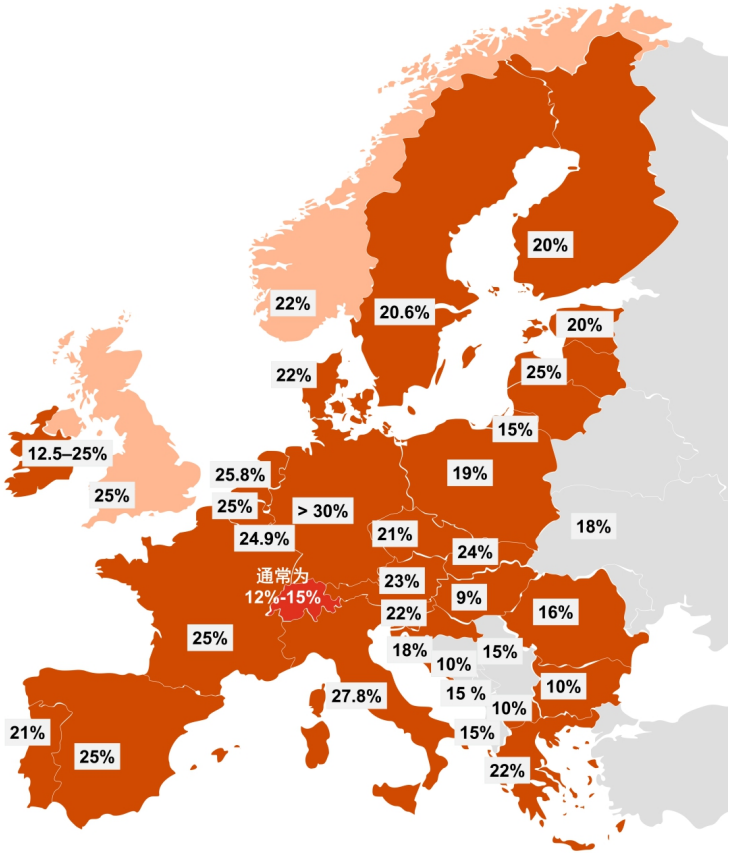
中企出海欧洲的供应链发展趋势与税务策略洞察

抓住欧洲的机遇：在供应链重新设计中保持领先的五种方法

普华永道欧洲税务总监 Daniela Honegger 女士详细解读了欧洲税务环境、走出去欧洲的投资架构及运营层面的核心考量。企业所得税差异方面，爱尔兰、瑞士等低税率国家成为投资热点，但企业需关注 OECD 全球最低税的影响；关税与间接税方面，欧盟对中国电动车、电池等产品加征反补贴税，企业需提前规划关税筹划方案。

欧洲企业所得税率



间接税的考虑

中国跨国企业在欧洲经营的主要间接税要求

增值税登记	财务代表	EORI代码
增值税资格	增值税合规	增值税发票
存档	文档要求	海关申明
支付增值税及进口关税	原产地及贸易协定	指定报关及代理机构

*** 数字时代的增值税（ViDA）**

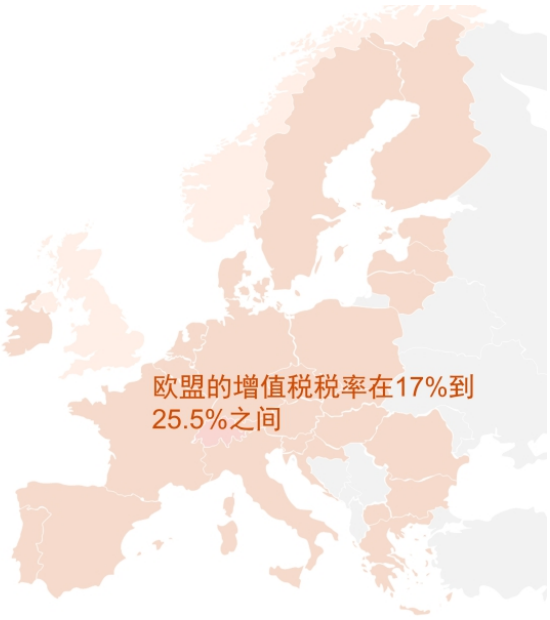
2025年4月开始的EU增值税重大改革。此次改革影响最广的是：

- 2030年7月1日起强制实行电子发票/电子申报
- 电子发票将成为新的标准（EU国家的统一方法）
- 数字报告要求：欧盟内部交易将以近乎实时的方式报告

间接税考虑

欧洲整体利益概览

- 跨成员国协调欧盟增值税制度
- 欧盟内部供应和采购规则
- 增值税退税机制
- 进口增值税延期和反向收费
- 增值税分组
- 保税仓储
- 一站式服务（OSS）和导入一站式服务（IOSS）
- 快速和可靠的增值税返还
- 关税及加工抵免
- 法律确定性和争议解决



