



架构

公共部门的AI代理

面向技术负责人的变革性多智能体平台详细指南



里面有什么

引言	01
----	----

人工智能代理为何重要 02

超级充电过程 语言、数据和上下文：自动化密钥 03	02
---------------------------	----

什么是AI代理？ 04

人工智能代理的解剖学 人工智能的演变：代理式人工智能中的自主性等级 07 多代理架构5 跨组织的代理空间合作 10 本地部署与云端 平台概述：自动化与代理智能的融合 13	09
	12

人工智能的真实面貌就是这样 14

公共部门现实中的用例	
使用ChatGPT和Zapier自动发布社交媒体帖子 15 处理公民邮件 16 通过WhatsApp自动抄表读数 17 使用Relevance AI自动化服务 18	

监控和仪表盘 21

批判性反思与局限性 22

从自主视觉到行动	23
六步公共部门领导者现在应采取的行动	

摘要与展望	27
我们从人工智能代理的崛起中学到了什么	

引言

公共部门正面临严重的技能型劳动力短缺，由于持续的人口结构变化，这一问题正在加剧。为应对此问题，增加自动化至关重要，使公共机构能够用更少的人员更高效地处理任务。

人工智能代理听起来很未来——而且确实如此。想想全自动流程和能自行解决问题的智能助手。这正是人工智能代理能带来的。那么你为什么应该关心呢？因为人工智能代理将你的自动化提升到了全新水平。

没有人工智能的自动化，就像电脑时代使用打字机一样；它比手写好，但它错失了现代技术所提供的变革潜力与效率。

现代自动化平台提供了一个坚实的基础：你构建工作流、传输数据、并自动化重复性任务。但当你们将AI代理集成到这些工作流中时，真正的转型才会发生——这些代理分析数据、做出决策、并以手动无法达到的精准度实时优化流程。

近期，毕马威研究学院的研究表明，公共部门组织已意识到这一潜力：90%的受访者计划在接下来的2-3年内实施代理式人工智能。¹ 但该领域发展迅速。代理式人工智能的概念仍在形成中，且通常较为复杂。许多解决方案是实验性的、零散的或技术性过深——这使得定位变得困难。这就是为什么我们在这一观点中强调清晰度：我们展示了典型的架构，比较了核心技术，并展示了人工智能代理如何在实践中跨领域、跨场景工作。

尽管存在日益壮大的商业平台生态系统——从开源到企业级——我们的目标在这里是展示什么是可能的，而不是描述单一解决方案。从公民与政府服务的互动到内部工作流程和非公开用例，代理方法重塑了我们对自动化的思考方式。

从这个角度来看，我们将阐明是什么让人工智能代理如此强大，它们如何运作，以及您如何巧妙地将它们集成到您的自动化战略中。无论是用于通信、数据处理还是创造性任务，它们所提供的可能性是无限的。

我们将探索跨领域的实际应用案例，包括公共服务领域，人工智能代理在公民沟通和行政效率方面解锁了新的潜力。随着行政工作量上升、人员资源有限以及对数字化服务的日益增长的需求，人工智能代理提供了具体的解决方案：更快的响应时间、可扩展的服务交付和智能案例处理。

公共部门环境与企业使用不同：它们需要最大程度的数据主权、透明的决策逻辑，并集成到现有的系统和职责中。与私营公司不同，政府机构还必须确保每一项自动化决策都具有法律问责性和可解释性。它们分崩离析的IT系统需要人工智能才能顺利集成，公民数据必须在国家法律下得到保护，这使得公共部门的AI部署比企业环境要复杂得多。

此观点旨在支持公共部门技术负责人应对这些复杂性。它提供清晰性、实用指导和架构见解，帮助您领导成功的AI驱动自动化计划。



人工智能代理为何重要

超级充电过程

当你将自动化、人工智能和自主代理结合起来会发生什么？让我们来分解一下：

- 自动化是指遵循预定义规则完成任务，无需人工干预的系统。
- 人工智能通过使系统能够从数据中学习、识别模式并做出数据驱动的决策来增强自动化。
- 智能体更进一步——它们不仅执行任务，还分析上下文，调整行为，并持续优化结果。

当这三个要素协同工作时，流程不仅仅重复；它们会演变。它们会学习、适应并持续改进。这才是真正的超级充电：那些不仅仅是执行指令，还能预见需求并聪明思考的系统。

在公共部门，这对可持续性和绩效尤为重要。生成式人工智能（GenAI）——包括基础模型和本地部署——使您能够实施符合最高安全、透明和效率标准的智能自动化。这意味着不仅更快的流程，而且更好的公共服务。

什么是基础模型？

基础模型是训练在庞大且多样化的数据集上的大规模人工智能系统，旨在适用于广泛的任務。其主要的子类别包括：

- **大型语言模型** 用于理解和生成文本的（大型语言模型）用于广泛能力。
- **小型语言模型** 用于轻量级视觉语言模型（VLMs）的（SLMs），用于集成视觉和文本数据。
- 其他专业类型，如音频基础模型和多模态模型，这些模型结合了多种数据模态。

语言、数据和上下文：自动化的关键

语言不仅仅指英语、德语或中文，它也指应用程序编程接口（API）、机器语言、机器人指令或控制序列的形式存在。然而，解锁真正自动化的不仅仅是语言本身；它是语言、数据和上下文的结合。

现代人工智能能够理解、处理和在这些不同形式的语言的上下文中应用它们。它从数据中提取意义，并根据这里和现在相关的因素调整其行为。这就是如何将语言转化为现实世界行动：通过将其与数据和上下文交织在一起，使流程更智能、更具响应性。

像微软的 Azure OpenAI 服务、OpenAI 的 GPT-5、谷歌的 Gemini、亚马逊的 Bedrock 以及 Mistral AI 的开源大型语言模型

模型不仅限于自然语言。它们同样能够解释编程代码、数据库查询、API调用等。

当一个模型不仅能用人类语言交流，还能在机器和控制语言中运行时，它的功能会大幅扩展。

在那个时刻，它不再仅仅是关于写作文本或者进行对话。它关乎控制系统、触发流程、分析数据以及做出决策——所有这一切都是实时进行的。

这种多语言能力是AI代理的基础。因为它们理解各种类型的语言——不仅限于自然语言——所以它们可以与不同的系统进行交流，处理数据，并自主地协调复杂的业务流程。然而，这些代理并不能取代人类。它们增强了人类的能力，创造了我们所说的“人机化学”。



什么是AI代理？

一个AI代理是一个智能软件系统，它能够自主感知其环境、推理并采取行动以实现特定目标。它结合了决策逻辑、动态适应性和领域特定智能，以在复杂、不断变化的环境中运行。因此，AI代理能够理解任务、执行任务并持续改进其性能。这些代理不只是遵循命令——它们能够自行做出决策、彼此之间分配任务，并交换中间结果。

处理： 利用算法和模型——尤其是大型语言模型（LLM）——该代理评估和处理这些数据。这远超基本模式识别，包括逻辑推理、上下文理解和创造性问题解决。

动作： 根据其分析，代理自主执行操作。这可能涉及发送消息、触发工作流程，甚至制定新策略。

每个AI代理的核心都包含三种基本能力：

2

感知： 代理从各种来源收集并分析数据——包括API、数据库、日志文件、文本、图像或实时传感器输入。

真正的游戏规则改变者，是代理理解和应用不同“语言”的能力。API、代码、数据库查询和自然语言成为它能够主动使用的工具。这种能力通常被称为“函数调用”——使用语言或代码输入，有针对性地激活特定的函数或流程。



2 戴夫·安德烈。葡萄酒解剖学：AI代理：感知、认知和行动。 <https://www.allaboutai.com/de-de/ki-agenten/anatomie/>. 2025. (访问于05.04.2025).

