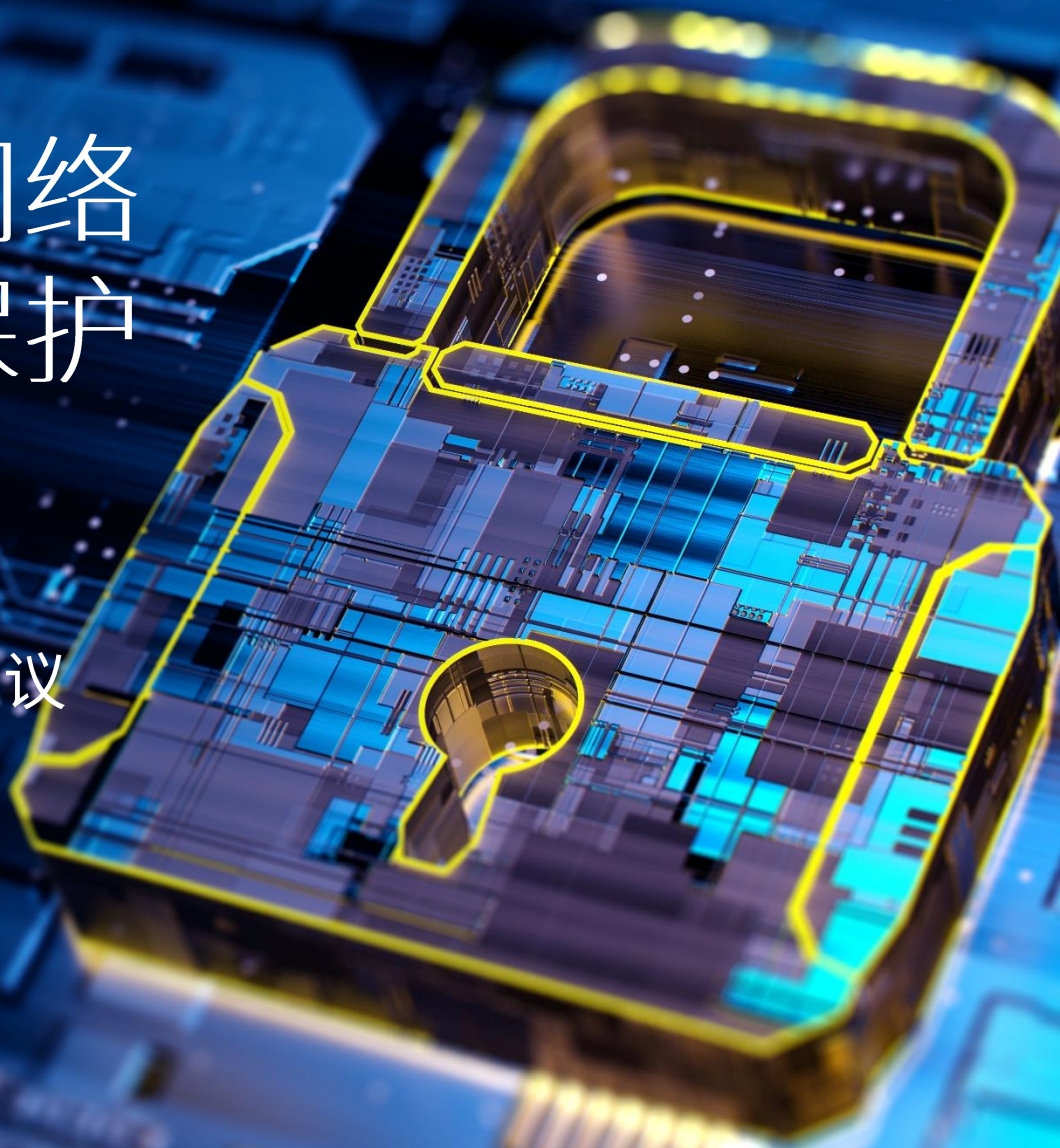
KPMG

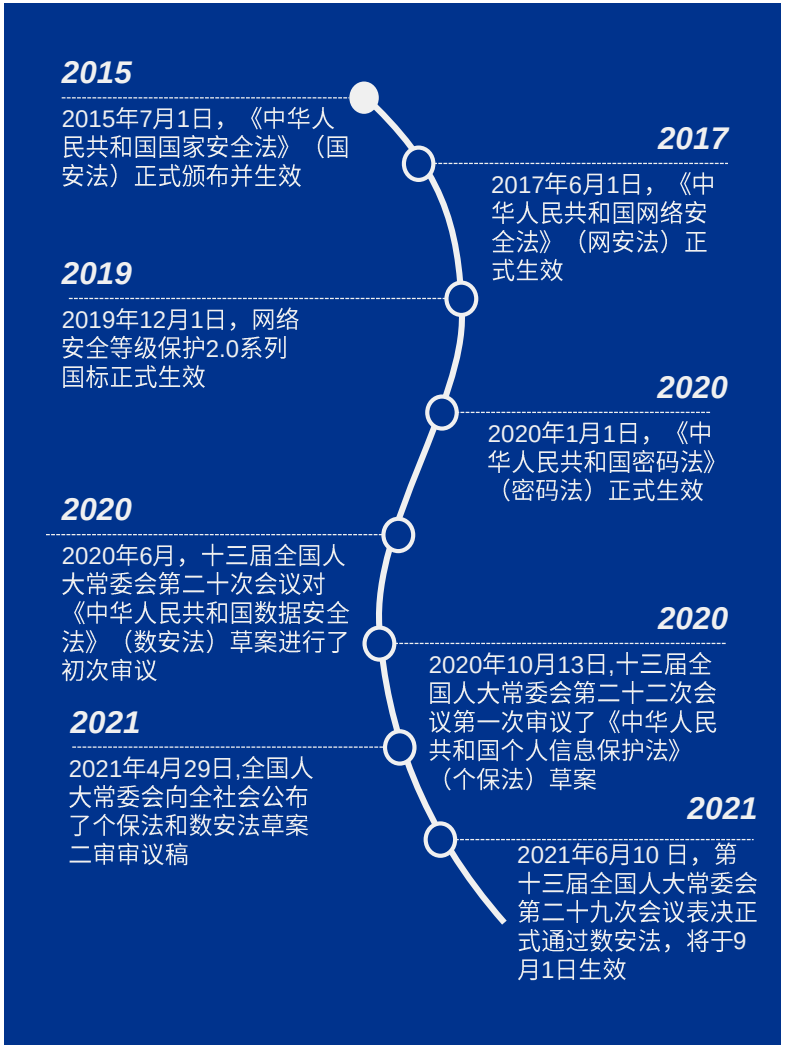
构建全面的网络安全和数据保护治理体系

数安法要点小结与应对建议



kpmg.com/cn

数安法和网安法构建安全治理的纵深边界



2015年7月1日，《中华人民共和国国家安全法》（国安法）正式颁布并生效，明确将网络安全和数据安全上升到国家安全的高度。

2017年6月1日，《中华人民共和国网络安全法》（网安法）正式生效，约定了在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理的相关安全管理义务和要求。

2021年6月10日，《中华人民共和国数据安全法》（数安法）正式颁布并将于2021年9月1日生效，规范在中华人民共和国境内开展数据处理活动及其安全监管，并约定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。即将出台的《中华人民共和国个人信息保护法》（个保法）亦会对个人信息这一特定类型数据的处理和保护要求进行进一步细化和补充。

在未来的6-12个月，建议进一步重点关注以下即将出台或定稿的相关法律法规及配套细则：

- 数据安全管理条例
- 重要数据目录
- 重要数据出境安全评估办法
- 关键信息基础设施保护条例
- 网络安全等级保护条例
- 个人信息出境安全评估办法

数安法要点概览

适用范围

1

- 在中华人民共和国境内开展数据处理活动及其安全监管；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
- 数据是指任何以电子或者其他方式对信息的记录

制度体系

2

- 数据分级分类保护、重要数据保护、国家核心数据保护制度
- 数据安全风险管理和监测预警机制
- 数据安全应急处置机制
- 数据安全审查制度
- 数据出口管制制度

监管部门

3

- 中央国家安全领导机构
- 各地区、各部门
- 行业主管部门（工业、电信、交通、金融、自然资源、卫生健康、教育、科技等）
- 公安机关、国家安全机关等
- 国家网信部门
- 国务院标准化行政主管部门和国务院有关部门

保护义务

4

- 处理活动应合法正当，符合社会公德和伦理
- 建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全；利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行数据安全保护义务，并应加强风险监测和事件应急响应
- 重要数据处理者还应明确数据安全负责人和管理机构，定期开展风险评估并报送报告，依据出境管理规定管理出境活动等

法律责任

5

- 责令改正，给予警告
- 罚款：
  - 组织：五万元~一千万元
  - 个人：一万元~一百万元
- 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
- 其他：依法追究刑事责任、依法承担民事责任、依法给予治安管理处罚等

数据分级分类保护

数安法

第六条 各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。

工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。

……

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、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。

