

能力越大，责任越大——数据分类分级制度评述

作者：潘永建 | 杨迅 | 朱晓阳 | 黄文捷

数字经济方兴未艾，正在日益与互联网、人工智能、云计算等行业深度融合发展。数据是数字经济的重要支撑，已成为除土地、劳动力、资本和技术外的第五类“生产要素”。数据保护与规范亟需法律从个人信息与隐私保护、企业数据权益、国家安全与监管等维度作出系统性的制度安排。作为数据保护制度的基础法律，《个人信息保护法》和《数据安全法》的重要性毋庸置疑。2021年4月29日，《个人信息保护法(草案二次审议稿)》《数据安全法(草案二次审议稿)》公布。从企业使用数据和合规遵从的视角，通力网安数据业务小组对审议稿作出系列解读，本文为第七篇《能力越大，责任越大——数据分类分级制度评述》。

数据是国家基础性战略资源，数据安全是国家安全的重要组成部分。严重的数据安全风险甚至可能给国家安全带来重大风险。近日，美国成品油管道运营商 Colonial Pipeline 因系统受到黑客攻击被迫关闭其美国东部沿海各州的成品油管道，美国宣布部分地区进入紧急状态以缓解公路运输成品油的压力。Colonial Pipeline 更是被迫向黑客组织支付了数百万美金以换取系统的解锁。因此，保障数据安全是维护国家主权、安全和发展利益的重要手段。

《数据安全法》的颁布是国家通过立法加强数据安全保护的必要措施。《数据安全法》(草案二次审议稿)(以下简称“二审稿”)明确提出国家机关和企业应建立数据分类分级保护制度。就企业而言，掌握的数据“级别越高”，表明企业的业务能力和数据控制能力强，但同时也意味着企业对数据的责任和义务越大。本文试图简要分析我国目前法律体系下的数据分类分级制度，为企业建立数据分类分级制度提供全局视角。

.....
如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

一. 为什么需要实施数据分类分级?

1. 数据分类分级对于国家的意义

(1) 管理重要数据和其他需要监管的数据

数据分类分级是监测、管理、防范数据风险的基础。数据安全性遭到破坏时可能给国家安全、公共利益、个人隐私、企业合法权益等带来负面影响。如果没有对数据进行分类分级,就难以判断数据的影响对象和影响程度,也就难以采取针对性的安全管理措施。例如,《网络安全法》规定 CII 的重要数据出境应先经过安全评估,如果没有数据分级分类,尚且不知有哪些重要数据,更遑论对其进行出境评估。

(2) 挖掘数据价值

《关于构建更加完善的要素市场化配置体制机制的意见》将数据纳入生产要素的范畴,提倡加快培育数据要素市场。对数据进行分类分级,有助于提高数据质量、规范性、和标准化,从而推动数据开放共享、提升数据资源价值,有利于全社会进一步挖掘数据价值。

2. 数据分类分级对于企业的意义

(1) 管理企业内部数据风险

在数据发展成为重要生产资源的当下,数据处理活动日益复杂,数据处理涉及的主体和环节越发多样化,企业内部数据可能存在各种被泄露、滥用、篡改的安全风险。对数据进行分类分级保护,有利于企业对其持有的数据“摸底”,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,对企业控制、处理的数据按照分类分级结果采取适当的安全措施。

(2) 满足外部合规要求

在国家对数据实施分类分级保护的背景下,企业被赋予个人信息保护、数据出境合规、重要数据合规等各类数据合规义务,企业内部实施数据分类分级保护亦有助于企业应对各类业务场景下的网络安全与数据合规义务。

二. 数据分类分级: 国家的视角

1. 国家层面的“自上而下”的数据分类分级制度

二审稿第 20 条提出,国家建立数据分类分级保护制度,对数据实行分类分级保护,加强对重要数据的保护;并要求各地区、各部门确定本地区、本部门以及相关行业、领域的重要数据目录,

对列入目录的数据进行重点保护。该条款反映出国家在数据安全领域的重要变革和制度建设,即建立一个“自上而下”的数据分类分级保护体系。

不同于二审稿中“自上而下”的数据分类分级保护体系,在此之前出台的地区性、行业性法律法规和规范文件对于数据分类分级保护体系采取“自下而上”的方式。这两种方式的差别在于,“自下而上”的保护体系将数据分类分级义务施加于企业,要求企业从自身业务实际情况出发对数据进行分类分级并采取相应的保护措施,对数据进行分类的维度主要基于不同的业务条线,对数据进行分级的维度主要基于数据安全事件对数据的完整性、保密性、可用性的影响后果;而“自上而下”的保护体系从国家监管的视角出发,确立建立国家层面的、统一的数据分类分级保护制度,提出国家、各地区、各部门将确立相应的分类分级保护标准、重要数据目录及重要数据保护措施。在“自上而下”的保护体系下,国家、地区、行业主管部门在数据分类分级保护制度中承担主要角色,负责制定统一的标准和目录、建立数据安全监管平台、对企业的分类分级工作进行监管和指导,而企业则需根据国家的分级分类,对自身的数据进行分类和保护。

