2026-HG-E020
EUN/AIA/GRC

区 域 国 别 研 究 报 告

上海市哲学社会科学规划办公室　　2026 年 8 月 10 日

欧盟《人工智能法》合规与风险防控研究报告

华东政法大学马克思主义学院、涉外法治研究院

上海市企业走出去综合服务平台

《区域国别研究报告》是上海市哲学社会科学规划办公室依托上海市各高校和科研院所专业研究力量，紧扣服务企业走出去现实需要，专为“上海市企业走出去综合服务平台”打造的区域国别研究品牌。

《报告》基于学者“在地研究”田野调研、企业出海实务经验以及其他信息，聚焦国别/区域、产业/行业、在地合规运营三类场景，推出三类系列成果。其中，**“国别报告”系列**以对象国政治、经济、社会、文化等内容为研究对象，重点围绕宏观经济形势、营商环境、中资企业经营状况、机遇挑战等维度，解析对象国各领域的发展态势，为企业海外布局提供决策参考；**“行业报告”系列**针对重点产业跨境布局或企业走出去的行业赛道，深入研判对象国的重点行业发展格局；**“合规报告”系列**回应企业海外合规运营实务关切，系统梳理对象国重点领域的监管要点，为企业在地运营提供应对策略参考。

摘　要

欧盟《人工智能法》（Regulation (EU) 2024/1689）是全球首部综合性人工智能监管法。该法建立了覆盖人工智能系统设计、投放、部署和使用全过程的横向监管框架，并通过市场准入形成广泛域外效力。该法以风险分级为主线，分别规制禁止性实践、高风险系统、特定透明度风险和最低风险应用，并对通用人工智能模型设置专门规则。2026 年 6 月，《人工智能数字综合修订案》出台。修订案推迟了两类高风险系统义务的适用日期。本报告以《人工智能法》及其附件、2026 年《修订案》、欧盟委员会（欧委会）实施指南、《通用人工智能行为守则》等为主要研究对象，以“条文-义务-场景”为分析主线，重点回应四个问题：第一，中资企业的产品、系统和模型是否落入《人工智能法》的适用范围及其风险层级；第二，提供者、部署者、进口商、分销商和授权代表分别承担何种义务；第三，通用人工智能模型规则、高风险符合性评定和修订后的适用时间表将如何影响产品架构、出海模式与合规预期；第四，企业应建立何种合规机制，以应对分阶段适用、标准滞后与执法强化并存的监管环境。

目　录

一、欧盟《人工智能法》基本框架

（一）适用范围

《人工智能法》第 2 条确立了广泛的属地和域外适用范围。其域外效力主要经由三条路径触发：其一，在欧盟市场投放人工智能系统或通用人工智能模型，无论其设立于欧盟境内还是第三国，均受该法约束；其二，设立或位于欧盟境内的部署者；其三，即便提供者与部署者均位于第三国，只要系统产生的输出在欧盟境内被使用，亦适用该法。路径三大幅压缩了第三国企业的规避空间。

（二）风险分级体系与核心义务

《人工智能法》通常被概括为四级风险结构。其中，不可接受风险对应禁止性规则；高风险对应严格的全周期义务；特定透明度风险对应信息披露要求；一般风险原则上不受强制约束。整体上，义务强度随风险水平提高而增加，体现了比例原则下的风险规制逻辑。

第一，禁止性实践。该法第 5 条禁止八类具有不可接受风险的人工智能实践。具体包括：（1）部署潜意识、有目的操纵或欺骗性技术，实质性扭曲个人或群体行为并造

成或可能造成重大损害；（2）利用年龄、残疾或特定社会经济处境所致的脆弱性；（3）依社会行为或人格特征对自然人进行评分，并导致脱离数据原始语境的不利待遇或不成比例的不利后果；（4）仅基于画像或人格特征评估、预测自然人实施犯罪的风险；（5）通过无差别抓取互联网或闭路监控影像中的面部图像，建立或扩充人脸识别数据库；（6）在工作场所与教育机构推断自然人情绪（医疗或安全目的除外）；（7）基于生物特征数据推断种族、政治观点、工会身份、宗教或哲学信仰、性生活或性取向的生物特征分类；（8）为执法目的在公共可达空间使用“实时”远程生物特征识别（限于寻找特定受害人、防止紧迫威胁、追缉重罪嫌疑人三类严格例外，并须经司法或独立行政机关授权）。欧委会于 2025 年 2 月发布专项指南，对各项禁止规则的构成要件和适用边界作出解释。2026 年《修订案》新增两项禁止规则。一是生成或操纵可识别自然人的非自愿亲密影像、视频、音频等材料；二是生成或操纵儿童性虐待材料。