一个 AI 代理的解剖学

要自主完成任务，一个AI代理会调用几个相互关联的组件协同工作。图1说明了AI代理的构成。

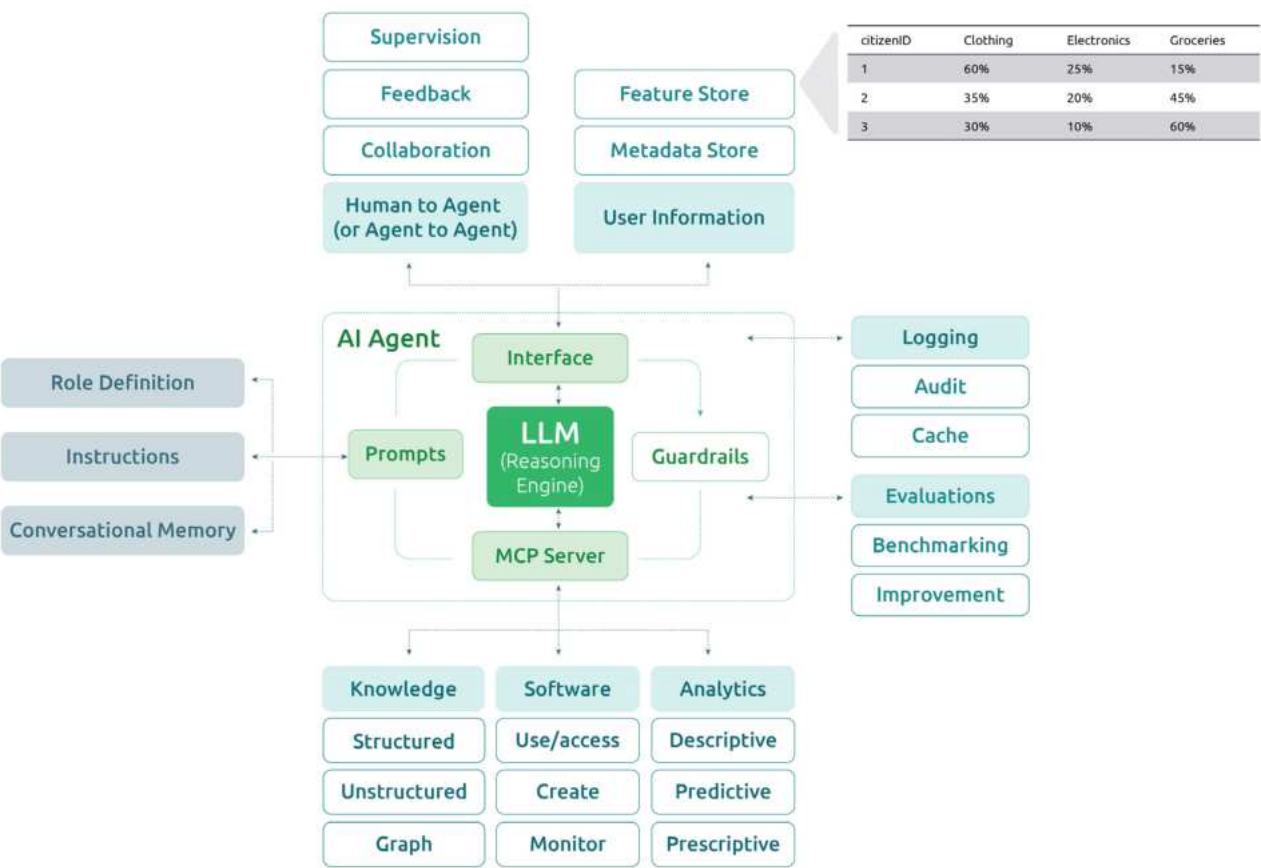


图1：人工智能代理的解剖结构
3,4

这里是如何运作的：
3

An **AI代理** 感知其环境并捕获文本、语音、图像或结构化信息等相关数据。其知识库包括存储的一般知识、特定领域的知识和随时间推移获得的专门知识。智能体动态扩展其 **知识库** 通过交互和学习。

根据感知数据和可用知识，代理使用基于规则的系统、机器学习或神经

网络。然后，它执行操作——例如调用api、查询数据或与

用户 通过利用 **工具** 通过 API 端点、用户界面或其他通信渠道。

一个关键使能者是MCP (**模型上下文协议**) ——一个可维护且可扩展的开源协议，用于将企业数据连接到人工智能系统。

4 通过提供标准化的 API，MCP 服务器充当代理和工具之间的中间人。这种标准化至关重要：它允许不同的代理访问相同的工具而不

3 aws。什么是人工智能代理？ <https://aws.amazon.com/de/what-is/ai-agents/> . 2023. (访问于06.04.2025). 4 <https://medium.com/@amosgyamfi/the-top-7-mcp-supported-ai-frameworks-a8e5030c87ab> 阿莫斯·贾姆菲. 顶级7个MCP支持的AI框架. 2025年4月。(访问于2025.04.06)。



需要定制集成。它还简化了复杂工作流的构建，并显著减轻了代理与其工具之间的连接。

代理可以使用这些标准化的 API 来触发特定功能、查询数据库、发送消息或与 Web 服务交互。更高级别的代理甚至可以动态地生成和编排额外的代理——这代表了代理智能的最高水平（参见“第 5 级：完全自主”，第 8 页）。

所有人工智能代理都能够从经验中学习并适应变化的环境，这使得它们随着时间的推移而持续改进。这种改进是由通过监督学习、无监督学习或强化学习方法获得的反馈和监督驱动的。

处理用户信息

另一个关键要素是智能体如何处理用户信息。这里有两个关键组件：元数据存储和特征存储，它们帮助智能体更好地理解上下文并生成个性化响应。

元数据存储： 存储有关用户或进程的通用信息，例如用户活动、交互历史记录或配置设置。

特征存储： 管理以表格形式存在的结构化属性。在公共部门，这可能意味着跟踪公民通常如何与政府服务互动——例如：上门 = 55%，电话 = 30%，在线门户 = 15%。基于这种行为画像，代理可以优先考虑沟通渠道，个性化提醒，甚至预先选择最有效的服务路径。

从技术上讲，每个人（通常通过公民ID或案件ID引用）都与一个动态配置文件相关联。代理会持续更新这些值，检测使用模式和偏好，并利用它们来生成定制化响应或更高效地引导流程。

另一个典型的例子来自电子商务：对于每个客户（通常用customerID表示），代理会追踪偏好——例如，服装=60%，电子产品=25%，杂货=15%。代理动态更新这些值，检测模式和偏好，并利用它们生成个性化推荐或精准营销内容。

人工智能的演化：具身人工智能的自主性等级

人工智能代理的自主性可以分为如图2所示的逐渐成熟的等级。

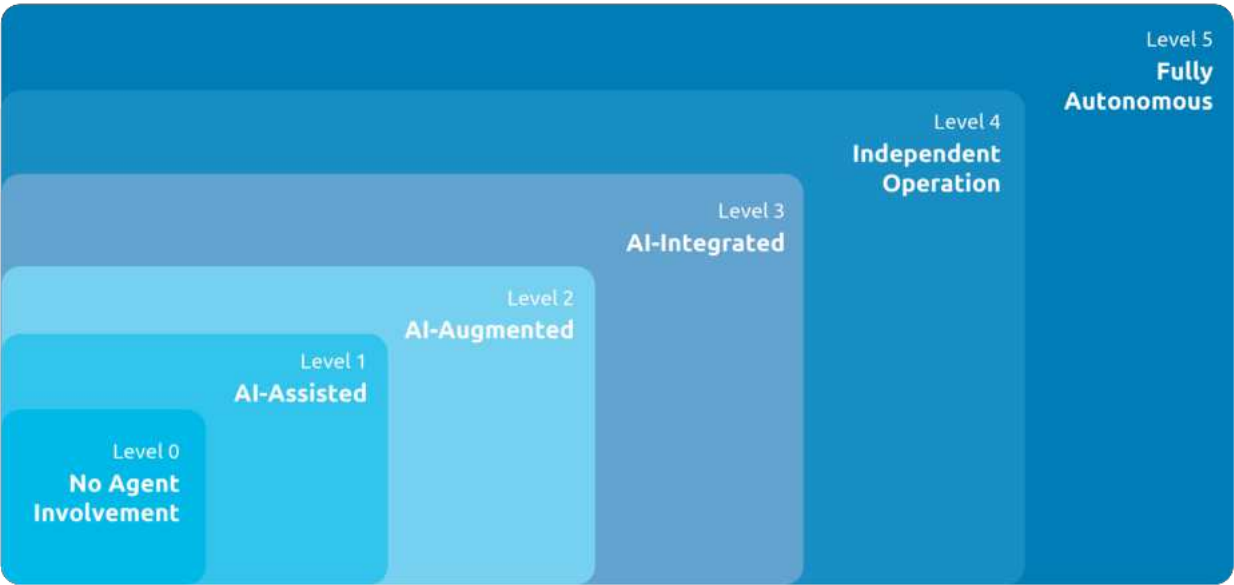


图 2：人工智能成熟度的六个级别

这些级别范围从级别 0（无人工智能参与）到级别 5（完全自主）。每个级别代表日益复杂的程度，从基本的 AI 辅助开始，逐步发展到决策支持和流程集成，最终以能够自我改进的独立、协作式 AI 代理而告终。

Level 0：无代理介入

在 0 级，完全不涉及人工智能。所有任务和决策完全由人工处理，没有自动化或人工智能辅助。

一级：AI 辅助

一级介绍了 AI 辅助功能，其中基于基本规则的工具支持预定义的工作流程。虽然自动化开始发挥作用，但人类

仍然深度参与所有决策过程。

二级：人工智能增强

迁移到二级，AI 变为决策增强型，提供推荐和见解以增强人类判断。尽管 AI 有助于优化工作流程和提高结果，但人类仍然对决策拥有完全控制权。

三级：AI 集成

在 3 级，人工智能被集成到流程中，半自主代理管理更复杂和跨职能的任务。人工监督减少，因为日常操作越来越多地由人工智能系统处理。

四级：独立操作

第4级标志着向独立人工智能操作的转变，其中多个人工智能代理实时协作以协调任务和做出决策。这通常被称为“群”，其中代理作为一个智能集体发挥作用。例如CrewAI、Microsoft AutoGen、LangGraph等框架

⁵和 OpenAI 的 Agents SDK

⁶– 替换了 OpenAI Swarm

⁷– 使集群的实现生效。人类参与程度最低，主要限于战略监督和特殊情况下的干预。

Level 5：完全自动驾驶

最后，第五级代表完全自主，人工智能系统作为自我进化的生态系统运行。这些代理不仅独立管理业务功能，而且随着时间的推移学习和调整其策略。人类输入仅用于高级治理、合规和伦理监督。



