关于负责任地使用人工智能技术的政策

信息技术 | 发布日期：2026 年 1 月 21 日 | 修订记录：无

本政策确立了麦格纳在运营、产品和业务流程中，负责任地使用和开发人工智能解决方案的承诺。这些解决方案虽能创造价值，但也可能为麦格纳、全体员工及其他利益相关方带来法律、声誉及其他潜在风险。严格遵守本政策，是推动人工智能安全合规应用、最大化价值机遇、最小化潜在风险的关键前提。

政策适用范围

本政策适用于麦格纳国际及其全球所有运营集团、分支（包括控股合资企业）、子公司及其他业务实体。本政策同样适用于所有代表麦格纳开展工作的人员，包括麦格纳全职/兼职员工、独立承包商、管理人员、董事、顾问和代理人——在本政策中，上述人员统称为“你”或“麦格纳相关人员”。

本政策明确了你在以下人工智能相关工作中，需遵循的负责任、合伦理、安全可控的使用与开发要求：

- 所有**人工智能解决方案**，包括**传统人工智能系统、生成式人工智能系统、人工智能体**和**智能型人工智能**;
- 任何由**人工智能解决方案**生成的**人工智能输出成果**。

人工智能解决方案的“使用”，指你运用麦格纳或第三方开发的现有**人工智能解决方案**，执行以下任务：

- 简单任务：如生成电子邮件或或图像、文本摘要、问题应答等；
- 复杂任务：如为麦格纳产品研发、业务流程优化和制造自动化项目提供技术支持等。

人工智能解决方案的 “开发”，指你与解决方案进行深度交互，具体涵盖以下任一行为：

- 制定**人工智能解决方案**的规范;
- 构建、设计、优化或训练**人工智能解决方案**的模型和算法;
- 采集、处理或训练**人工智能解决方案**的基础数据集;
- 测试或验证**人工智能解决方案**的功能与性能；
- 使用第三方工具开展**开发**工作。

人工智能解决方案的**开发**用途包括：

- 仅供内部使用（例如制造自动化）；
- 供外部利益相关方使用（如客户、供应商及其他商业合作伙伴）；
- 集成至麦格纳产品中。

人工智能解决方案的**开发主体**包括：

- 麦格纳内部人员（例如通过英伟达 Isaac Sim 等第三方工具，或CATIA 等传统系统的人工智能功能进行开发）；
- 为麦格纳提供服务的第三方合作方；
- 麦格纳员工与第三方开发人员组成的联合团队。

除 “使用”和“开发”外，本政策中所有加粗标注的术语定义，详见本政策**附录 A**。

麦格纳负责任地使用人工智能技术准则

在实现**人工智能**生产力价值的同时降低风险、保障员工安全，是麦格纳的核心目标。你需要严格遵守以下原则与规范，为达成上述目标发挥关键作用：

1. 理解并管控人工智能解决方案的使用风险

人工智能解决方案的应用存在多重风险，你需要充分认知并协助管控，具体包括：

- **偏见：人工智能解决方案**可以学习并强化训练数据中的隐含偏见，进而导致结果偏差与非预期后果（如招聘决策中的歧视性倾向）。你必须时刻警惕偏见风险，以审慎态度评估**人工智能输出成果**是否存在偏见。
- **网络安全威胁：人工智能解决方案**可能被用来发动网络攻击、窃取身份信息、破坏系统安全。你不能将**人工智能解决方案**用于任何非法用途。同时，严禁在**人工智能解决方案**中安装未经授权的插件、连接器、附加组件或应用程序编程接口，以此助力麦格纳抵御网络攻击及其他外部威胁。
- **缺乏透明度：人工智能**算法的运行逻辑尚未被充分理解，且常常产生有缺陷的**人工智能输出成果**。如下文所述，你必须对**人工智能输出成果**进行监督，以确保其准确性、可靠性、相关性、无偏见性，且符合既定使用场景要求。
- **保密性和数据隐私：**许多**人工智能解决方案**在使用过程中会采集数据，可能导致开发者接触机密数据、受法律保护的数据及个人信息。你必须禁止第三方**生成式人工智能系统**，利用**麦格纳所有或管控的输入数据**（含麦格纳相关人员的个人信息）开展模型训练、开发或修订工作。
- **知识产权：生成式人工智能系统**生成的**输出成果**，可能侵犯第三方知识产权。例如，未恰当引用标注的文本内容、未经授权使用或复制的图像、艺术品、设计方案、软件代码等素材，以及涉嫌侵犯第三方专利的产品设计或工艺方案。

