



毕马威

# 数据安全：护航数字经济高质量发展

《网络数据安全条例》历经3年正式发布，于2025年1月1日正式生效。

2024年11月



# 增强数据安全保障能力是企业基本的合规义务，也是企业在数字化时代保持竞争力的应时之举

2023年中共中央、国务院印发了《数字中国建设整体布局规划》明确指出：增强数据安全保障能力，建立数据分类分级保护基础制度，健全网络数据监测预警和应急处置工作体系。



## 增强数据安全保障能力是基本合规义务

数据安全正经历着从立法到实践的逐步转变。目前，个人信息保护监管闭环已日益完善，也同步促进了数据安全的规范化和系统化管理。重要数据的识别和保护、灵活便捷的数据出境监管机制的探索，也还在持续推进。企业仍需密切关注，积极合规。



## 数据安全技术创新的动力和底气

随着大数据、人工智能和区块链等新兴技术的广泛应用，企业面临新的安全挑战。为确保技术创新顺利进行，企业需不断更新安全措施，并高度关注数据安全，以识别并应对潜在风险。



## 保护好数据就是保护好核心竞争力

数据中蕴含着商业机密、客户信息和市场洞察等，这些数据的安全与保密直接关系到企业的业务稳定性和市场竞争力。只有通过加强数据安全管理，确保数据的完整性和可用性，企业才能在激烈的市场竞争中立于不败之地，实现可持续发展。

# 《网络数据安全管理条例》是网安法、数安法、个保法下首个国务院正式发布的管理条例

2015

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

2017

6月1日，《中华人民共和国网络安全法》（网安法）正式生效

2019

5月，国家互联网信息办公室关于《数据安全管理办法（征求意见稿）》公开征求意见

2021

9月1日，《中华人民共和国数据安全法》（数安法）正式生效

2021

11月1日，《中华人民共和国个人信息保护法》（个保法）正式生效

2021

11月1日，国家互联网信息办公室关于《网络数据安全管理条例（征求意见稿）》公开征求意见

2024

8月30日，国务院常务会议审议通过《网络数据安全管理条例（草案）》

2024

9月30日，《网络数据安全管理条例》签发，2025年1月1日生效

截至2024年9月，已有多个行业主管部门，包括工业和信息化部、中国人民银行、教育部发布了关于工业和信息化领域、金融行业、教育行业、电信行业及汽车行业等的数据安全相关管理办法。

## 适用范围

- 在中华人民共和国境内开展网络数据处理活动及其安全监督管理；
- 在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，符合个保法第三条第二款规定情形的依法适用；
- 在中华人民共和国境外开展网络数据处理活动，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
- 自然人因个人或者家庭事务处理个人信息的，不适用本条例。

## 重点关注

### 一般规定：

- 数据安全治理方针
- 数据安全生命周期管理
- 数据安全管理体系
- 数据安全安全技术

### 特定数据处理活动要求：

- 国家安全审查
- 个人信息保护
- 重要数据安全
- 数据出境安全管理
- 网络平台服务提供者数据安全

## 违规后果

- 主要参照网安法、数安法、个保法，针对一般规定、网络安全审查和重要数据安全，作出以下补充：
  - 罚款（单位最高一千万元，直接负责的主管人员和其他直接责任人员最高一百万元）
  - 单位可责令改正，给予警告，没收违法所得，责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照等

# 数据分类分级是数据安全治理的基础

## 影响对象



## 影响程度



根据数据在经济社会发展中的重要程度，以及一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益造成的危害程度，将数据从高到低分为**核心数据**、**重要数据**、**一般数据**三个级别。按照数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对经济运行、社会秩序、公共利益或个人、组织合法权益等造成的危害程度，将**一般数据**可以从低到高分**为 1 级、2 级、3 级、4 级**共四个级别。

数据安全分类	数据安全等级	数据定级要素	
		影响对象	影响程度
一般数据	1级	个人权益、组织权益	无危害
	2级	个人权益、组织权益	一般危害
	3级	个人权益、组织权益	严重危害
	4级	个人权益、组织权益	特别严重危害
经济运行、社会秩序、公共利益		一般危害	
重要数据		经济运行、社会秩序、公共利益	严重危害
		国家安全	一般危害
核心数据		经济运行、社会秩序、公共利益	特别严重危害
		国家安全	特别严重危害或严重危害

