、对内合规义务: 对外向监管部门履行备案和数据安全评估等义务; 对内在企业内部按照数据 CIA 原则(即数据保密性 Confidentiality、完整性 Integrity 和可得性 Accessibility)进行分类管理。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市建国门北大街 8 号 华润大厦 4 楼 T: +86 10 8519 2266 F: +86 10 8519 2929	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野