第二，高风险系统。第 6 条通过两条路径界定高风险系统。一是附件一路径，即人工智能系统本身属于欧盟统一产品立法所规制的产品，或者构成其安全组件，并且相

关产品须依法接受符合性评定。典型领域包括医疗器械、体外诊断设备、电梯、无线电设备和民用航空。2026 年《修订案》将《机械条例》所覆盖的相关系统转入部门法监管路径，不再直接适用《人工智能法》的高风险实体要求。二是附件三所列的独立高风险系统，涉及生物特征识别与分类、关键基础设施、教育与职业培训、就业和劳动者管理、基本公共服务与私人服务、执法、移民庇护和边境管理、司法与民主程序等八个领域。高风险系统须满足第 8 至 15 条规定的实体要求，包括全周期风险管理、数据治理、技术文档、自动日志、使用说明、人工监督，以及准确性、稳健性和网络安全。提供者还须建立质量管理体系，完成符合性评定，加贴 CE 标识，并进行数据库注册。部署者则须依照使用说明运行系统，配置具备能力的人工监督人员，确保输入数据与预期用途相关，并妥善保存日志。公法机构、提供公共服务的私人主体，以及使用信用评分或人寿、健康保险风险评估系统的部署者，还须在使用相关附件三高风险系统前开展基本权利影响评估。

第三，透明度义务。第 50 条针对特定使用场景规定横向透明度义务。严格而言，第 50 条的透明度义务可与高风险分类交叉适用，并非独立、封闭的风险层级。该法

规定，与自然人直接交互的系统，须使自然人知悉其正在与人工智能交互；生成合成音频、图像、视频或文本的系统，其提供者须确保输出以机器可读格式标识为人工智能生成或操纵；部署者对深度伪造内容以及以告知公众公共利益事项为目的发布的人工智能生成文本负有披露义务，其中构成明显的艺术、创意、讽刺或虚构作品组成部分的，可以不妨碍作品呈现的适当方式履行；情绪识别与生物特征分类系统的部署者须告知受影响的自然人。

第四，最低风险应用。未触发上述义务的人工智能系统，原则上不承担额外义务。第 95 条鼓励企业和行业组织制定自愿行为准则，将高风险系统的部分要求推广至其他人工智能系统。

（三）通用人工智能模型专门规则

第五章针对作为技术底座的通用人工智能模型，区分了一般义务与系统性风险加重义务。一般模型提供者须编制技术文档，向下游提供必要信息，制定遵守欧盟版权法的政策，并公开训练内容摘要。但累计训练计算量超过 1025 次浮点运算的模型，原则上被推定具有系统性风险。其提供者还须开展模型评估和对抗性测试，识别并缓解系

统性风险，报告严重事件，并落实网络安全措施。第三国提供者原则上须在投放欧盟市场前委任欧盟授权代表。2025 年 7 月发布的《通用人工智能行为守则》为履行透明度、版权及安全义务提供合规路径。

（四）治理架构

《人工智能法》建立了欧盟集中协调与成员国分散执法相结合的治理架构。AI 办公室依据欧委会 2024 年 1 月 24 日决定设立，隶属于通信网络、内容与技术总司。欧委会对通用人工智能模型规则享有排他监督和执法权，并将具体任务交由 AI 办公室执行。欧洲人工智能委员会负责协调成员国立场，科学专家组与咨询论坛分别提供独立技术评估和利益相关方意见。成员国则须指定市场监督机关和通报机构，负责落实执法和相关责任。2026 年《修订案》进一步强化了集中执法。AI 办公室对两类系统取得排他管辖权：一是模型与系统由同一提供者或同一企业开发的通用人工智能模型下游系统；二是构成或嵌入超大型在线平台、超大型在线搜索引擎的系统。产品安全、关键基础设施、执法、边境管理、金融和司法等特定系统仍由国家机关监管。AI 办公室同时取得信息调取、调查、远程或现