⁵ langchain. langgraph. <https://github.com/langchain-ai/langgraph>. 2024年。(访问于06.04.2025)。⁶ OpenAI. OpenAI Agents SDK. <https://github.com/openai/openai-agents-python>. 2025。(访问于11.04.2025)。⁷ OpenAI. Swarm. <https://github.com/openai/openai-agents-python>. 2024年。(访问于2025年04月06日)。

案例研究

使用上下文感知自动创建工单

一个多智能体架构在现实世界应用中能带来什么实际价值？

一个引人注目的例子来自德国联邦就业局 (Bundesagentur für Arbeit, BA)。与埃森哲 (Capgemini) 合作，他们在支持超过 40,000 名员工的社会福利流程的内部系统 ALLEGRO 中，通过人工智能代理来实现在 IT 服务工单创建方面的自动化。

与其依赖僵化的、基于规则的自动化，该解决方案使用一组人工智能代理协同工作，将变更请求和用户故事转化为结构化的 Jira 工单。这些代理提取相关信息，分解任务，生成完整的工单，并审查输出以保持一致性和避免重复——所有这些都在该机构的内部基础设施中完成，并完全符合数据保护标准。

这种方法不仅简化了运营并提升了输出质量，还展示了人工智能代理如何通过接管重复性任务来支持——而不是取代——公共部门员工，让他们专注于更复杂、更具增值作用的责任。

Capgemini. 用于管理的 KI 代理：联邦劳工局如何使用大型语言模型。 <https://www.capgemini.com/de-de/news/kundenprojekte/ki-agenten-fuer-die-verwaltung/>. 2025。(访问于28.07.2025)

多智能体架构

多智能体架构将多个专用智能体集成到一个协调系统中。
8 这些系统由承担不同任务、相互通信并处理复杂工作流程的自主代理组成。一个特别令人兴奋的方面是将语言模型与专业工具和子代理相结合，从而实现跨不同功能的智能编排。

这正是 LangChain 等框架发挥作用的地方。LangChain 通过允许创建代理链来体现多代理方法。这些是分层结构的业务流程，其中不同的代理执行特定任务，如信息检索、数据处理或决策制定。代理链的灵活配置允许实现远超简单问答交互的复杂场景。

9

根据具体应用场景。图3展示了不同的可能性：

单体药物： 一个代理处理所有任务。从技术上讲，这不是一个多代理设置，但它为更复杂的系统提供了基础构建模块。这种方法简单，但在复杂场景中通常效率低下，因为代理必须独自管理每个进程。

网络架构： 多个同级别代理并行工作并共享信息。这种设置灵活且可扩展，但可能会导致数据处理中出现不一致性。

主管架构：一个中央智能体
协调多个从属代理。该模型特别适用于将任务委托给专业代理，并高效地聚合它们的结果。

多智能体架构的设计有所不同

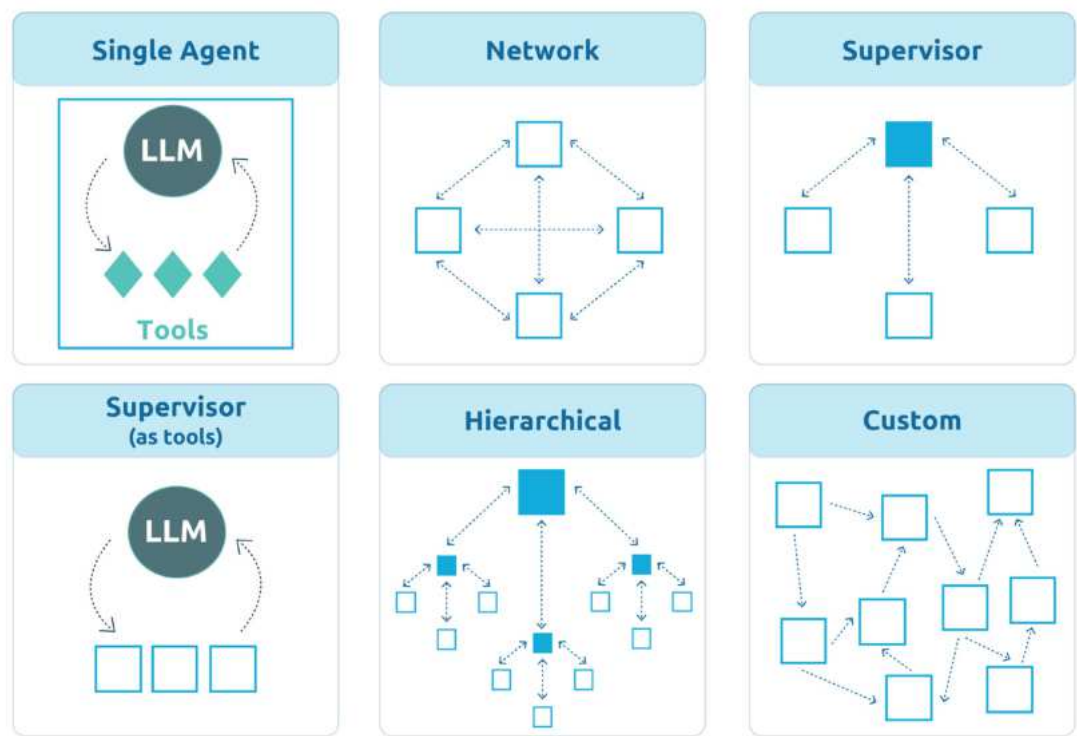


图3：多智能体架构概述

8

8 langchain。多智能体系统。 https://langchain-ai.github.io/langgraph/concepts/multi_agent/ . 2025. (访问于06.04.2025). 9 <https://docs.n8n.io/advanced-ai/examples/agent-chain-> n8n文档。展示代理和链之间的关键区别。 [比较/](https://docs.n8n.io/advanced-ai/examples/agent-chain-compare/) . 2024. (访问于06.04.2025).

主管作为工具： 在这个模型中，专用代理作为工具或模块，由主代理调用。这种方法适用于具有明确定义的功能领域的模块化系统。

层级： 多层代理以金字塔结构组织。高层代理将任务委托给低层，这种架构特别适用于具有许多子组件的复杂过程。

自定义： 定制架构，专门为特定用例的需求而设计。这

模型提供了最大的灵活性，但也需要最高的开发工作量。

在多智能体架构中，智能体间（A2A）通信协议正带来智能体自主性的新维度。这些协议使人工智能智能体能够在无人干预的情况下协调任务。一个显著的例子是谷歌的A2A协议，它促进了自主智能体之间结构化、可扩展的交互——这对于构建多智能体系统来说是一个极好的补充。

组织间代理空间中的协作

想象一个共享的智能体环境，其中由不同公共机构操作的智能体可以跨边界无缝地交互和协调任务。

通过自动化常规流程，这些代理机构使公民和公务员从手工劳动中解脱出来，为更有意义的活动释放出时间和资源。



示例 1：安排学校旅行

你是一位职业学校教师，正在为你的班级策划一个为期一周的教育旅行到哥本哈根，作为一项欧盟资助项目的部分。你给人工智能代理一个明确的目标：

为20名学生计划一次从2025年10月12日到19日的教育旅行，前往哥本哈根。包括

从柏林乘坐火车旅行，住宿在旅舍或青年中心，每天至少参加两项教育活动（例如参观一所丹麦职业技术学校、一个科技博物馆或参加创业之旅）。总费用包括入场费、餐费、门票、住宿费和火车旅行费：不超过9,000欧元。有资格获得伊拉斯谟+资金支持。