参考：GB/T 43697-2024 《数据安全技术 数据分类分级规则》

# 金融行业在数据安全治理的重点关注

金融行业目前已针对数据安全起草并发布了多项行业内的法规和标准，包括《中国人民银行业务领域数据安全管理办法（征求意见稿）》、《银行保险机构数据安全管理办法（公开征求意见稿）》、《JR/T 0197-2020 金融数据安全 数据安全分级指南》、《JR/T 0171-2020 个人金融信息保护技术规范》等。在《网络数据安全条例》正式生效后，依据已发布的相关法规和标准，金融行业应重点关注以下领域。

## 数据分级分类

- 按照业务分类，梳理数据资产，识别重要数据、核心数据，形成重要数据目录
- 建立数据分级分类实施制度
- 根据数据分级分类采取差异化安全保护措施
- 实施数据目录的动态管理与维护

银行保险机构数据安全管理办法（公开征求意见稿）		中国人民银行业务领域数据安全管理办法（征求意见稿）
一般数据	其他一般数据	一般数据
	敏感数据	
重要数据		重要数据
核心数据		核心数据

## 关键挑战

- ✓ 考虑不同法规中数据安全级别的映射关系，外资行还需统筹考虑境内与境外的数据资产，降低管理成本
- ✓ 数据分级分类的不精确会影响差异化安全保护措施的落地
- ✓ 动态管理与维护是持续性工作而非一次性

## 数据安全治理与管理

### 安全治理架构：

- 明确数据安全相关内设部门职责分工，细化定责问责规程
- 指定数据安全归口管理部门
- 重要数据处理者书面明确数据安全负责人和数据安全牵头管理内设部门

遵循“谁管业务，谁管业务数据，谁管数据安全”的基本原则

# 金融行业在数据安全治理的重点关注（续）

## 数据安全治理与管理

### 数据安全体系建设：

- 建立数据安全治理、数据分级分类、数据安全治理、数据安全技术、数据安全风险评估等方面的相关制度要求
- 对网络数据进行分类分级保护，对所处理网络数据的安全承担主体责任

### 数据服务管理体系：

- 建立数据服务管理体系、制定数据服务规范、建立专职的数据服务团队

## 数据生命周期管理

- 结合《JR/T 0197-2020 金融数据安全 数据安全分级指南》、《JR/T 0223-2023 金融数据安全 数据生命周期安全规范》明确全生命周期各环节中不同层级数据安全保护管理要求
- 执行全生命周期各环节中不同层级数据安全保护措施要求，包括数据收集、数据加工、数据使用、数据共享、委托处理、共同处理、数据转移与提供、数据公开、数据跨境、销毁与删除、数据传输、数据备份与存储
- 集团内部共享数据应采取保护措施，共享敏感及以上数据应获得主体的授权和同意

## 数据安全事件管理

- 建立数据处理活动安全风险监测和告警机制
- 制定数据安全事件定级判定标准和应急预案
- 强化内部人员和培训管理，加强人员安全意识，落实安全事件应急预案
- 依据不同的监管机构规范应急响应与处置工作，及时有序上报事件及处置情况
- 接受社会监督，建立便捷的网络安全投诉、举报渠道，公布投诉、举报方式等信息，及时受理并处理网络安全投诉、举报

## 数据安全监督管理

- 建立数据安全监督合规要求和规范
- 依据不同监管机构的要求开展全面的数据安全审计工作
- 每年开展一次全面的数据安全风险评估，并依据要求完成上报工作
- 对有关主管部门依法开展的网络安全监督检查予以配合

## 关键挑战

- ✓ 当前两方监管的要求存在差异，金融机构应求同存异，具体问题具体分析，避免重复建设
- ✓ 依据不同的数据层级采取不同的安全措施，构建适应新技术环境的数据安全技术保护体系
- ✓ 构建覆盖数据全生命周期的安全管控时，需要结合实际的数据场景考虑所需的数据安全的核心技术能力，如加密、数据脱敏、数字水印、数据防泄漏、隐私计算、数据自动化定级达标等，同时还需要考虑如何通过技术工具、产品平台（数据安全应用）的方式将相应技术落地实现
- ✓ 在面对数据安全事件时，需要能够迅速识别、评估、应对并恢复业务
- ✓ 从金融监管角度当前非常关注如何对数据安全事件进行有效的管理，包括事件实质发生后，如何进行应急处置与监管报备，金融企业应针对应急相关的流程、演练着重进行建设
- ✓ 常态化数据安全评估和审计工作，持续与监管保持沟通