  你不得采用侵犯第三方知识产权（包括版权、专利权、设计权和商标权）的方式，使用**人工智能解决方案**及**输出成果**。

  此外，若使用**人工智能解决方案**创作需受知识产权法保护的工作成果，你必须与麦格纳集团知识产权法务团队协作，确保麦格纳对基于**人工智能输出成果**形成的工作成果享有合法保护权。

2. 履行监督管理职责

人工智能输出成果在最终定稿、采信和内外部共享之前，都需要严格的人工审核。鉴于你需要对工作中使用的**人工智能输出成果**承担责任，在采用相关成果前，务必开展审慎评估、逻辑分析与合理判断。

对于已知违反适用法律、侵犯他人权利，或可能损害麦格纳声誉的**人工智能输出成果**（如侵犯他人著作权或商标权的内容），严禁采信使用。若经合理核查后，仍无法确认**人工智能输出成果**的有效性，尤其是在涉及重大法律或声誉风险的情况下，不得采信该成果。

3. 使用麦格纳核准的人工智能解决方案

麦格纳已对多款**人工智能解决方案**开展合规性验证，以确保符合我们的网络安全标准以及保密和数据隐私政策。你应该尽可能使用麦格纳**认可的人工智能解决方案**，包括：

- **MAVIS;**
- 微软 M365 Copilot 和 Copilot 聊天助理;
- GitHub Copilot 代码与编程助理;
- 微软 Azure 人工智能基础模型平台;
- 亚马逊 Bedrock 基础模型访问与管理服务；
- DataBricks平台。

如果你计划使用**人工智能解决方案**，且拟输入麦格纳所有或管控的数据，必须首先在麦格纳 **AI MagNET – 人工智能解决方案及技术（ AI Solutions and Technologies）**确认该工具是否列入核准清单。如果尚未获批，你需在 **MagNet** 提交申请并遵循相应的审批流程。

向未核准的**人工智能解决方案**录入的任何**输入数据**，均无保密保障，可能导致麦格纳知识产权保护权益受损。

4. 禁止使用场景

你不得使用**人工智能解决方案**从事任何违反法律规定，或损害麦格纳声誉的行为，包括各类欺诈、歧视、骚扰、威胁、霸凌及其他有害行为。此外，严禁使用**人工智能解决方案**进行以下操作：

- 以有害方式操纵他人行为或利用他人弱点，包括利用年龄、残障状况、特定社会经济背景等方面的弱势；
- 以可能导致歧视或伤害的方式，对他人进行评估或分类，包括基于社会行为或个人特征的评判；
- 通过无差别抓取人脸图像，创建面部（情绪）识别数据库；
- 在工作场所对他人进行情绪识别；
- 基于敏感或法律保护的个人特征，包括种族、宗教、年龄、性取向、政治观点等，对他人进行分类并可能由此引发歧视或伤害。

5. 包含人工智能免责声明

在任何涉及**人工智能解决方案**的情况下，你都应该添加**人工智能**免责声明，如果不这样做可能会对他人造成合理伤害或误导。

- **法律要求：**在任何**适用法律**要求包含免责声明的情况下，你必须严格执行。
- **最佳实践：**对于日常邮件等常规内容，一般无需添加声明；对于面向公众或对业务有重大影响的场景（如高度依赖**人工智能**生成的内容、可能对决策产生重大影响的成果），则**应**考虑添加声明。

其他**必须**添加**人工智能**免责声明的特定情形，包括：

- **人工智能解决方案**与人类直接交互（如聊天机器人），且具备合理认知能力的人员无法明确识别交互对象为**人工智能**时；
- 您使用或发送的**人工智能输出成果**包括经过篡改的图像、音频或视频，且该内容足以以假乱真或被合理认为真实时；
- **人工智能输出成果**拟作为事实性或权威性内容，向内外部利益相关方发布涉及公共利益的信息（如影响客户或其他利益相关方的产品、服务、安全相关沟通内容）时。

建议采用以下声明模板：“以下内容由人工智能解决方案生成。”

本要求存在部分例外情形：若**人工智能**生成文本经过人工审核编辑，且审核人承担编辑责任，则无需标注；若交互场景中**人工智能**属性已明确可知，亦无需添加声明。

6. 人工智能解决方案的采购与开发流程

如果你计划采购（包括购买、许可、订阅）或开发/联合开发**人工智能解决方案**，需通过麦格纳 **AI MagNET – 人工智能解决方案及技术（ AI Solutions and Technologies）**的指定链接，严格遵循麦格纳人工智能解决方案审批流程。

这一过程包括两个重要步骤：

- **第一步**：对计划开展的**人工智能**项目、创意构想及应用场景进行备案管理，提升工作透明度，评估商业价值与财务可行性，减少重复投入，强化治理与风险管理；
- **第二步**：对经审核的**人工智能解决方案**，完成文档编制、类别划分及风险评估工作。