如图4所示，谷歌Agentspace中的几个专业代理在这种情况下无缝协作：

研究代理： 收集关于教育机构、公共项目和欧盟合作伙伴的信息。

交通代理： 检查合适的火车连接和团体旅行优惠，使用交通API。

住宿代理： 查找目的地附近的可用住宿，并比较价格和位置。

融资代理： 计算总成本，根据Erasmus+指南验证资金资格，并生成申请。

程序规划代理： 组装合适的日常教育活动。

所有结果均由编排代理收集，该代理协调日程、可用性和预算约束以确定最优计划。最后，预订代理处理预订、生成发票，并编制完整的旅行档案以供行政管理或资金用途。

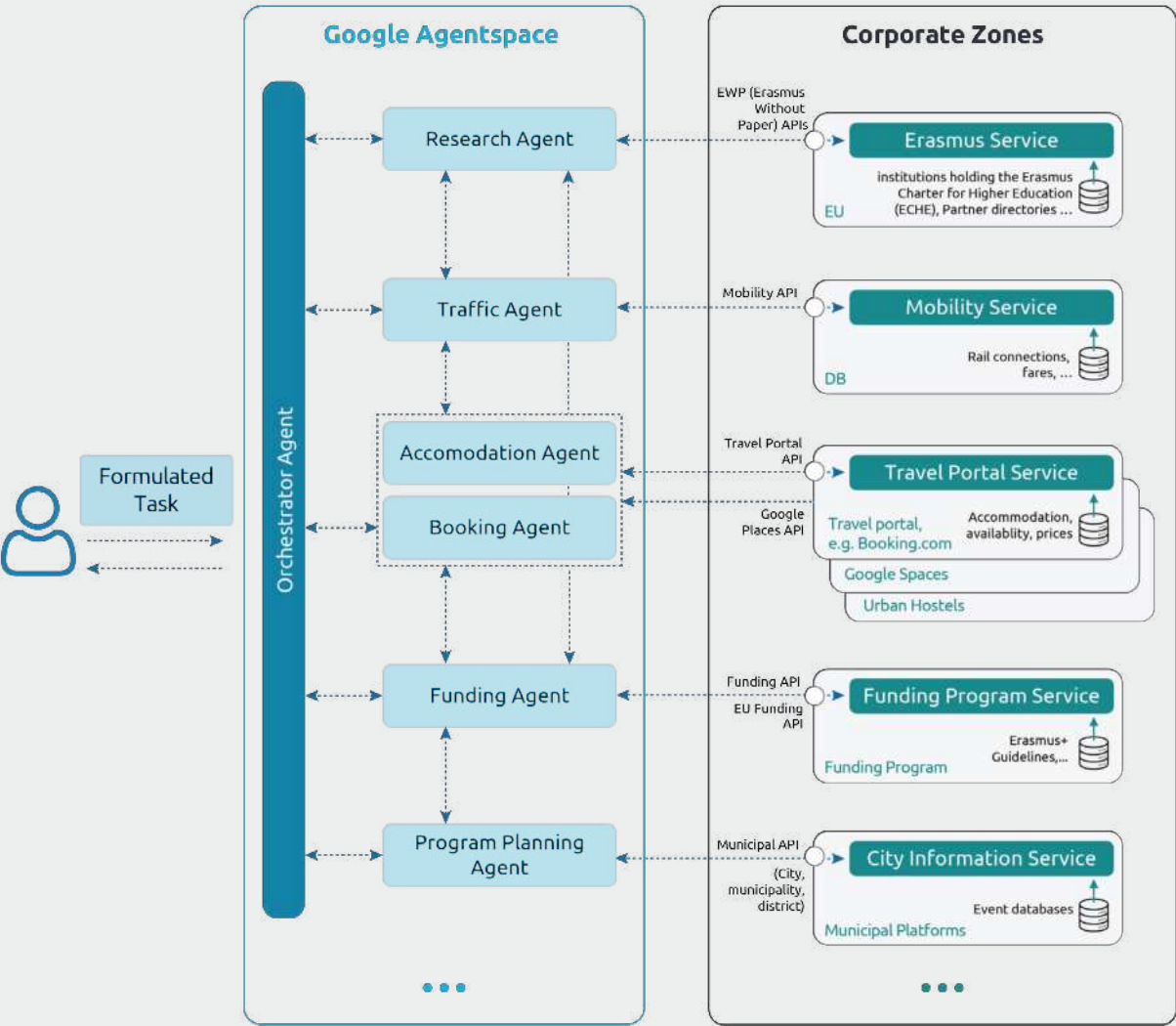


图4：谷歌Agentspace中跨组织的智能体交互——AI驱动教育旅行规划示例

示例 2：对议会质询的 AI 支持式回复

您正在联邦劳动市场政策部工作。一个议会调查组到来，包括15个关于青年失业项目、按区域分配资金以及近期举措的可衡量成果的详细问题。回应的截止日期很紧迫，所需信息分布在内部数据库、过往报告、统计门户和政策文件中。

代替手动协调多个单位，一个 **AI代理群** 被部署以高效处理该任务。

The **文档检索代理** 搜索以前的报告、立法文件和知识库，以提取相关的段落和图表。

The **数据聚合代理** 从政府仪表板中提取最新统计数据，并按地区和时间范围进行协调。

The **政策背景代理** 交叉引用资助指南和项目目标，以确保声明符合现行法律框架。

The **草稿代理** 使用行政语言制定初步答案文本，根据议会惯例调整语气和风格。

The **验证代理** 检查完整性、事实一致性以及与内部立场的一致性。

最后，**协调器代理** 汇总所有回复，构建文档结构，并准备最终的人工审核和部级批准。

这种做法可以加快周转时间，减少人工工作量，并提高各部门之间的一致性——同时保持完全透明和人工监督。

本地与云端

人工智能代理不仅限于超大规模云基础设施；它们也可以部署在主权公共云和本地基础设施上。

几个所提出的系统提供完整的本地部署选项，包括：

n8n：开源平台，可完全本地部署。为集成提供最大灵活性，并掌握数据流的完全控制权。

制造：可作为企业版提供，支持私有托管或专用实例（即仅由一个组织使用的软件的私有版本），适用于大型组织。

相关性AI：明确提供私有云和单租户部署，非常适合处理敏感流程。

弹性堆栈（Elasticsearch，Kibana）：开放-默认源，可完全部署在私有服务器或隔离网络上。

虽然人工智能代理可以部署在本地以满足特定的监管或安全要求，但这些环境通常面临固有的局限性。这些局限性包括受限的硬件可扩展性、对大规模或最先进人工智能模型的支持有限，以及维护高可用性和连接性的挑战。随着人工智能工作负载变得越来越复杂和数据密集型，这些约束可能会阻碍创新和响应能力。

云主权平台通过结合云原生的可扩展性与严格的数据主权和合规性，为公共部门组织提供了强大的替代方案。诸如

delos cloud10 可以让您在主权环境中部署人工智能代理，并对数据流、模型行为和集成拥有完全控制权。类似地，schwarz集团的云平台stackit提供基于欧洲的基础设施，在支持现代人工智能工作负载的同时，确保符合GDPR规范并保障运营主权。

这些平台弥合了超大规模服务提供商的灵活性与企业本地部署的控制之间的差距。它们使公共部门组织能够安全高效地运行高级人工智能代理——而不会在性能、合规性或信任方面妥协。

平台概述：自动化与代理智能融合

可用的自动化和代理平台种类繁多。在自动化方面，像Make、Zapier或n8n这样的传统平台专注于基于规则的工作流程，连接服务并简化重复性流程。在代理方面，像Relevance AI或LangChain这样的现代代理平台使用能够自主行动、做出决策并持续改进的AI代理。

但是随着这些平台格局的演变，这两种类型之间的界限正越来越模糊。许多提供商现在提供混合解决方案——例如n8n的“AI Agent Node”或Zapier的“AI Actions”——将这些智能代理集成到自动化流程中。这些发展开辟了新的可能性，但也要求更深层次的技术理解，特别是对于复杂或定制的用例。图5显示了这些工具和平台如何交互。

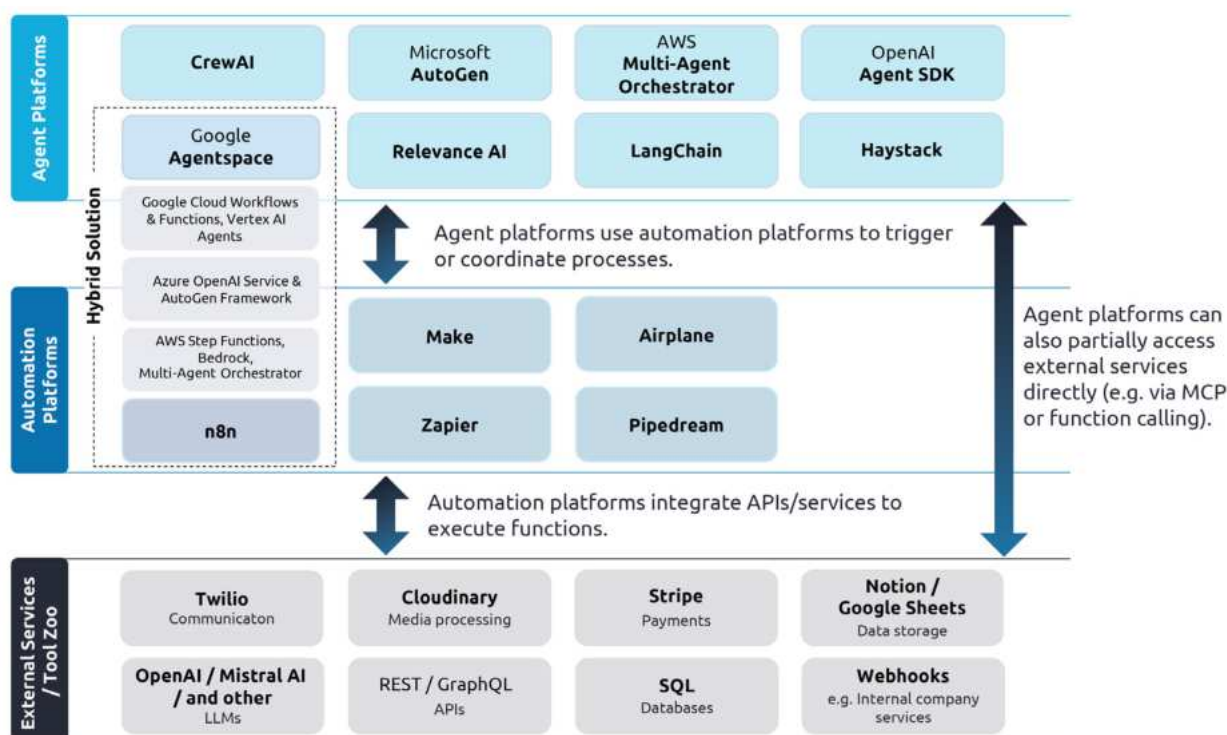


图5：平台概述及其交互方式

10 德洛斯云是一个为德国公共部门数字化转型而设计的云平台，提供数据存储、处理管理服务。

这就是AI的真实面貌

公共部门现实中的用例

处理大量来件请求的政府机构可以从人工智能解决方案中受益。例如：

- 可自动响应关于表格、截止日期或营业时间的公民服务中心。

- 为入学或学校假期等问题提供一致回答的学校管理。

- 处理居留许可和文件要求的，提供多语言回应的移民办公室。

- 回复关于申请状态或正式要求的建筑部门。

- 处理与文件相关的后续工作的社会服务机构。

本节中的用例是具有公共服务相关性的解决方案示例。它们基于当今可用的具体解决方案和供应商，但可以轻松地转移到其他自动化平台。工作流几乎保持不变，尤其是在连接外部 API 方面。