# 特定数据处理活动要求

专题管理事项应重点关注与其他相关合规要求和实践的衔接与补充

## 国家安全审查

- 网络数据处理者开展网络数据处理活动，影响或者可能影响国家安全的，应当按照国家有关规定进行国家安全审查

主要参考：国安法、网安法、数安法、关键信息基础设施安全保护条例、网络安全审查办法

## 个人信息保护

- 个人信息处理者总体合规要求应以个保法和其他相关个人信息保护规定为主，在以下方面应遵循补充要求：
  - 细化个人信息转移的具体条件、保存期限的具体落实等
  - 向其他网络数据处理者提供、委托处理个人信息的处理情况记录，应当至少保存3年
  - 处理1000万人以上个人信息的，还应当遵守适用于重要数据的处理者的有关于网络数据安全负责人和网络数据安全管理机构、以及提供、委托处理、共同处理个人信息前开展风险评估的相关要求

其他主要参考：个保法、网安法、GB/T 35273个人信息安全规范等

## 数据出境安全管理

- 数据出境安全管理总体合规要求应以网安法、个保法、数安法和其他相关最新数据出境规定为主，在以下方面应遵循补充要求：
  - 国家采取措施，防范、处置网络数据跨境安全风险和威胁。任何个人、组织不得提供专门用于破坏、避开技术措施的程序、工具等；明知他人从事破坏、避开技术措施等活动的，不得为其提供技术支持或者帮助

其他主要参考：网安法、个保法、数安法、数据出境安全评估办法、个人信息出境标准合同办法、促进和规范数据跨境流动规定等

# 特定数据处理活动要求（续）—— 网络平台服务提供者

## 网络平台服务提供者数据安全

- 网络平台服务提供者在数据安全方面的管理要求在《条例》中被首次提出，主要包括：
  - 明确接入其平台的第三方产品和服务提供者的网络数据安全保护义务，督促第三方产品和服务提供者加强网络数据安全，其中，应用程序分发服务的网络平台服务提供者还应当建立应用程序核验规则并开展网络数据安全相关核验
  - 通过自动化决策方式向个人进行信息推送的，个性化推荐易关闭、个人特征标签可删除
  - 国家鼓励网络平台服务提供者支持用户使用国家网络身份认证公共服务登记、核验真实身份信息
- 此外，大型网络平台服务提供者：
  - 每年度发布个人信息保护社会责任报告
  - 跨境提供网络数据，应当遵守国家数据跨境安全管理要求，健全相关技术和管理措施，防范网络数据跨境安全风险
  - 不得利用网络数据、算法以及平台规则等，开展不当网络数据处理活动，损害用户合法权益
  - 如涉及重要数据处理，年度风险评估还应充分说明关键业务和供应链网络数据安全等情况

网络平台服务提供者面向大量用户和平台内经营者提供服务，可能包括：提供信息发布和互动的社交媒体平台、提供支付服务的网络平台、提供视听服务的网络平台、提供应用程序分发服务的网络平台、预装应用程序的智能终端等设备生产者等。

大型网络平台服务提供者是指注册用户5000万以上或者月活跃用户1000万以上，业务类型复杂，网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响的网络平台。

# 特定数据处理活动要求（续）——重要数据安全治理

## 重要数据安全治理

《条例》对涉及重要数据的网络数据处理者在以下方面提出明确要求：

### 数据安全治理方针

- ✓ 应当明确网络数据安全负责人和网络数据安全机构，网络数据安全负责人应当具备网络数据安全专业知识和相关管理工作经历，由网络数据处理者管理层成员担任，有权直接向有关主管部门报告网络数据安全情况
- ✓ 发生合并、分立、解散、破产等情况的，应当向省级以上有关主管部门报告
- ✓ 应当每年度对其网络数据处理活动开展风险评估，并向省级以上有关主管部门报送风险评估报告

### 数据安全生命周期管理

- ✓ 提供、委托处理、共同处理重要数据的应当遵守额外规定（比如开展风险评估、处理情况记录保留至少3年）

### 数据安全管理体系和管理技术

- ✓ 国家鼓励使用数据标签标识等技术和产品，提高重要数据安全治理水平

目前，关于重要数据的识别和保护，部分行业领域主管（监管）部门已明确其行业数据分类细则，确定重要数据和一般数据范围，如工业、电信、卫生健康及教育。同时，部分自贸区已针对重要数据发布了详细的规定和识别指南，如《中国（北京）自由贸易试验区数据出境负面清单管理办法（试行）》及《中国（天津）自由贸易试验区企业数据分类分级标准规范》等。

重要数据的定义和识别细则尚未明确的行业，可参考《GB/T 43697-2024 数据安全 数据分类分级规则》、《信息安全技术 重要数据识别指南（征求意见稿）》来指导识别工作。