2. 地区和行业层面的数据分类分级保护

在地区和行业层面,已有不少法律法规从数据分类分级的角度规范本地区或本行业的数据安全相关活动。下表总结了其中一些重要的法律法规。在重要数据领域,根据二审稿第 20 条的规定,可以预见,在国家、地区、行业层面,将颁布更多、规范效力更强的重要数据目录,重要数据的认定标准将逐渐清晰。

发文机关	法律法规名称
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》
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	《个人信息信息保护技术规范(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)(送审稿)》

3. 数据安全审查制度

二审稿第 23 条提出,国家建立数据安全审查制度,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。尽管二审稿尚未明确影响国家安全的数据处理活动的具体范围,我们理解此类数据处理活动主要指的是重要数据和个人信息出境。国家互联网信息办公室曾于 2017 年发布《个人信息和重要数据出境安全评估办法(征求意见稿)》、于 2019 年发布《个人信息出境安全评估办法(征求意见稿)》,试图对重要数据和个人信息的出境活动以安全评估的方式实施审查。

根据以上两部《评估办法》，重要数据或个人信息出境可能影响国家安全、损害公共利益、或难以有效保障个人信息安全的，不得出境。

数据安全审查制度的具体细则尚未颁布。可以预见的是，数据安全审查制度的内容将与数据分类分级保护制度的内容相互关联。首先，数据安全审查中需要明确影响或者可能影响国家安全的数据类型，即对数据进行分类；其次，需要明确该类数据对国家安全的影响程度，即对数据进行分级。经过安全审查将被采取相应限制性措施的数据类型很有可能将是重要数据和个人信息。

三. 数据分类分级：企业的视角

1. 识别 CIIO 与重要数据

如前文所述，目前生效法律法规对重要数据的保护主要集中在对关键信息基础设施运营者(以下简称“CIIO”)的重要数据境内存储和出境安全评估制度。除关键设施基础运营者以外的其他重要数据处理者对于重要数据的安全保护义务，将由国家网信部门会同国务院有关部门制定相关管理办法。

(1) 识别 CIIO

CIIO 的识别是一项复杂且综合性的工作。简而言之，CIIO 的认定采取的是灾害后果测试的方法。

关于 CIIO 认定的具体步骤、方法和特殊问题，请见我们的后续文章。

(2) 识别重要数据

重要数据与国家安全、经济发展，以及社会公共利益密切。虽然重要数据的界定角度是从对国家的影响出发，但是重要数据的最终落脚点绝大多数还是在企业。对于重要数据的判断采用“后果测试”的标准：未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析，可能对国家安全、经济发展以及公共利益等造成影响的数据属于重要数据。单条或是汇聚后的数据均可构成重要数据。

常见的重要数据如核设施、化学生物、国防军工、人口健康、金融等领域数据，大型工程活动、海洋环境以及敏感地理信息数据、关键信息基础设施的系统漏洞、安全防护等网络安全信息。此外，《数据安全管理办法(征求意见稿)》指出，重要数据一般不包括国家秘密、国家情报、个人信息、企业生产经营和内部管理信息。

关于重要数据的具体范围，目前可供参考的主要文件是《信息安全技术 数据出境安全评估指南(征求意见稿)》附录《重要数据识别指南》，《重要数据识别指南》中描述了通信、电

子信息、化工、人口健康、金融等行业的重要数据的范围。前文提到，二审稿指出，国家、各地区、各部门将确立重要数据目录。预计在国家、地区、行业层面，将颁布更多、规范效力更强的重要数据目录，重要数据的界定标准将更加清晰。

2. 识别其他受到特殊监管的行业数据

科学数据、证券期货业数据、医疗健康数据、工业数据、金融数据等属于其他受到特殊监管的行业数据，各行业主管部门针对其主管领域企业处理的数据制定了各类法规规章、提出数据分类分级保护的要求，例如《科学数据管理办法》《证券投资基金经营机构信息技术管理办法》。