欧盟人工智能法案(“EU AI Act”)与数字运营韧性法案（“DORA”)介绍

人工智能法案（“AI Act”）

建立统一的法律框架，以促进可信人工智能的发展，保护基本权利，并确保人工智能系统的安全性和可靠性

- 生效日期：2024年8月1日
- 全面适用日期：2026年8月2日

适用范围

1.欧盟境内AI产业链上的各类主体

2.域外效力：

- ✓**在欧盟市场提供AI系统/产品**
- ✓**AI系统的输出在欧盟使用**

关键内容

1.AI系统/模型/产品风险级别

2.透明度要求

3.数据安全与保护要求

4.符合道德与伦理准则

5.非欧盟企业需在欧盟指定授权代表

企业合规建议

1.梳理人工智能系统/模型/产品，并根据法案要求判断风险级别

2.明确在人工智能系统/模型/产品方面的角色定位（提供者、部署者、进口者、分发者和产品制造商等）

3.根据人工智能系统/模型/产品的风险等级，及相应的角色，识别法案要求的合规义务

4.开展差距评估，并制定合规措施的整改计划

5.建立人工智能治理框架，以实现持续合规

违规处罚

⚠ **罚款：使用禁止性AI -** 最高3500万欧元或全球营业额的7%

违反高风险要求 - 最高1500万欧元或全球营业额3%

数字运营韧性法案（“DORA”）

通过建立统一监管及网络威胁应对规则，全面提升欧盟金融体系的数字运营韧性

- 生效日期：2023年1月16日
- 全面适用日期：2025年1月17日

适用范围

1.金融行业实体

2.第三方 ICT 服务提供商（如：服务器、路由器、存储设备、5G/光纤、卫星通讯、云服务、物联网、视频会议）

3.域外效力：**与法案涵盖实体建立业务关系**

关键内容

1.董事会与管理层承担个人责任

2.重大事件4小时内报告

3.年度基本测试、每3年高级测试

4.第三方管理

企业合规建议

1.开展差距分析，识别与法案要求的合规差距

2.ICT风险管理框架，对现有的信息安全防护措施进行梳理与风险评估，对高风险项进行整改，以确保其具备抵御网络威胁的能力

3.制定第三方管理策略、制度与流程，加强第三方风险管理，明确与第三方服务商各自的职责与义务

4.根据法案的要求，建立或完善的事件响应预案

5.建立与监管部门协作以及信息共享机制

违规处罚

⚠ **罚款：**企业最高可达200万欧元或全球营业额的2%，**个人最高100万欧元**

☒ **执照吊销**

通用数据保护条例(“GDPR”)与网络弹性法案(“CRA”)介绍

通用数据保护条例（“GDPR”）

为应对数字时代个人数据滥用风险，统一成员国数据保护标准并赋予公民数据控制权，推动全球数据保护立法及数字经济健康发展

- 生效日期：2018年5月25日

适用范围

1.在欧盟内部设立的数据控制者或处理者

2.域外效力：

✓为欧盟内数据主体提供商品/服务

✓基于国际公法成员国的法律对其有管辖权的数据控制者

关键内容

1.数据全生命周期管理

2.数据主体权利响应

3.数据跨境传输

4.默认隐私设计

5.数据泄露通报

企业合规建议

1.开展全面的差距分析，识别风险，整改路线图

2.梳理数据映射清单，识别个人数据处理场景

3.构建符合法规要求的组织架构及相应的职责分配

4.建立数据保护政策框架，包括隐私政策、同意书和数据处理协议等

5.设计完整的DPIA数据隐私评估工具，以满足定期审核的需要

6.确保数据主体对数据的访问、更正、删除的权利得到响应

7.全面开展培训和意识度培训，并形成长效机制

违规处罚

⚠ **罚款：**最高可达2000万欧元或全球营业额的4%

☒ **服务关停**

网络弹性法案（“CRA”）

欧盟范围内首部针对具有数字元素的有形和无形产品的专项立法，旨在为数字产品制造商引入通用网络安全规则。

- 生效日期：2024年12月10日
- 全面适用日期：2027年12月11日

适用范围

1.具备数字组件的**软（如：手机应用，云服务）硬（如：IoT 设备，智能家电）件产品**

2.类别：默认（如：一般智能家电）、I类（如：VPN）、II类（如：防火墙）、关键类（如：CPU，HSM）

3.豁免领域：医疗设备、航空器材、汽车

关键内容

1.出厂预设最高安全级别

2.限制非必要功能与数据收集

3.产品安全自我评估、第三方评估、监管复核

4.用户可清除个人数据

5.24小时报告漏洞

企业合规建议

1.开展差距分析，识别与法案要求的合规差距

2.识别并记录产品中包含的漏洞和组件，构建软件材料清单（SBOM）

3.设计、开发和生产数字产品时，应确保其符合基于风险的适当网络安全水平，确保其无已知漏洞且具有安全默认设置

4.针对产品所面临的风险，及时解决和修复漏洞，包括提供安全更新

5.根据法案的要求，在意识到数字产品存在可被积极利用的安全漏洞或数字产品发生安全事件后24小时内，通知欧盟网络安全局（ENISA）

违规处罚

⚠ **罚款：**最高可达1500万欧元或全球营业额的2.5%

☒ **限制或禁止产品销售、召回产品**