工业

工业

- 工业和信息化领域数据安全管理办法（试行）
- YD/T4981-2024 工业领域重要数据识别指南
- 汽车数据安全管理办法（试行）

电信

电信

- YD/T3867-2024 电信领域重要数据识别指南

交通

金融

自然资源

卫生健康

教育

科技

金融

- 中国人民银行业务领域数据安全管理办法（征求意见稿）
- 银行保险机构数据安全管理办法（公开征求意见稿）
- JR/T 0197-2020 金融数据安全 数据安全分级指南

卫生健康

- 卫生健康行业数据分类分级指南（试行）

教育

- 教育系统核心数据和重要数据识别认定工作指南（试行）

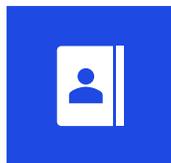
# 行动建议

“对网络数据实行分类分级保护，明确各类主体责任，落实网络数据安全保障措施。要厘清安全边界，保障数据依法有序自由流动，为促进数字经济高质量发展、推动科技创新和产业创新营造良好环境”



## 推进数据安全分级优化与落实

进一步推进数据安全分级工作的有效落实，结合外部合规要求和企业自身管理需要，实现数据资产分类和数据安全分级的有机结合，并通过技术和工具的应用，提升数据安全分级工作的可操作性和便利性，加大数据安全分级工作对数据处理活动和系统应用的覆盖面，为数据生命周期保护奠定良好基础。



## 加快数据安全管理体系总体建设

应尽快建立健全数据安全治理体系建设，建立基本组织保障和制度体系保障，包括但不限于数据安全保护总则、数据生命周期安全管理原则、数据安全事件管理和应急预案、数据安全投诉处理机制、数据安全风险与合规管理机制等。



## 有针对性的开展数据生命周期管理和数据安全治理技术落地

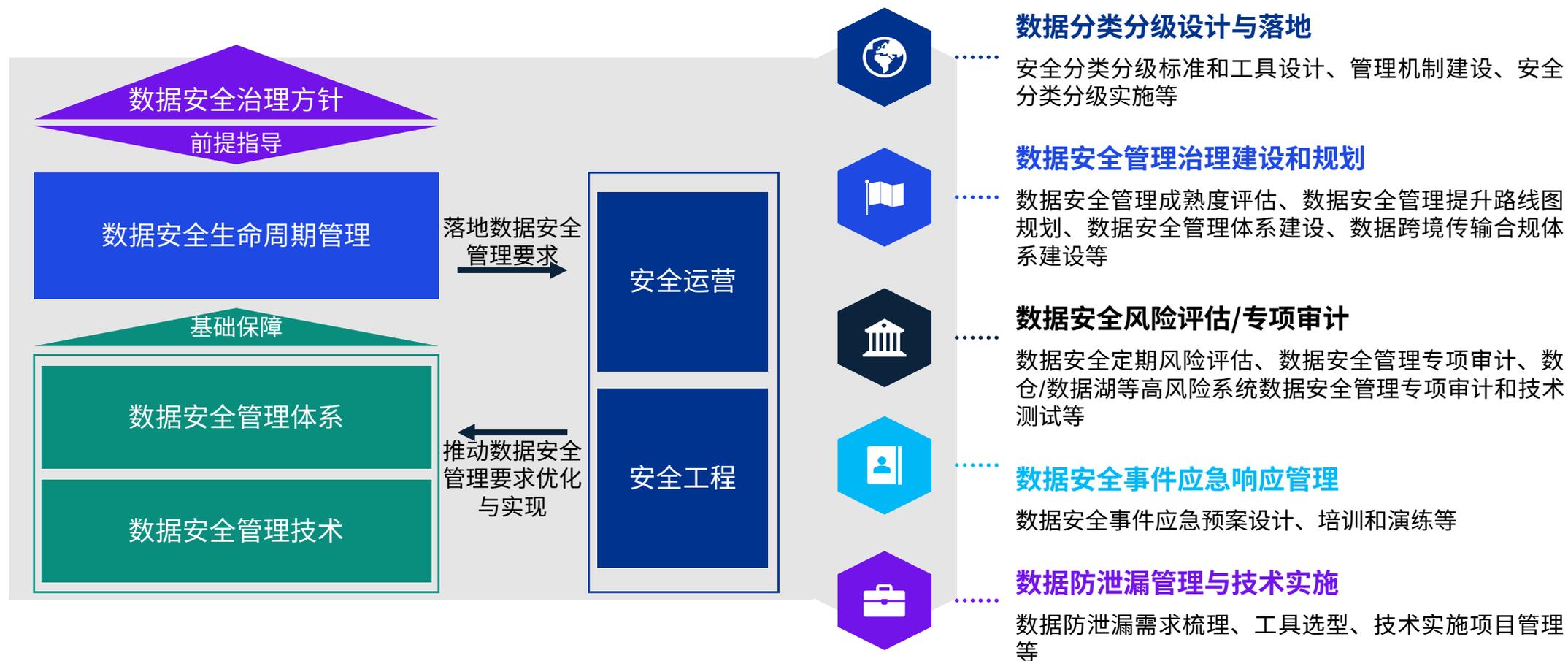
针对安全级别较高的数据及其所涉及的平台和基础设施环境，优先考虑加强数据安全治理技术管理措施的落地，包括但不限于加强加密控制措施、访问控制措施、备份和恢复管理机制、日志和事件监控机制等，以有效保障此类数据等完整性、保密性和可用性。