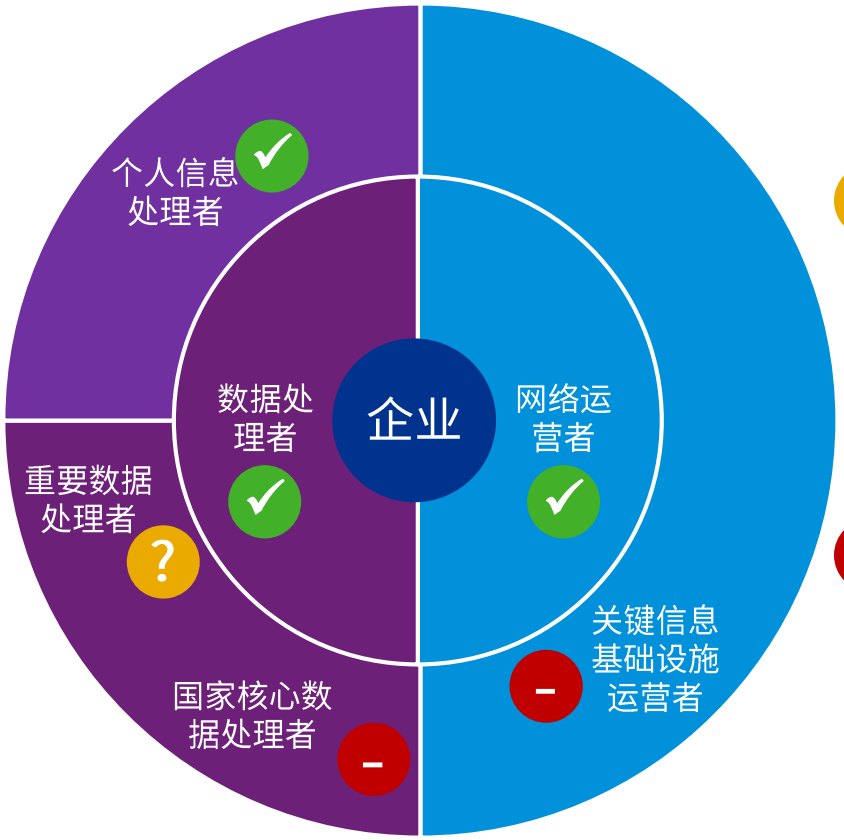
各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

- 数据分级分类是数据安全管理工作的基础，企业现有的内部数据分级分类制度和方法在未来可能需要进一步调整和优化，以与国家的数据分类分级保护制度进行衔接
- 重要数据目录和重要数据具体目录的确定，需进一步密切关注各行业主管部门的相关要求

工业	电信	交通	金融	自然资源	卫生健康	教育	科技
工业和信息化部		交通运输部	中国人民银行	自然资源部	国家卫生健康委员会	教育部	科学技术部
《工业数据分类分级指南（试行）》（2020）		《金融数据安全 数据安全分级指南》(JR/T0197—2020)		《信息安全技术 健康医疗数据安全指南》（GB/T 39725-2020）		中华人民共和国人类遗传资源管理条例（2019）	