场检查、接受约束性承诺、处以罚款和周期性罚款等执法权。

（五）处罚梯度

《人工智能法》第 99 条设置三档行政罚款。违反禁止性实践的，最高为 3500 万欧元；违法者属于企业时，也可按其上一财政年度全球营业额的 7%计算，以较高者为准。违反提供者、授权代表、进口商、分销商、部署者、通报机构或透明度义务的，最高为 1500 万欧元或全球营业额的 3%。向主管机关或通报机构提供错误、不完整或误导性信息的，最高为 750 万欧元或全球营业额的 1%。对中小企业及初创企业，各档罚款均以固定金额和营业额比例中的较低者为上限。2026 年修订将这一优惠部分扩展至小型中盘企业，但仅适用于第二、三档罚款。通用人工智能模型提供者由欧委会集中处罚，最高为 1500 万欧元或上一财政年度全球营业额的 3%，以较高者为准。该处罚体系具有明显的威慑取向，企业不能将固定罚款金额作为风险上限。

（六）分阶段适用时间表

协调标准、合规工具和成员国执行准备的滞后，推动欧盟调整高风险规则的适用时间。《修订案》放弃与标准就绪状况挂钩的“条件启动”，改用固定日期，以提高监管的可预期性。《修订案》将在《欧盟官方公报》公布后第三日生效。

主要适用节点如下：

2025 年 2 月 2 日：禁止性实践和人工智能素养义务适用；

2025 年 8 月 2 日：通用人工智能模型规则、治理架构、通报机构制度和一般处罚规则适用；

2026 年 8 月 2 日：第 50 条透明度义务适用，欧委会开始行使对通用人工智能模型提供者的罚款权。此前已投放市场的合成内容生成系统，须在 2026 年 12 月 2 日前满足机读标识义务；

2026 年 12 月 2 日：涉及非自愿亲密材料和儿童性虐待材料的新增禁止规则适用；

2027 年 8 月 2 日：存量通用人工智能模型完成合规；成员国至少设立一个人工智能监管沙盒；

2027 年 12 月 2 日：附件三独立高风险系统适用；

2028 年 8 月 2 日：附件一嵌入产品的高风险系统规则适用。

二、中资企业关键合规议题

（一）域外适用基本原则

按第 2 条的适用逻辑，中资企业至少会在以下四类场景中被纳入规制。一是向欧盟出口内嵌人工智能功能的硬件或软件产品，如智能家居、可穿戴设备、车载系统与企业级软件服务。只要其产品在欧盟市场“投放”，境内厂商即构成提供者，与其是否在欧盟设有实体无关。二是跨境提供通用人工智能模型或模型接口服务。三是在欧运营的平台、电商与物流子公司在招聘、风控、内容推荐等内部流程中部署人工智能系统，则构成部署者。四是系统本身部署于中国境内，但其输出内容被有意用于欧盟境内。上述判断均以系统或模型的投放与使用行为为准，企业组织形态上的“离岸”并不产生隔离效果。

价值链角色决定企业承担何种义务。提供者承担系统设计、符合性评定和上市后监督等主要责任；部署者承担合规使用、人工监督和日志保存等义务；进口商与分销商则以准入核验、信息留存、纠正措施和监管协作为主。授权代表负责在欧盟境内承接监管联系和特定程序性任务。角色认定应当逐一对应具体系统、业务场景和入市方式，

不能仅依据集团内部称谓或合同名称判断。

第三国高风险系统提供者须在系统进入欧盟市场前，书面委任设立于欧盟境内的授权代表。第三国通用人工智能模型提供者也负有相应义务，但不具有系统性风险且符合条件的自由开源模型除外。授权代表须核验和留存合规文件，回应主管机关请求，并配合调查和风险处置。相关文件原则上须保存十年。授权代表并不取代提供者，也不承接其全部实体责任。中资企业通过欧盟子公司、进口商、经销商、平台或其他中间主体入市，只会增加价值链角色和执法接口，不能消除境外提供者义务。