使用ChatGPT和Zapier自动化社交媒体帖子

社交媒体不再仅仅是网红的游乐场。公共部门组织越来越认识到数字化可见性的战略价值，社交媒体正作为一种参与和推广的工具而日益受到关注。

在人才日益短缺和人口结构变化的大背景下，在领英、Instagram和Facebook等平台上拥有强大的影响力，对于被视为一个现代且有吸引力的雇主至关重要。与此同时，真诚的沟通促进社会凝聚力，并为成功故事、创新和以公民为中心的服务提供舞台。积极的

外部图片并不仅仅是锦上添花，它是建立信任和吸引新人才战略必需品。

创建、发布和记录社交媒体内容可以自动化，以ChatGPT为中心进行。ChatGPT不仅是一个创意内容生成器，也是一个整个自动化链的触发器。

zapier充当了一个桥梁，连接chatgpt（在那里必须创建一个自定义gpt）和连接的工具（见图6）。

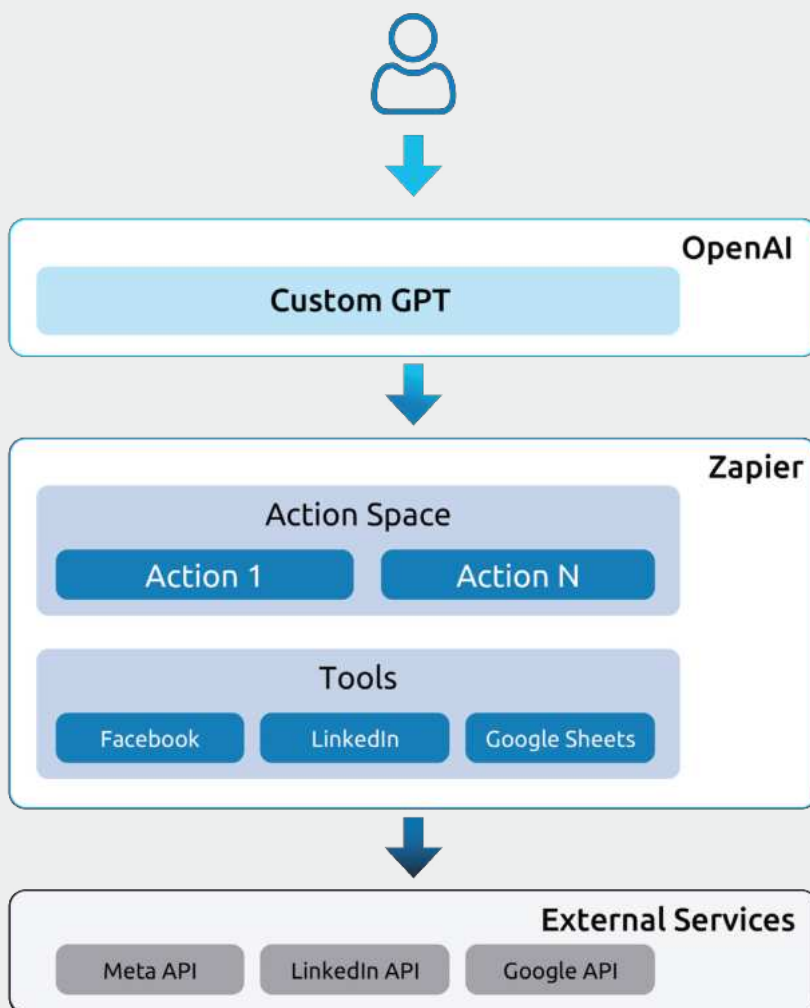


图6：通过自定义GPT触发Zapier操作

ChatGPT将用户交互中的数据和结果传递给Zapier，Zapier随后使用通过API连接的工具执行后续操作。常见的用例是社交媒体帖文的自动创建和发布：当你输入主题“**人工智能在人才培养中**”，您的自定义 GPT 将生成两篇定制帖子。Zapier 然后将

自动将其发布到您选择的平台，并将帖子网址记录在 Google Sheet 中。通过这种方法，您不仅可以节省宝贵的时间，还可以确保在您的社交媒体渠道上获得一致且高质量的结果。

处理公民邮件

政府机构正在处理大量涌入的请求。人工智能可以帮助对电子邮件进行分类和处理并相应采取行动。Zapier管理数据流并使用GPT功能，例如文本生成、分析或决策。具体方法如下：

分析请求：Zapier提取电子邮件的内容，并将主题行和消息正文等相关数据传递到您的自定义GPT。

生成回复：您的GPT会根据查询生成专业且个性化的回复。

发送或记录响应：Zapier 会自动将 GPT 生成的回复发送给客户，或将其存储在 Jira、HubSpot 或 Salesforce 等系统中。

使用“通过Zapier的AI”¹¹

在应用程序中，您可以将语言模型集成到任何工作流程中。该应用程序可以承担各种任务，例如从表格（Google Sheets、Airtable）生成报告、提供自动化的常见问题解答响应、总结内容或制作个性化消息。



¹¹ Zapier. <https://zapier.com/blog/ai-by-zapier-guide/>。(访问于06.04.2025)

通过 WhatsApp 自动读取电表读数

这个现实世界的应用案例展示了日常行政流程如何变得更高效和更便于民众。在德国的霍夫市，当地公用事业公司使用WhatsApp让居民可以数字提交他们的电表读数。这个渠道门槛低，这意味着它易于访问，无需专用应用或技术知识。它也是直接的，并且已经是用户日常的一部分——非常适合现代的公民沟通。

这种解决方案可以使用 Twilio API 结合 Zapier、Make 或 n8n 等自动化平台来构建。WhatsApp 处理用户输入，而自动化平台管理后端协调和处理——从数据捕获到存储。

这里有一个可能的流程：一位公民通过邮件收到一个二维码。扫描后，一个自动化平台（例如 Zapier、Make 或 n8n）被触发，通过 Twilio 发送一条 WhatsApp 消息给该公民，要求其提交电表的照片。

公民通过图像回复。平台触发人工智能图像识别服务，提取并验证电表读数。读数随后自动存储在数据库或企业资源计划（ERP）系统中。最后，公民通过WhatsApp收到确认，之后通过电子邮件收到账单。

优势显而易见：无需登录——只需WhatsApp。用户进入门槛低，与手动填写的网页表单相比，媒体干扰极少。整个解决方案可以使用Zapier、Make或n8n等平台，以及Twilio等API来实现。例如使用n8n的本地进行设置，不仅可以实现快速灵活的集成，还能确保完整的数据主权——建立信任。如果需要，它还可以在整个人国家范围内无缝扩展。

图7提供了发送WhatsApp消息的架构的示意图。

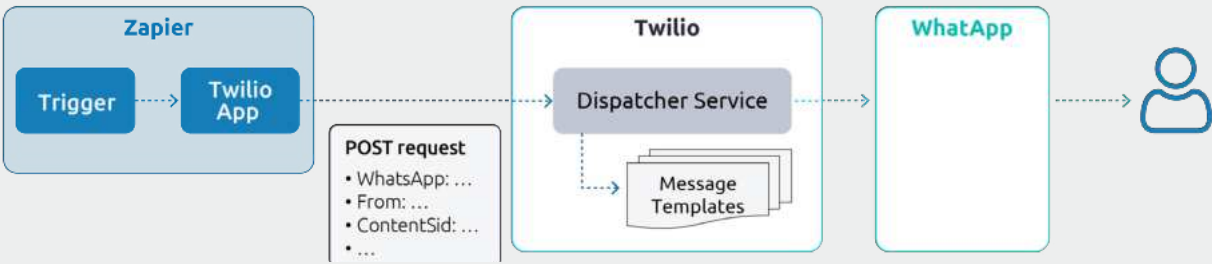


图7：通过Twilio自动发送WhatsApp消息





使用 Relevance AI 自动化服务

服务自动化可以显著提高政府服务的公民申请流程——这既有利于公民，也有利于员工。例如，它可以及早检测缺失的附件，并实现更快、更省力的响应。它还可以帮助弥补数字公共服务的差距，尤其是在流程仍然依赖邮件或基于PDF的申请的情况下。它可以通过分析非结构化文本，自动将申请转交给合适的人来做到这一点。这在涉及电厂或风力涡轮机申请等复杂申请且包含高级概念的情况下同样适用。