示例

理解企业的多重身份



企业基本作为网络运营者（网安法），数据处理者（数安法）和个人信息处理者（个保法草案）

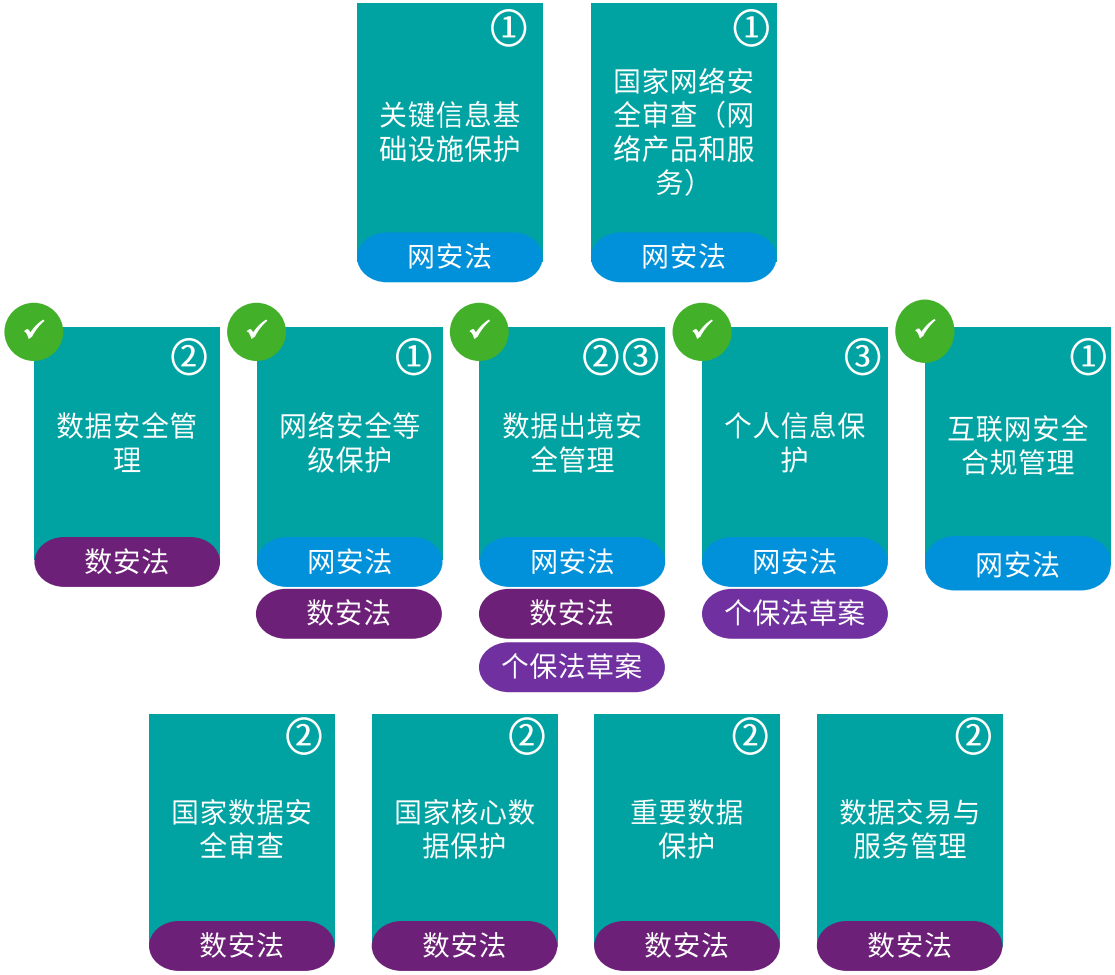
部分企业可能涉及重要数据的处理

- ✓ 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
- ✓ 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

少数企业可能涉及国家核心数据的处理和（或）关键信息基础设施运营

- ✓ 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
- ✓ 一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施

进一步扩大的安全合规要求



企业从基本合规义务出发，应建立健全：

1. 信息安全管理体系
2. 数据安全管理体系
3. 个人信息管理体系

基本外部合规举措概览

- 网络安全等级保护评估、认证
- 数据安全检测评估、认证
- 个人信息保护评估、认证
- 报送个人信息保护负责人的姓名、联系方式等
- 个人信息和重要数据出境安全评估
- 报告网络安全事件
- 报告数据安全事件
- 报告个人信息安全事件

对企业现有安全治理体系的主要影响

强调全生命周期数据安全管理，原有的纯技术的、片面的数据安全管理手段或措施应当进行梳理和重塑，与企业的数字化转型、数据治理和运营管理有机结合，从上至下、多方协作以实现切实有效的、可落地的安全治理。

关注网络空间安全和数据保护，个保法草案和数安法覆盖数据保护的点和面，网安法则从网络空间安全角度在传统信息安全管理基础上提出要求；企业应按自身业务技术运营和数据处理的情况，确保原有信息安全管理、数据安全管理和个人信息管理在地域范围上、业务范围上、技术范围上能够有效覆盖和落实已提升至法律层面的中国网络安全和数据保护要求。

重申本地化与数据出境安全管理，结合网安法、数安法和个保法草案，个人信息（达到一定数量）和重要数据本地化的要求已从法律层面扩大至所有网络运营者，如何确定合理的本地化策略，并将数据跨境传输作为数据生命周期管理活动的一部分进行常态化管理，是企业需要面对和解决的问题。

需要本地化的不仅仅是数据和系统，一方面企业应至少指定本地的网络安全负责人，按需任命个人信息保护负责人和数据安全负责人，建立网络安全、数据安全、个人信息管理机构；另一方面，随着数据和系统的本地化，配套的基础设施和安全运维也同样需要搭建本地化团队、流程和工具予以支撑，在全球化运营框架下合理规划和建设本地的安全运营中心。

毕马威网络安全服务

全球化的网络安全和
法律服务专业团队

丰富的网络安全和
数据保护规划落地经验

良好的网络安全生态圈互动与协作关系

可定制化、可持续管理的
技术解决方案

联系我们

石浩然
毕马威中国
网络与信息安全咨询
服务合伙人
电话：+852 2143 8799
henry.shek@kpmg.com

张令琪
毕马威中国
网络与信息安全咨询
服务合伙人
电话： +86 (21) 2212 3637
richard.zhang@kpmg.com

张倪海
毕马威中国
网络与信息安全咨询
总监
电话： +852 2847 5062
brian.cheung@kpmg.com

黄芃芃
毕马威中国
网络与信息安全咨询
总监
电话： +86 (21) 2212 2355
quin.huang@kpmg.com

郝长伟
毕马威中国
网络与信息安全咨询
总监
电话： +86 (10) 8508 5498
danny.hao@kpmg.com

kpmg.com/socialmedia