（二）高风险系统的评定

附件三与中资企业出海业务主要存在五类交集。第一，人力资源科技。包括招聘筛选、绩效评价、劳动关系决策，以及依据个人行为或特征实施任务分配和劳动者管理的系统。第二，教育科技。包括入学评估、学习成果评价、教育层级判断和在线考试监控。第三，金融科技。包括自然人信用评分，以及人寿和健康保险的风险评估与定价，但金融欺诈检测除外。第四，生物特征应用。包括远程生物特征识别、情绪识别和特定生物特征分类。仅用于确认

个人所声明身份的生物特征验证，不被列为高风险。工作场所或教育机构中的情绪识别，以及依据生物特征推断部分敏感属性，还可能触及第 5 条禁止性规则。第五，关键基础设施。包括用于关键数字基础设施、道路交通以及水、气、供热和供电管理的安全组件。

不同类型的高风险系统适用不同评定路径。附件一 A 节产品类系统适用相应部门立法的评定程序，并将《人工智能法》的实体要求纳入同一评定。附件三第 1 类生物特征系统在完整适用协调标准或共同规范时，可以选择内部控制或第三方评定；相关标准不存在、未被完整采用或受到限制时，则须依据附件七接受第三方评定。附件三第 2 至 8 类系统原则上采用附件六内部控制程序，无须公告机构介入。

（三）通用人工智能模型出海的专门义务

中资企业通过托管接口、模型授权或开源发布向欧盟提供通用人工智能模型，均可能构成市场投放。判断标准是模型是否在商业活动中首次向欧盟市场提供，是否收费并非决定性因素。自由开源豁免具有严格条件。模型须采用允许访问、使用、修改和分发的自由开源许可，并公开

权重、架构和使用信息，方可免除技术文档、下游信息提供及授权代表义务。版权政策和训练内容摘要义务仍须履行。具有系统性风险的模型不得适用上述豁免。累计训练计算量超过10^{25}次浮点运算的模型，原则上被推定具有系统性风险；提供者须在达到或者知悉即将达到门槛后两周内通知欧委会。未达到该门槛的模型也可能基于能力、影响范围等因素被指定为系统性风险模型。

《通用人工智能行为守则》属于自愿合规工具。签署并遵守守则，可以作为证明履行技术文档、下游信息、版权政策及系统性风险义务的方式，有助于降低行政负担并提高监管可预期性，但不产生法定的合规推定。训练内容摘要仍须依欧委会模板单独编制和公布。不签署守则并不构成违法，但企业须提出其他充分的合规措施，并向欧委会证明其适当性。

（四）执法不确定性

当前不确定性主要来自三个方面。**第一，协调标准尚未完整发布。**风险管理、数据治理、技术文档、人工监督和网络安全等要求的技术落实方式，仍将受到后续标准内容和发布时间的影响。**第二，附件一产品同时受到《人工**

智能法》和部门产品立法约束。2026 年《修订案》允许欧委会在部门法已提供等效保护时，通过授权立法限制部分重复义务，并要求其最迟于 2027 年 8 月 1 日前发布合规指南。因此，不同行业的最终合规界面仍需结合后续授权立法、指南和部门标准判断。**第三，欧委会指南、标准化成果、行为守则和技术模板仍在持续更新。**企业不能将一次性法律审查等同于持续合规，而应建立法规监测、版本比对和内部规则更新机制，确保产品设计与文件体系同步调整。

《人工智能法》是以风险、用途和价值链角色为基础的横向立法，企业国籍并非其法定分类或处罚标准。目前亦无充分证据表明欧盟将基于企业的中国背景实施差别化执法。欧盟自 2019 年起将中国同时定位为合作伙伴、经济竞争者和“制度性对手”，此后又将“去风险”、经济安全和关键依赖控制纳入对华政策框架。针对中资企业的选择性监管有潜在可能性。

三、实操建议

（一）进入欧盟市场前的合规评估

第一，建立人工智能资产清单与风险筛查机制。人工智能资产识别是入市合规的起点。企业应建立覆盖对欧业务的系统与模型清单，包括对外销售的软件和智能硬件、在欧子公司使用的内部工具，以及对外提供的模型、接口和云服务。在此基础上开展五步筛查：一是判断对象是否属于人工智能系统，排除仅执行基础数据处理或完全依照人工设定规则运行、缺乏推断能力的传统软件；二是核查是否触及禁止性实践；三是依据附件一、附件三和第 6 条第 3 款判断高风险属性；四是识别第 50 条透明度义务；五是判断是否涉及通用人工智能模型及系统性风险。欧委会的人工智能系统定义指南属于非约束性解释文件，可作为边界判断的重要依据。企业应对筛查过程和依据形成分级记录。对不属于人工智能系统、未触发透明度义务等结论，建议保留内部评估记录。提供者依据第 6 条第 3 款认定附件三所列系统不构成高风险的，则须在投放或投入使用前形成书面评估，并完成欧盟数据库登记。