## 关注与个人信息管理、网络安全运营的衔接与运行

个人信息作为特殊的数据类型，其管理具有一定的特殊性，企业内部的数据安全管理组织和人员在处理个人信息安全方面，应与企业现有的个人信息保护框架体系有效融合；此外，在数据安全技术的建设与落实方面也与传统的信息安全、网络安全存在交叉与依赖，应考虑以数据安全为目标，对现有的网络安全技术措施进行重新审视和调整，以确保数据安全。

# 毕马威数据安全解决方案协助企业一站式管理 数据安全风险



# 联系我们

## 张令琪

科技咨询服务首席合伙人  
毕马威中国  
电话: +86 (21) 2212 3637  
邮箱: [richard.zhang@kpmg.com](mailto:richard.zhang@kpmg.com)

## 张倪海

科技咨询技术风险管理服务业务合伙人  
毕马威中国  
电话: +852 2847 5026  
邮箱: [brian.cheung@kpmg.com](mailto:brian.cheung@kpmg.com)

## 李振

科技咨询技术风险管理服务业务总监  
毕马威中国  
电话: +86 (10) 8508 5000  
邮箱: [jz.li@kpmg.com](mailto:jz.li@kpmg.com)

## 郝长伟

科技咨询技术风险管理服务首席合伙人  
毕马威中国  
电话: +86 (10) 8508 5485  
邮箱: [danny.hao@kpmg.com](mailto:danny.hao@kpmg.com)

## 林海燕

科技咨询技术风险管理服务业务合伙人  
毕马威中国  
电话: +852 2143 8803  
邮箱: [lanis.lam@kpmg.com](mailto:lanis.lam@kpmg.com)

## 黄芃芃

科技咨询技术风险管理服务业务合伙人  
毕马威中国  
电话: +86 (21) 2212 2355  
邮箱: [quin.huang@kpmg.com](mailto:quin.huang@kpmg.com)

## 邬敏华

科技咨询技术风险管理服务业务总监  
毕马威中国  
电话: +86 (21) 2212 2888  
邮箱: [fm.wu@kpmg.com](mailto:fm.wu@kpmg.com)

## 周文韬

科技咨询技术风险管理服务业务合伙人  
毕马威中国  
电话: +86 (21) 2212 3149  
邮箱: [kevin.wt.zhou@kpmg.com](mailto:kevin.wt.zhou@kpmg.com)

## 宋智佳

科技咨询技术风险管理服务业务总监  
毕马威中国  
电话: +86 (21) 2212 2888  
邮箱: [jason.song@kpmg.com](mailto:jason.song@kpmg.com)



[kpmg.com/cn/socialmedia](https://kpmg.com/cn/socialmedia)



如需获取毕马威中国各办公室信息, 请扫描二维码或登陆我们的网站: <https://home.kpmg/cn/zh/home/about/offices.html>

所载资料仅供一般参考用, 并非针对任何个人或团体的个别情况而提供。虽然本所已致力提供准确和及时的资料, 但本所不能保证这些资料在阁下收取时或日后仍然准确。任何人士不应在没有详细考虑相关的情况及获取适当的专业意见下依据所载资料行事。

©2024 毕马威华振会计师事务所(特殊普通合伙) — 中国合伙制会计师事务所及毕马威企业咨询(中国)有限公司 — 中国有限责任公司, 均是与毕马威国际有限公司(英国私营担保有限公司)相关联的独立成员所全球组织中的成员。版权所有, 不得转载。在中国印刷。

毕马威的名称和标识均为毕马威全球组织中的独立成员所经许可后使用的商标。