智能代理可以回答有关垃圾收集时间表、标识符 (ID) 更新、儿童保育注册或福利资格的问题——这些任务通常具有重复性、时效性和资源密集性。客服也可以更快地分析传入的工单，并且全天候 24x7 小时运作。标准的密码重置或虚拟专用网络 (VPN) 访问等问题能够快速且一致地解决。

最后，代理平台可以接管非结构化数据的智能处理——那些无法由固定规则处理的内容，例如自由文本、聊天记录、支持查询以及复杂表单输入。

例如，Relevance AI 提供了一个强大的代理层：能够理解、解释、分类并触发针对性操作或后续问题的代理。这些代理可以委派给子代理或跨上下文协作。

这些例子说明了 Relevance AI 如何为政府服务、教育机构和 IT 运营中的基于语言的非结构化流程添加缺失的智能层。对于复杂、法律敏感或情绪化的查询，将自动触发“升级给人类”功能。这将请求交给人类案件处理员——连同所有分析步骤、已分类内容和回复草稿——以便他们能够快速、准确和富有同情心地回应。

在人力资源（HR）部门，Relevance AI通过筛选相关档案、起草回复并将合适的候选人转发给招聘团队来预筛选申请。它还向申请人发送自动化的状态更新。

在高等教育领域，它始终如一地并根据官方指南回答学生关于课程注册、考试程序或经济援助的请求。

图8说明了系统的工作原理。

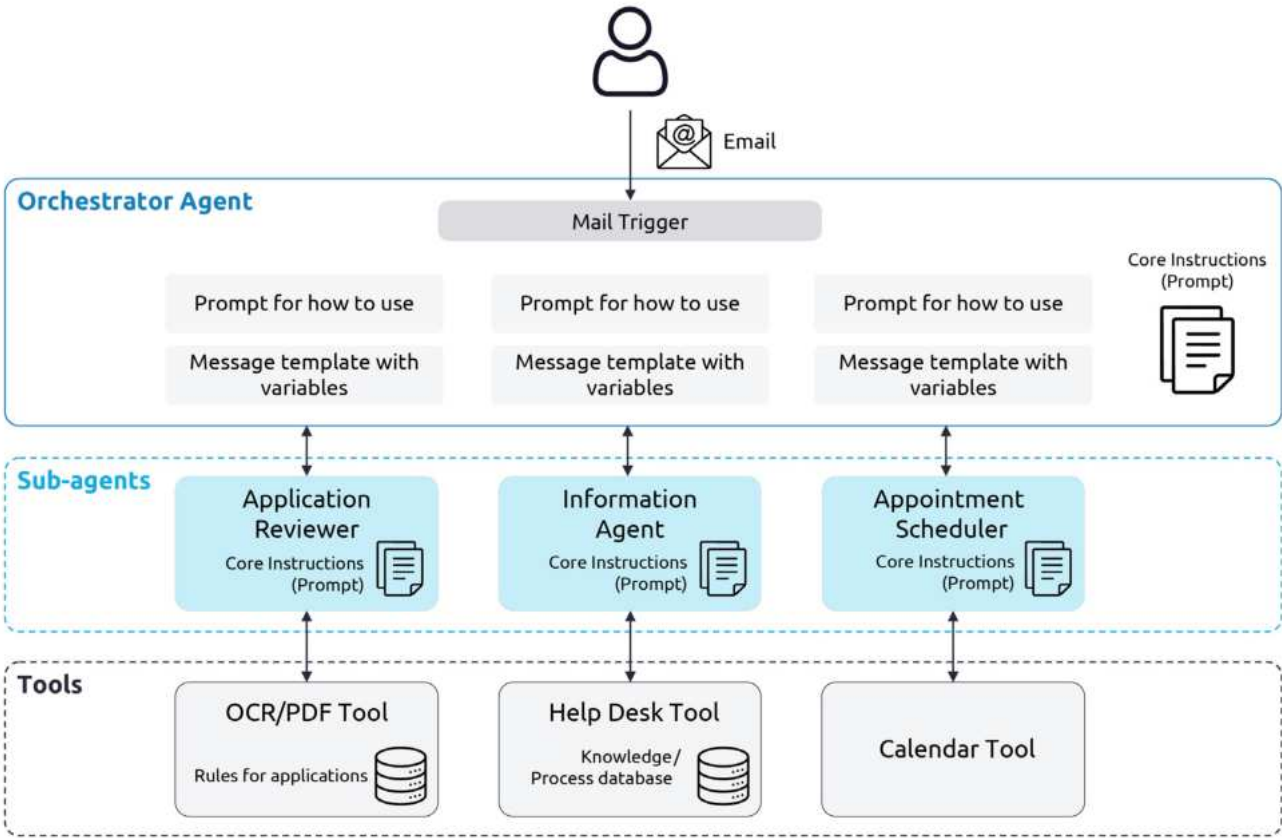


图 8：服务自动化相关性 AI 架构

在人力资源场景中，一个中央协调代理处理传入的电子邮件。主要组件是核心指令——一个中央提示，它定义了代理如何推理、沟通和做决策。协调器分析主题行、内容和附件，将请求分类（例如作为申请、信息请求或预约查询），并将其转发给合适的子代理。遵循“分而治之”的原则，具有明确角色的专业子代理接管任务的各个部分。每个子代理通过包含主题、消息正文、附件或用户上下文等变量的消息模板接收其输入，因此它确切地知道要处理哪些内容。

（包括必填字段、签名和IBAN），并在需要时制定后续问题。它从PDF附件中提取数据，使用基于规则的逻辑或大型语言模型进行评估，并生成清晰易懂的回复。

同时，信息代理处理有关营业时间、部门职责或请求当前状态的一般查询。为此，它访问内部行政流程和知识数据库。

预约调度器扫描员工日历查找可用时间段，并通过电子邮件发送预约确认。如果所需信息缺失，它会自动联系请求者以完成调度流程。

例如，申请审查员分析传入的申请，检查它们是否完整



监控和仪表盘

自动化加速流程，但缺乏监控，它很快就会变成一个黑匣子。这就是为什么监控是任何生产级人工智能或 workflow 架构的核心要素——尤其对于公共部门组织而言，透明度是其优先事项。

目前市场上最强大且开源的解决方案之一是 Elastic Stack，它由用于数据索引的 Elasticsearch、用于数据处理和传输的 Logstash 以及用于数据可视化的 Kibana 组成。这些工具被广泛认为是许多组织实时仪表板和运营监控的事实标准。

无论您是在客户服务中跟踪支持工单，还是在实时跟踪应用程序，它都在保持流程透明、及早识别瓶颈以及实现数据驱动决策方面发挥着关键作用。

以实时应用监控为例。假设你正在运行一个处理传入申请的自动化流程，例如资助申请、休假请求或服务工单。这些申请通过网页表单或电子邮件提交，并使用 Zapier、n8n 或 Make 等工具通过工作流进行处理。

图9展示了一个使用 Zapier 的架构，用以演示如何实时监控此过程。

自动监控用例（例如持续数据可视化）高度多样化。



图 9：使用 Elastic Stack 的自动仪表板

这种方法总是能实现完全透明：收到了多少申请？哪些类别最常见？流程卡在哪里？

严格的数据保护要求。同时，该系统非常灵活：您可以集成几乎任何数据源，并可视化对您的运营至关重要的关键指标——无论您身处公共管理、IT 支持或工业生产。

Elastic Stack 的主要优势在于它是开源的，可以免费使用，并且可以托管在自己的服务器上——这使得它非常适合拥有

批判性反思与局限性

人工智能代理和自动化平台提供了巨大的效率提升，但也带来了必须被有意识地应对的挑战。

复杂性和实现工作量

构建复杂的代理架构需要在规划、配置、测试和监控方面投入大量精力。虽然像n8n、Relevance AI或Make这样的系统在技术上具有灵活性，但它们需要对流程、数据流和安全要求有深入的了解——尤其是在公共部门。

成本和资源

尽管许多工具提供开源或免费套餐模式，但运行生产环境通常会对服务器基础设施、扩展、维护和高级功能许可产生大量成本。本地部署确保数据主权，但也增加了运营和人员需求——给本就面临劳动力短缺的公共部门组织增加了额外压力。

风险和误差来源

自动化系统的可靠性仅取决于它们的输入和配置。配置不当的代理可能会产生错误的响应、错误处理敏感数据，或者在缺乏适当监控的情况下无意中升级流程。如果没有明确定义的错误处理和人工升级途径，残留风险仍然存在。

伦理和法律方面的考虑

在公共沟通或行政管理中部署人工智能代理触及伦理维度：对公民的透明度、非歧视性决策以及敏感个人数据的保护。必须确保合规性、公平性和问责制处于最高水平。

应用“负责任的AI”（换句话说，整个生命周期中开发和部署合法、符合伦理、技术稳健的AI系统）使公共部门组织能够满足这些要求。在公共部门，这意味着不仅要通过设计安全的系统来保护数据，还意味着要维持公众对政府机构如何使用自动化方式的信任。