第二，明确价值链角色并实施设计端排除。企业应逐

系统、逐市场绘制提供者、部署者、进口商、分销商和授权代表的角色地图。合同可约定文件提供、技术协助和损失分担，但不能对抗法定角色认定。贴牌销售、商标变更、重大修改或预期目的调整，均可能使原进口商、分销商或部署者转化为提供者。第三国高风险系统提供者应在产品进入欧盟市场前委任欧盟授权代表。第三国通用人工智能模型提供者原则上也负有同类义务。禁止性功能应在设计端予以排除。工作场所情绪识别、敏感属性生物特征推断等功能，应在欧盟版本中技术禁用或实施可靠的地理隔离，不能仅依靠用户协议限制用途。

第三，审慎选择进入欧盟市场的模式。不同入市模式决定责任配置和监管接口。境内企业以自身名称直接投放产品的，通常构成提供者；有形产品进入欧盟市场时，通常还会形成欧盟进口商角色。由欧盟子公司入市的，只有在子公司开发或委托开发系统，并以自身名称或商标投放时，才构成提供者；仅承担进口或销售职能的，仍属于进口商或分销商。由欧盟合作方以自身品牌投放的，合作方可能成为提供者。在高风险系统场景下，境内技术供应方与欧盟合作方应依据第 25 条，以书面协议明确技术文档、系统访问和持续协助责任。欧盟子公司或合作方架构可以

缩短监管沟通链条，但不能当然消除境内企业的协作责任，也不能当然将罚款计算范围限定于欧盟子公司单体。

（二）日常运营的合规机制

第一，建立质量管理与内部治理体系。高风险系统提供者应依第 17 条建立质量管理体系，覆盖合规策略、设计开发、数据治理、风险管理、上市后监测和严重事件报告。企业可参考 ISO/IEC 42001 搭建人工智能管理框架，并与既有质量管理体系衔接。但国际标准本身不产生《人工智能法》下的合规推定，仍须按照后续协调标准和欧盟规则逐项核验。企业宜设立跨部门人工智能合规机制，由法务、产品、工程、数据和安全部门共同参与。内部制度应明确决策责任、风险升级、暂停使用和例外审批权限。会议记录、测试报告和决策依据应同步归档，避免管理制度与实际运行相脱节。

第二，完善文档、日志与登记管理。技术文档应随系统版本持续更新，并纳入配置与变更管理。提供者须自高风险系统投放市场或投入使用后保存技术文档、质量管理文件和符合性材料十年。提供者和部署者对其控制范围内的自动日志，原则上均须保存至少六个月；其他法律规定

更长期限的，从其规定。附件三高风险系统原则上须在投放市场或投入使用前完成欧盟数据库登记。依据第 6 条第 3 款主张系统不构成高风险的提供者，也须登记其判断及理由。2026 年《修订案》仅简化后一类登记的信息要求，并未取消登记义务。企业应建立文档、日志、登记信息和产品版本之间的对应关系，确保监管调查时能够完整还原系统状态。

第三，运行入市后监测与事件响应机制。提供者须建立与系统风险相适应的入市后监测机制，持续收集和分析系统运行数据，并将监测计划纳入技术文档。2026 年《修订案》将原定的统一实施模板改为欧委会指导文件，并要求其中包含可供企业使用的模板。企业在相关指导发布前，仍应根据产品风险自行设计监测指标、数据来源和复审周期。严重事件应在确认系统与事件存在因果关系或合理可能性后立即报告，最迟不得超过知悉事件后 15 日。涉及广泛侵权，或者严重且不可逆地扰乱关键基础设施运行的，最迟为 2 日；造成人员死亡的，最迟为 10 日。企业可设置“24 小时内部上报、48 小时初步定性”的内部目标，并预先确定调查、报告、整改、停用和召回责任人。