根据你在人工智能解决方案采购或开发工作中承担的角色，你可能被认定为该解决方案的 “开发者”，并需据此遵守本政策、麦格纳负责任地使用人工智能技术政策、人工智能开发者规程及《欧盟人工智能法案》（EUAIA）的相关要求。

7. 人工智能智能体

你可以通过麦格纳核准的**人工智能解决方案**，使用为满足特定工作需求而开发的**人工智能智能体**。**人工智能智能体**属于人工智能解决方案范畴，完全适用本政策的各项规定。

若你作为业务负责人，拟部署**人工智能智能体**供个人或团队使用，需通过上文第 6 条所述的两个步骤，事先获得审批。同时，在**人工智能智能体**全生命周期内（从初始设计到系统退役，含智能体间通信环节），你需协调技术团队完成必要的监控与监督工作，确保其符合治理要求、企业信息技术标准及相关指南，且遵循**负责任地使用人工智能技术政策**。此外，你还需严格执行**《人工智能开发者规程》**中关于**人工智能智能体**的其他管理要求。

补充说明

1. 遵守麦格纳政策及适用法律

在**使用**或**开发人工智能解决方案**的所有场景中，你必须严格遵守**适用法律**、麦格纳**负责任地使用人工智能技术政策**及其他相关政策（如《保密信息政策》、《数据隐私政策》等）。相关法律及麦格纳政策清单详见本政策**附录 B**。此外，麦格纳及本政策适用人员的相关义务，均需以适用法律为前提。若本政策与适用法律存在冲突，应在**适用法律**要求的前提下，尽可能贴合本政策的核心宗旨进行解读。

2. 遵守客户、供应商及其他第三方要求和保密协议

在**人工智能解决方**案中处理第三方数据与信息时，你必需严格遵守合同约定的限制条款与禁止性规定。在部分情形下，向**人工智能解决方案**输入第三方数据可能违反保密协议或其他保密约定，此类操作均被禁止。你应与事业部、地区或公司法务部门充分沟通，明确相关保密义务、限制条件及合同约束条款，避免麦格纳违反合同承诺。同时，你必须严格遵守《麦格纳保密政策》。

3. 培训

麦格纳将提供资源和培训，帮助你更好地理解人工智能解决方案的能力边界与局限性。你需要按时完成所有必要的培训。

4. 报告机制

在开发**人工智能解决方案**过程中，若遇系统故障，或发现存在偏见、有害性、失实性、异常性的**人工智能输出成果**，必需及时监控、记录并上报。多数情况下，可通过**人工智能解决方案**内置的报告功能直接提交；若系统无相关功能，或你认为风险 / 后果较为严重，可通过**麦格纳热线**的**数据隐私/人工智能相关问题**板块进行上报。

如果你发现任何涉嫌违反本政策或侵犯麦格纳知识产权的行为，，应立即通过**麦格纳热线**进行报告。

根据所在地区及具体情形，你可能需要向相关政府机构履行报告义务。本政策的任何条款，均不限制你以个人身份与政府机构进行沟通。

5. 合规监督

麦格纳保留对相关人员遵守本政策情况的监督权利。公司将建立健全管理机制，预防、监控并应对人工智能解决方案相关事件，包括损害性输出、偏见性输出及安全、保密、数据隐私泄露事件。

6. 违规责任

若违反本政策条款，你将受到相应纪律处分，情节严重者可能被解除劳动合同。

7. 咨询方式

如需获取更多信息或相关指导，请联系指定的**全球人工智能负责人**，或发送邮件至：**ai.governance@magna.com**。

发布时间：	2026 年 1 月 21 日
修订记录：	无
下次复审时间：	2027 年第一季度
发布部门：	人力资源与信息技术
批准部门：	人力资源与信息技术

附录 A – 术语定义

智能型人工智能（Agentic AI）：指具备一定自主规划、行动及任务执行能力，且始终处于人类监督之下的**人工智能解决方案**（即**智能型人工智能**是一种能够自主行动、规划流程、实现目标的技术能力）。

人工智能（AI）：即人工智能技术的统称。

人工智能智能体（AI Agents）：指在受控参数范围内，运用智能技术代表用户执行特定任务或工作流程的专用工具或系统（即**人工智能智能体**是实际应用中承载智能能力、执行任务的工具或系统）。典型示例包括：微软 Teams 中用于会议排期、员工咨询应答的**人工智能智能体**，以及各类专业**人工智能**助手等。