根据具体的应用场景，**欧盟人工智能法案**也可适用——尤其是在决定影响个人权利或需要人工监督的情况下。在德国，**行政程序法 (Verwaltungsverfahrensgesetz)** 明确禁止自动化法律授予的人为判断权。其他国家采取不同的立场：**阿拉伯联合酋长国** 例如，刚刚引入了相关法律条款，允许在某些条件下做出完全自主的行政决策。

尽管存在这些挑战，人工智能代理和自动化平台的价值潜力依然巨大。它们为更有意义、更具价值的工作创造了空间，提升了服务质量，并提供了使行政和业务流程面向未来的独特机会——只要它们被深思熟虑和负责任地实施。

一瞥关键风险

风险区域端口	
复杂度	高设置和维护工作量以可靠运行
成本和资源	为托管、扩展和许可证支付的重大运营成本
错误来源	故障配置或监控缺失可能导致功能故障
伦理考量 透明度、偏见和数据保护相关的风险	
合规性 严格符合GDPR、数据主权和问责制的要求	

从自主视觉到行动

六步公共部门领导者现在应采取的行动



智能体式AI标志着自动化在设计、部署和治理方面的根本性转变。对于技术负责人和架构师来说，挑战在于将这种潜力转化为安全、可观察且深度融合的系统。关键

以下步骤概述了从概念到实现的转变过程，为将代理式AI集成到现实世界、公共部门工作流程中提供了一条实用的路线图。

1. 建立强大的数据基础

为了让人工智能代理能够自主且具有上下文感知地做出决策，你需要一个强大且管理良好的数据基础设施。这一基础步骤至关重要：人工智能代理只有在所依赖的数据是高质量、可访问且值得信赖时，才能表现良好。¹² 在建立这一基础的过程中，以下是一些重要的步骤：

公民ID、案件ID和文档类型）以便人工智能代理以相同的方式解释数据。

- 创建一个统一语义数据模型
确保系统使用相同的术语（例如

- 通过api提供干净、可靠的数据：使用api网关或数据层，为代理提供最新、经过验证的信息——最大限度地降低产生幻觉或逻辑过时的风险。

¹² 凯捷公司。政府数据基础：从人工智能愿景到执行。
<https://www.capgemini.com/insights/research-library/data-mastery-in-government/> . 2025 (访问于03.07.2025).

- 追踪数据源和变更：使用元数据工具查看数据来自哪里、如何变化以及代理如何使用它。这对于故障排除和审计至关重要。

- 建立验证数据的过程：设置系统以捕获诸如缺失字段、意外格式或异常模式等问题——尤其是在使用基于事件的系统（如 Kafka 或 webhook）时。

- 使用合成数据或测试数据安全地训练代理：为测试代理创建安全、隔离的环境，以保护实时系统和个人数据

当你微调行为时。

- 为了确保您的AI代理在安全合规的框架内运行：

- 使用模型代理或网关，如PromptLayer或Azure API Management，来控制访问。

- 执行请求验证、个人信息的屏蔽以及限制大语言模型的使用。

- 选择满足合规要求的托管模型环境需要（例如主权云）或零信任本地部署）

2. 评估系统层面的自动化准备情况

- 每个AI代理的功能、风险和备份计划都要有文档记录。

- 首先确定自主自动化可以嵌入到您现有技术栈中的位置。重点考虑那些已经部分数字化并且可以通过 API、webhook 端点或 Kafka 或 RabbitMQ 等消息队列系统进行连接的流程。常见的例子包括：

- 通过服务门户触发的工作流 • 具有可靠 CRUD API 或 webhook 功能的系统

- 应用事件驱动架构原则，精确定位代理可以监听、行动和自主传递结果的位置。从一开始就要明确系统负责什么以及如何避免可能导致错误的重复操作。

- 带有结构化附件的 входящие почты (PDF 文件, 表单)

3. 选择合适的代理运行时架构，然后针对上下文进行设计

- 选择一个适合您运营约束的执行模型。在选择时，要考虑诸如速度、需要扩展的程度、您的数据存储位置以及监控的便捷性等因素。

那些能够自行做决定、逐步推理并选择下一步做什么的东西。

- 人工智能代理需要短期和长期上下文。保存它们的思维过程有助于使结果更一致，更清晰，也更容易审查。

- n8n 非常适合本地部署或离线环境。它具有可视化、低代码的特点，并通过“AI Agent 节点”或 HTTP 集成支持 LLMs。

- 短时记忆

使用令牌缓冲区、滑动窗口或摘要缓冲区等工具来保留最近的对话历史记录。

- Relevance AI和LangChain是模块化、以Python为核心的框架，适用于构建能够记忆事物、使用工具并协同工作的基于LLM的多智能体系统。

- 长时记忆

使用类似 Redis 或 Pinecone 的数据库来存储重要事实、用户偏好或随时间推移的行为。这些对分析和个性化有所帮助。

- openai代理sdk、autogen和crewai适用于更高级别的自动化，例如代理

4. 系统性地编写工程师提示和界面

- 与其将提示视为一次性技巧，不如像真正的软件组件一样构建它们：

 - 使用带变量的模板（例如用户元数据或先前的操作），以便提示能够适应不同的情况。
 - 设置代理可以使用工具，使用 OpenAI 函数调用、LangChain 工具或 ReAct 模式。
- 跟踪提示版本，就像你跟踪代码一样使用 GitOps 或 Config-as-Code 管道。
 - 添加规则和设置（例如模式检查）温度限制）以使AI的行为更可预测的。

小贴士：为分类、摘要或资格检查等常见任务构建共享提示库和内部 API。

5. 策略性地识别和优先使用用例

并非所有用例都适合代理自动化。使用基于四个关键维度的决策矩阵来确定实施优先级：

标准描述	最适合智能体AI
常规强度 任务发生的频率如何（每日/每周 vs. 很少？）	高频任务（例如：邮件回复）
关键性 什么是法律、财务或声誉风险如果出什么问题？	低至中等（例如：常见问题解答、提醒）
创造性任务是否需要主观判断共情，还是解读政策？	低创造力（例如，表格检查）
结构化能力 规则能否描述该过程数据，或模式？	高度结构化（例如：校验）
跨这四个维度映射潜在用例，并首先实施“高惯例/低创造力/高结构性/低关键性”象限中的用例。例如：	
• 对邮件进行分类并发送模板回复。• 检查某人是否符合基本的资格要求。	• 阅读文件和填写表格。• 安排预约并发送提醒。
你也可以通过将它们与合适的技术模式和工作工具相匹配来选择用例。避免从一开始就着手高度创意或政策关键的任务。相反，应从低风险的用例入手，在那里你可以安全地测试、衡量成功并快速迭代。	

模式类型	典型用例	工具堆栈示例
检索增强型生成 (RAG)	处理关于文件的查询	LangChain + Pinecone + LLM
函数调用代理	运行基于API的工作流	OpenAI/Gemini + Zapier/n8n + REST API
代理群	管理部门间协作	AutoGen + LangGraph + Redis 内存
本地 NLP	处理以合规性为中心的电子邮件和文件	spacy + haystack + n8n + postgres

6. 时刻监控、测试并改进你的系统

自主系统是动态的，但你需要能够看到它们正在做什么。在仪表板上显示关键统计数据——包括技术统计数据，如速度和错误，以及运营统计数据，如用例数量和成功完成数量。

- 设置请求跟踪和日志记录（使用 Elastic Stack 和 OpenTelemetry 等工具）。
- 记录每个提示的详细信息，例如使用了多少个令牌、模型版本以及响应时间。
- 当人工智能未能达到置信度阈值或需要人工介入时应制定备用计划。
- 使用红队测试方法定期测试系统的鲁棒性、偏见和非典型情况。