第四，将部署者义务嵌入日常流程。在欧子公司使用

外购高风险系统时，应将第 26 条要求转化为标准操作流程。具体包括，依照使用说明运行系统；指定具备能力、培训和权限的人员实施监督；确保可控输入数据与预期目的相关且具有充分代表性；监测系统运行；保存日志至少六个月；在工作场所使用前告知受影响劳动者及其代表。系统可能产生法定风险时，应暂停使用，并及时通知提供者、分销商和市场监督机关。公法机构、公共服务提供者，以及使用信用评分、人寿或健康保险风险评估系统的部署者，还应在使用前开展基本权利影响评估。采购阶段则宜核验提供者身份、CE 标识、符合性声明、使用说明和数据库登记状态，并在合同中约定持续监测、事件通报、技术支持和整改责任。需要区分的是，公共机关不得使用应登记而未登记的系统；对一般私人部署者，上述核验主要属于降低采购和使用风险的审慎措施。

（三）分阶段时间表下的合规排期

第一，优先落实 2026 年近端义务。2026 年 8 月 2 日是当前最紧迫的合规节点。自该日起，第 50 条透明度义务全面适用。对话式产品应完成交互身份告知，情绪识别和生物特征分类系统应建立受影响人告知机制，新投放的

生成式系统应具备合成内容机读标识功能。同日起，欧委会开始全面执行通用人工智能模型规则，并可以依法实施罚款。2026 年 8 月 2 日前已投放市场的生成式系统，可在 12 月 2 日前完成第 50 条第 2 款规定的机读标识改造。2026 年 12 月 2 日起，生成或操纵非自愿亲密材料和儿童性虐待材料的新增禁止规则适用。生成式产品应在此前完成风险测试并设置分层防护。仅通过用户协议禁止相关用途，通常不足以证明提供者已采取合理且充分的保障措施。通用人工智能模型企业还应在 2026 年 8 月 2 日前确定是否加入《通用人工智能行为守则》，并建立训练计算量监测和内部升级机制。模型达到或者预计达到系统性风险推定门槛时，应确保两周通知义务能够及时履行。

第二，倒排高风险系统合规工期。附件三系统和附件一产品类系统的相关义务，分别自 2027 年 12 月 2 日和 2028 年 8 月 2 日起适用。数据治理、风险管理和技术文档积累周期较长，应优先启动。可能需要第三方评定的生物特征系统，还应提前确认评定路径和通报机构安排，避免集中申报造成延误。企业应将存量过渡安排纳入版本管理。相关日期前已有同一类型和型号的系统合法投放市场或投入使用，且设计保持不变的，后续同型号产品原则上可

以继续投放。适用日后发生重大设计变化的，则须全面履行高风险系统义务。因此，每次功能升级均应经过技术与法律联合审查，并形成版本差异和风险判断记录。合理安排版本冻结和升级时间并不当然构成规避，但排期依据应当真实、完整且可供复核。企业还应持续跟踪协调标准的制定进程。有条件的企业可通过欧洲子公司、行业协会或标准化机构参与草案评议，提前识别技术要求，降低正式标准发布后的改造成本。

第三，建立规则跟踪机制。企业应建立统一的监管响应和规则监测机制。建议设置单一对外接口，预先确定授权签署人、本地法律顾问和翻译支持，并将内部响应时限设置为短于法定期限。近端义务实施阶段宜按月跟踪欧委会指南、实施和授权法案、协调标准及技术模板。标准发布、监管文件更新或产品发生重大迭代时，应立即重新开展合规差距评估。

结　语

《人工智能法》正在重塑人工智能产品和服务进入欧盟市场的基本条件。对中资企业而言，其影响可概括为三点。第一，企业合规成本结构性上升，但监管时间表趋于明确。第二，高风险系统规则延期不等于《人工智能法》整体延期。第三，欧盟合规能力具有跨市场复用价值。围绕风险管理、数据治理、技术文档和人工监督建立的制度体系，不仅服务于欧盟市场准入，也可为企业应对其他法域不断扩展的人工智能监管提供基础。