人工智能开发者规程（AI Developer Procedures）：即麦格纳制定的**人工智能开发者规程**。

人工智能输出成果（AI Outputs）：指由**人工智能解决方案**生成的各类内容（包括文本、图像、音频、视频、软件代码）、结果、建议、决策及其他输出形式。

人工智能解决方案（AI Solution）：指所有人工智能相关的系统、功能、应用场景、产品、平台及工具，涵盖**传统人工智能系统**、**生成式人工智能系统**、**人工智能智能体**及**智能型人工智能**。

适用法律（Applicable Law）：定义详见本政策**附录 B**。

核准人工智能解决方案（Approved AI Solutions）：指符合麦格纳信息技术安全协议及保密要求，且已通过核准、部署用于麦格纳业务运营的人工智能解决方案。麦格纳**核准人工智能解决方案**清单可在**此处**查阅**。**

人工智能解决方案的 “开发”：指你与解决方案进行深度交互，具体涵盖以下任一行为：：

- 制定**人工智能解决方案**的规范;
- 构建、设计、优化或训练 **人工智能解决方案**的模型和算法;
- 采集、处理或训练支撑**人工智能解决方案**的基础数据集;
- 测试或验证**人工智能解决方案**的功能与性能；
- 使用第三方工具开展**开发**工作。

人工智能解决方案的**开发**用途包括：

- 仅供内部使用（如制造自动化场景）；
- 供外部利益相关方使用（如客户、供应商及其他商业合作伙伴）；
- 集成至麦格纳产品中。

人工智能解决方案的**开发主体**包括：

- 麦格纳内部人员（例如通过英伟达 Isaac Sim 等第三方工具，或CATIA 等传统系统的人工智能功能开展开发）；
- 为麦格纳提供服务的第三方合作方；
- 麦格纳人员与第三方开发人员组成的联合团队。

《欧盟人工智能法案》（EUAIA）：即欧盟颁布的人工智能专项法规。

生成式人工智能系统（Gen AI Systems）：指主要基于数据学习的模式，具备生成新内容（如文本、图像、音频、视频、代码等）或自主规划执行多步骤任务以实现目标的能力，而非仅对现有数据进行分析或分类的**人工智能解决方案**。

输入数据（Inputs）：指录入**人工智能解决方案**的各类输入信息、数据、查询指令、命令、资料及文档。

麦格纳（Magna）：指麦格纳国际及其全球所有事业部、分支（含控股合资企业）、子公司及其他业务实体。

麦格纳所有或管控的输入数据（Magna-owned or controlled inputs）：指由麦格纳保管、占有或管控，且归属于麦格纳、麦格纳相关人员、麦格纳客户、供应商及其他商业合作伙伴的各类数据、信息及文档。

麦格纳相关人员（Magna Persons）或你（you）：指所有代表麦格纳开展工作的人员，包括麦格纳全职 / 兼职员工、独立承包商、管理人员、董事、顾问及代理人。

MAVIS：指麦格纳自主研发的人工智能虚拟信息系统助手。

负责任地使用人工智能技术政策（RAI Principles）：即麦格纳制定的**负责任地使用人工智能技术的专项政策**。

传统人工智能系统（Traditional AI Systems）：指基于统计 / 机器学习模型及规则化逻辑，对现有数据进行分析或分类，进而输出预测结果、建议方案或决策依据的**人工智能解决方案**。此类系统不具备生成新内容或自主规划执行多步骤任务的核心能力。

人工智能解决方案的 **“使用”**：指你运用麦格纳或第三方开发的现有**人工智能解决方案**，执行以下任务：

- 简单任务：如生成电子邮件或图像、文本摘要、问题应答等；
- 复杂任务：如为麦格纳产品研发、制造自动化项目提供技术支持等。

附录 B – 适用法律**及麦格纳相关政策**

适用法律

“**适用法律（Applicable Law）**”：指所有不时生效的、与**人工智能解决方案**的选型、使用、开发及部署相关的法律、法规、规章、条例、法令、指令、判决、指南及政府要求，包括：

- 欧洲议会及欧盟理事会 2024 年 6 月 13 日颁布的《欧盟人工智能法案》（法规编号：(EU) 2024/1689）

麦格纳相关政策

- **《麦格纳保密信息政策》**
- **《麦格纳信息披露政策**》
- **《麦格纳数据隐私与保护政策、规程及指南**》
- **《麦格纳信息分类政策**》
- **《麦格纳安全政策**》
- **《麦格纳全球电子邮件、互联网/内联网及社交媒体政策**》
- **《麦格纳信息技术 / 运营技术安全政策》**
- **《麦格纳网络安全事件响应政策**》
- **《麦格纳健康、安全与环境政策》**