随着数据分类分级保护制度的发展，在各类法规规章笼统提出数据分类分级保护要求的基础上，已有部分法律法规和规范性文件明确提及分类分级标准并细化了相应的保护措施，其中比较有代表性的例如《工业数据分类分级指南(试行)》、行业标准《金融数据安全 数据安全分级指南(JR/T 0197-2020)》(以下简称“《金融数据指南》”)。由于各行业的数据分类分级保护制度的具体内容可能存在较大差异，以下我们仅以《金融数据指南》为例，试说明数据分类分级保护的一般思路。

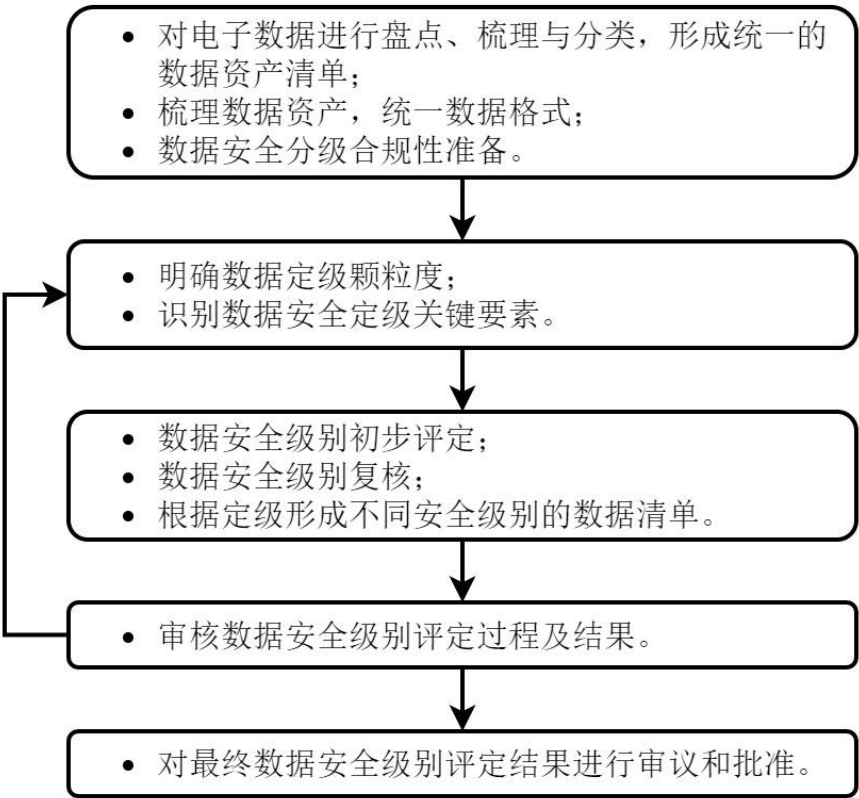
《金融数据指南》规定了金融数据安全分级的目标、原则和范围，以及数据安全定级的要素、规则和定级过程，为金融业机构开展数据安全分级工作提供指导。

(1) 定级标准

《金融数据指南》将金融业机构数据安全性遭到破坏后会对影响对象(包括国家安全、公众权益、个人隐私、企业合法权益)造成的影响分为四个等级：非常严重、严重、中等、轻微，再根据影响对象和影响程度将数据安全级别从高到低分为 5 级-1 级。《金融数据指南》明确提出重要数据的等级不得低于 5 级。

(2) 定级流程

金融数据安全定级过程包括数据资产梳理、数据安全定级准备、数据安全级别判定、数据安全级别审核及数据安全级别批准，具体工作流程如下图所示。



(3) 保护措施

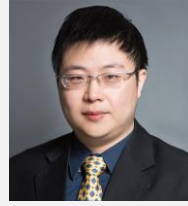
《金融数据指南》并未直接规定不同级别的金融数据的保护措施。《金融数据指南》第 5.3.1 条在描述不同级别金融数据的特征的过程中间接提及了对金融数据在访问和使用环节应当采取的保护措施。5 级-3 级金融数据一般针对特定人员公开，且仅为必须知悉的对象访问或使用；2 级金融数据一般针对受限对象公开，通常为内部管理且不宜广泛公开；1 级金融数据一般可被公开或可被公众获知、使用。

从企业的视角来看，为履行数据分类分级义务，企业首先应识别重要数据合规要求，判断自身是否构成 CIIO、是否掌握重要数据，其次应识别其他受到特殊监管的行业数据合规要求。在二审稿确立国家层面建立数据分类分级保护制度的背景下，企业更应主动合规，借此东风，建立全流程的数据风险管理制度，一站式解决数据分类分级、重要数据合规、个人信息保护、特殊监管的行业数据合规等多项数据合规要求。

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



杨 迅
+86 21 3135 8799
xun.yang@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

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

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

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

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

伦敦

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

免责声明:

本出版物仅供一般性参考, 并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2021