不同企业应根据业务类型配置合规资源。未落入高风险范围但触发第 50 条义务的企业，应优先完成交互告知、合成内容标识和内部人工智能素养建设，并将禁止性功能清单嵌入产品评审流程。附件三高风险系统提供者应立即启动合规排期，优先处理数据治理、风险管理和技术文档。通用人工智能模型提供者面临更紧迫的时间压力，应尽快完成版权政策、训练内容摘要、行为守则选择和系统性风险门槛监测。在欧子公司则应将部署者义务纳入采购、使用、人工监督和事件响应流程。

各类企业的共同任务，是建立可以持续验证的合规证

据链。在以文档和可追溯性为基础的监管体系中，制度是否真实运行，比制度是否形式存在更为重要。因此，企业应将合规要求嵌入产品全生命周期，而非在市场投放前集中补充文件。

未来一段时期，企业应重点跟踪三项变量：协调标准和欧委会指南的发布进度、产品部门法与《人工智能法》的衔接安排，以及成员国执法资源和案件优先事项的差异。2026 年 7 月发布的高风险系统指南仍处于征求意见阶段，说明部分分类边界和操作要求仍在细化。企业应建立常态化规则监测和触发式复核机制，在标准、指南或产品功能发生重大变化时，及时更新风险判断与合规方案。

关键提示

第一，本报告所引法规与数据截至 2026 年 7 月 16 日。2026 年《修订案》经欧洲议会（6 月 16 日）与理事会（6 月 29 日）批准后刊载《欧盟官方公报》生效，其正式编号与个别条文的最终表述以公报文本为准；协调标准清单、实施指南与模板处于滚动更新之中，适用前应核对最新版本。

第二，高风险义务的延期不改变其余义务的实施节奏。禁止性实践自 2025 年 2 月 2 日起已经适用，透明度义务与欧委会对通用模型提供者的执法权自 2026 年 8 月 2 日起适用，合成内容机读标识义务与新增禁止情形自 2026 年 12 月 2 日起适用。

第三，部分企业设想借助欧盟进口商或分销商“间接入市”以规避提供者义务，该路径并不可行。提供者身份取决于系统以谁的名义或商标投放市场，而非合同上的身份安排。同时，第 23 条、第 24 条要求进口商与分销商在经手之前核验符合性评定、技术文档与 CE 标识，欧盟交易方必然通过合同将合规要求与违约责任向上游转嫁，合规成本终将回到境内厂商。

第四，《人工智能法》合规不替代 GDPR、《数字服务法》与部门产品立法等既有欧盟法义务。两套体系叠加适用、须并行满足。

第五，本报告系一般性研究分析，不构成针对具体交易或个案的法律意见；企业作出重大合规决策之前，应结合具体事实征询具有欧盟执业资质的专业机构。

附件：核心数据来源

1.欧盟《人工智能法》（Regulation (EU) 2024/1689）。

2.欧盟《人工智能数字综合修订案》（Digital Omnibus on AI）及其立法文件，包括欧盟委员会提案 COM(2025) 836 final 和欧洲议会、欧盟理事会通过的 PE-CONS 30/26 文本。

3.欧盟委员会发布的《人工智能系统定义指南》《禁止性人工智能实践指南》。

4.欧盟委员会发布的《通用人工智能模型提供者义务范围指南》《通用人工智能行为守则》及《通用人工智能模型训练内容公开摘要说明与模板》。

5.欧盟委员会《设立欧洲人工智能办公室的决定》（C(2024) 390 final），以及欧盟委员会官方网站发布的《人工智能法》治理架构、执法机制、实施时间表与监管沙盒等资料。

6.欧盟委员会关于高风险人工智能系统的标准化请求（C(2025) 3871 final），以及欧洲标准化委员会（CEN）和欧洲电工标准化委员会（CENELEC）发布的相关标准化文件。

7. 欧盟《通用数据保护条例》（Regulation (EU) 2016/679）、《数字单一市场版权指令》（Directive (EU) 2019/790）、《数字服务法》（Regulation (EU) 2022/2065）及《机械条例》（Regulation (EU) 2023/1230）。

王志鹏（华东政法大学马克思主义学院）
曲光毅（华东政法大学涉外法治研究院）

联系地址：淮海中路 622 弄 7 号 308 室

联系电话：021-33165460

联系邮箱：zbzh@sh-popss.gov.cn