• 运行受控实验并通过跟踪系统运行情况以及它如何帮助用户来衡量影响：

- 每个案例或任务节省的时间。
- 决策的准确性，例如分类或路由。
- 模型漂移和幻觉率。
- 用户体验（内部和外部）。
- 系统需要多久才能交还回人类。

创建“代理记分卡”以持续检查绩效，随时间改进行为，并确保结果清晰可追溯。

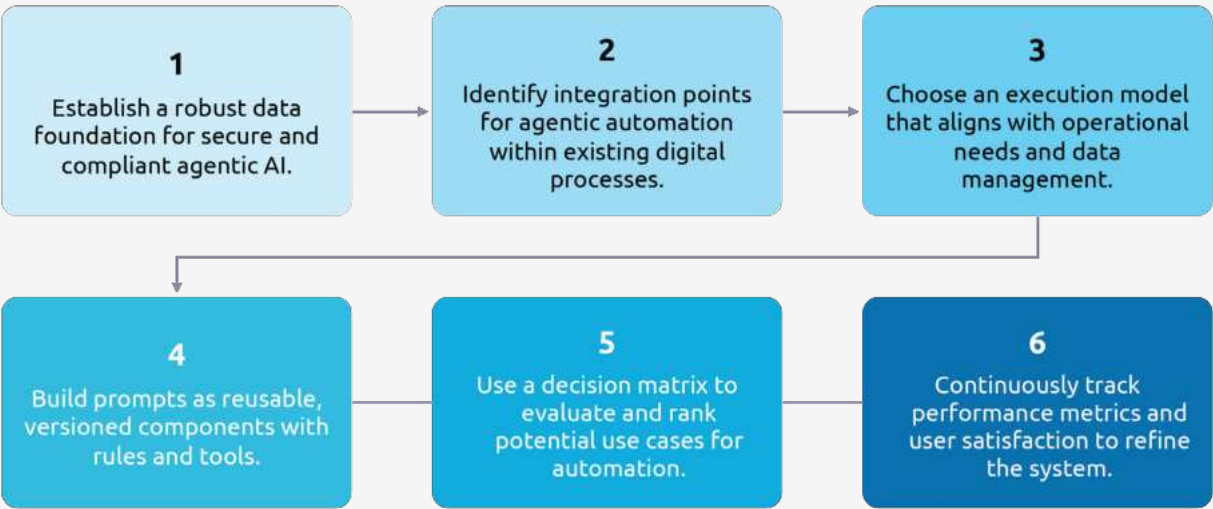


图 10：政府部门领导实施自主 AI 的路线图

代理式AI不仅仅是一个战略概念；它标志着一个新的软件范式。架构师和工程师对其成功至关重要，他们负责构建不仅智能而且安全、可观察的系统。

并且合规。但公共部门真正的冲击并非仅仅来自使用人工智能。它来自工程深度嵌入现实公共部门工作流程的人工智能系统。

摘要和展望：

我们从人工智能代理的崛起中学到了什么

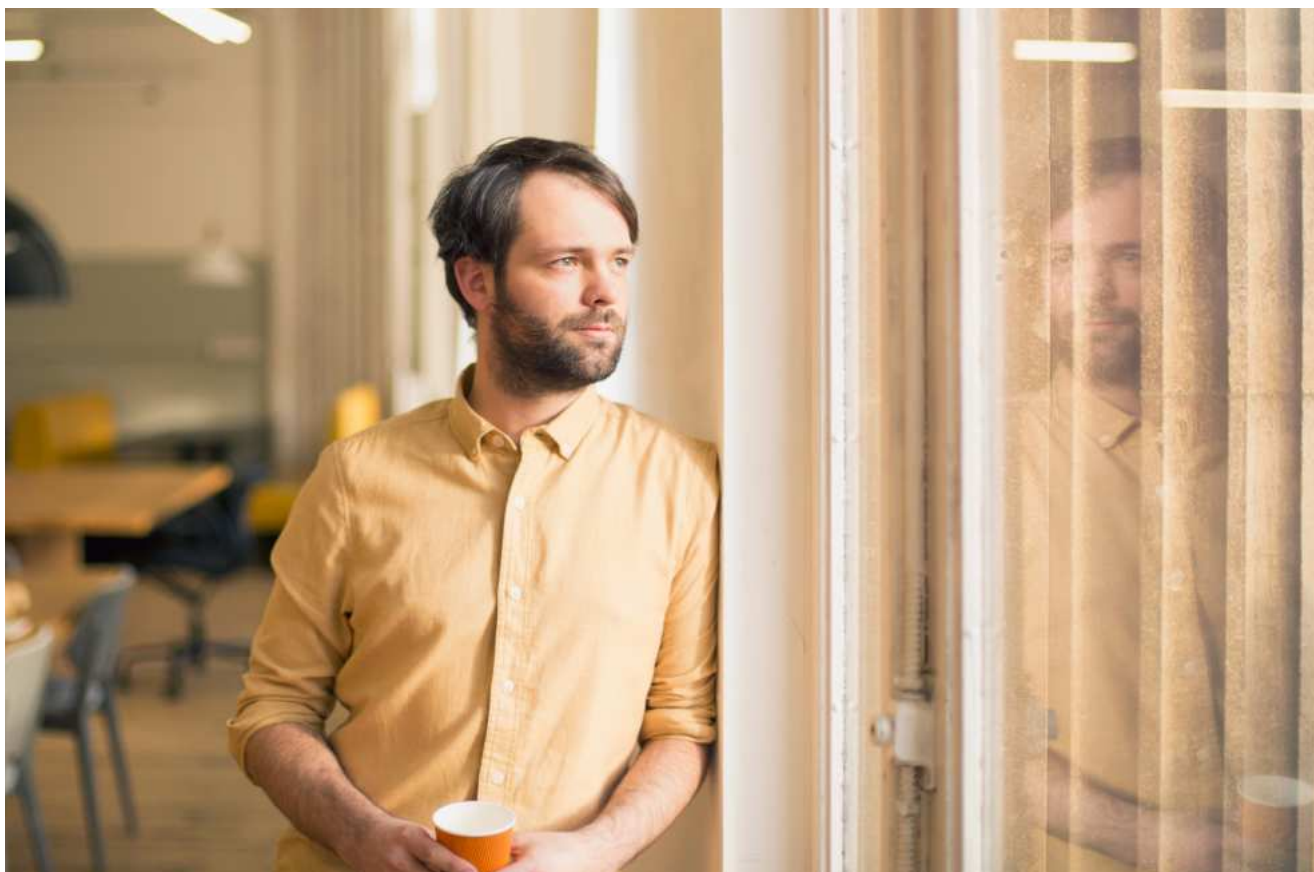
AI智能体不再是一种未来愿景——它们已经重塑了我们自动化工作、应对复杂性以及跨领域提供服务的方式。从基础协作助手到动态多智能体系统，这一观点展示了智能架构如何释放真实潜力：提升可扩展性、更智能的工作流程，以及超越传统自动化的定制化交互。

但实现AI代理并非即插即用过程。它需要周密的设计、法律意识、技术专长和强烈的责任感。这就是我们没有仅仅展示可能性，而且还要展示需要注意什么——从数据保护到可解释性。

关键点？

尤其是在公共部门，影响是具体的。无论是回应公民请求、协调跨部门沟通，还是处理政策文件，代理人都帮助减轻工作量，提高一致性，并释放人力以执行复杂、增加价值的任务。

你不需要一夜之间就建立起一个完全自主的系统。从小处着手，保持战略眼光，逐步构建你的智能体生态系统——拥有合适的工具、用例和合作伙伴。技术已经成熟。时机已经成熟。关键在于我们要明智地运用它。



如何思爱普可以帮助您

设计人机交互代理系统

我们通过将人类验证嵌入到需要酌情处理或问责制的决策过程中，确保人工智能代理增强而不是取代您的工作队伍。

实现透明且可审计的逻辑

我们使用可解释模型和可追溯的工作流程来构建我们的架构，以便公共机构能够满足透明度、文档记录和审查的法律要求。

坚持全面数据主权

我们在主权云（例如 Delos 云、StackIT）或本地基础设施上部署 AI 代理平台，以确保系统符合 GDPR 和国家数据保护法律。

与遗留系统集成以及与公共IT环境集成

我们专注于将代理工作流程连接到现有的管理系统——包括专业程序、登记册和文档管理系统——而不会中断当前操作。

分析您当前的 IT 与数据格局

我们评估您的基础设施，识别集成机会，推荐最合适的代理平台——开源、云原生或主权——并全面实施。

开发领域特定代理

我们为政府应用场景（如公民沟通、资格检查或文档分类）训练和配置AI代理，所有内容均根据您的语言、语气和流程逻辑进行定制。

通过负责任的AI治理建立信任

我们帮助建立与欧盟人工智能法案相符的治理框架。这些涵盖风险分类、监督结构、红队测试以及人工智能行为的持续监控。

训练您的团队进行混合协作

我们通过有针对性的技能提升计划、研讨会和安全实验的沙盒环境，帮助公务员有效利用人工智能。



从 Capgemini 阅读更多

共振人工智能框架（普华永道）

智能体的崛起：信任是人类-人工智能协作的关键（[毕马威研究 institute](#)）

想大处，从小处着手：释放政府中生成式人工智能和智能体式人工智能的变革力量（[毕马威](#)）

政府数据基础：从人工智能愿景到行动（[毕马威研究 institute](#)）

连接点：公共部门的数据共享（[毕马威研究 institute](#)）

作者

您想和我们开始对话吗？那么请随时联系我们：



埃尔达尔·苏丹诺夫

商业企业架构师总监 沃尔沃 德国 eldar.sultanow@capgemini.com



拉斯·山德森

首席技术官 公共部门 宝洁德国 lars.sante@capgemini.com



塞德亚·伊科兹

毕马威德国业务分析师 ceyda.icoz@capgemini.com

关于埃森哲

毕马威是一家提供人工智能支持的国际商业与技术转型合作伙伴，为客户创造切实的商业价值。我们畅想企业的未来，并借助人工智能、技术和人才将其变为现实。凭借近60年的深厚传承，我们是一家在50多个国家拥有42万名员工的有责任感和多元化的集团。我们凭借深厚的行业专业知识及强大的合作伙伴生态，提供端到端的服务和解决方案，发挥我们在战略、技术、设计、工程和商业运营方面的能力。本集团2024年的全球收入为221亿欧元。

让梦想成真 | www.capgemini.com

