SPHERITY RESEARCH | EXECUTIVE RESEARCH BRIEF

Europe’s Fundamental AI Opportunity

Trust as a production factor, industrial renewal and the economics of transformation speed

Companion to the full academic paper

Bo Harald
Why-Advisory Oy

Carsten Stöcker
Spherity GmbH

Prepared: September 2026
Evidence cut-off: 30 August 2026

Executive proposition

Europe's strongest near-term AI opportunity is to build the world's most capable interoperable execution environment for AI acting across organisations, industries, public authorities and physical systems. Foundation models diffuse globally, while offensive AI capabilities, deepfakes, synthetic data manipulation and fabricated credentials proliferate at near-zero marginal cost. In a world where unverified digital signals can no longer be trusted, the ability to let companies, AI agents and machines act across organisational and cyber-physical boundaries with verifiable authority and evidence becomes hyper-scarce.

In this “zero-trust by default threat landscape,” trust becomes a primary production factor: it dictates which combinations of data, capital, technology and human skills can be safely deployed, and which consequential real-world actions can be authorised. Economic value remains embedded in local production systems, critical data, professional rules, physical machinery, supply chains, worker knowledge and public processes. Europe can turn these assets into trusted execution capital: reusable authority, cryptographic evidence, shared semantics, assurance and runtime controls that allow consequential B2B/B2G, digital and physical actions to be executed with absolute integrity. The economic result depends on policy direction, implementation speed, complementary investment, corporate resource reassignment and the diffusion of capability across firms, regions and public institutions.

Seven messages

1. AI productivity is an implementation outcome. Models create value when organisations redesign processes, improve data, build skills, manage risk and move resources from legacy activity into higher-value uses.

2. Trust is becoming an indispensable production factor in an adversarial AI world. As zero-cost offensive AI and data manipulation erode confidence across digital and physical supply chains, trust becomes a hard operational requirement.

3. Verifiable identity, legal authority, tamper-proof evidence, shared semantics and runtime controls reduce transaction costs, defend against synthetic fraud, and dramatically expand the scope of cross-company and cyber-physical action that can be safely automated from B2B/B2G transactions to autonomous physical AI systems.

4. Europe has a leading starting position in trusted industrial, agentic and physical execution across organisational boundaries. This plays to its strengths in engineering, regulated markets, public institutions, official registers and cross-border standards and provides a natural defense against systemic disinformation and automated manipulation.

5. AI Governance, Trustworthy AI and Trusted AI perform complementary functions. Governance sets legitimate purposes and accountability. Trustworthy AI defines required system qualities. Trusted AI makes selected claims and controls cryptographically verifiable at the point of action.

6. Opportunity and transition risk arrive together. Employment, community stability, security, market concentration, distribution and public trust require systemic and holistic leadership across government, industry and society.

7. The authors' model illustrates a 2040 real-GDP uplift below one per cent in fragmented drift, around four per cent in coordinated acceleration and around ten per cent in trusted industrial leadership. These are conditional scenarios, not forecasts.

Trust becomes a production factor, a shield against systemic disinformation, and a source of speed when it is designed as reusable infrastructure. Speed becomes a source of productivity when it expands authorised action and produces durable capability in a zero-trust world.

Contents

1 Europe's strategic productivity window

Europe enters the agentic AI era with a valuable but time-sensitive combination: a large Single Market, globally significant manufacturing and engineering capabilities, strong public institutions, leading research clusters and an established framework for digital identity, cybersecurity, data protection and AI governance. The same economy faces weak productivity growth, large investment needs, demographic pressure and higher expenditure on ageing, defence, energy systems, climate adaptation and infrastructure. The Draghi report estimated additional annual investment needs of roughly EUR 750 to 800 billion by 2030. Eurostat reported an EU old-age dependency ratio of 34.5 per cent at the beginning of 2025 [1, 2].

This makes productivity a social-system variable. A smaller labour pool raises the value of automation. Greater automation raises dependence on digital and cyber-physical systems. That dependence increases the value of security, functional safety, resilience and verifiable authority. Durable output gains can expand the income and contribution base from which pensions, healthcare, care services, security and public infrastructure are financed. Political institutions still determine how incremental capacity is allocated.

The macroeconomic evidence supports ambition with discipline. Acemoglu [3] estimates a cumulative total-factor-productivity effect below 0.66 per cent over ten years under conservative task assumptions. OECD central scenarios place the annual labour-productivity contribution across major advanced economies at approximately 0.5 to 1.0 percentage point over the next decade, conditional on adoption and capability [4]. Firm-level evidence also associates AI adoption with higher productivity when software, data, training and capital deepen together [5]. The range is wide because access to a model is only the beginning of transformation.

Figure 1 summarises the causal channels and the public-capacity feedback loop.

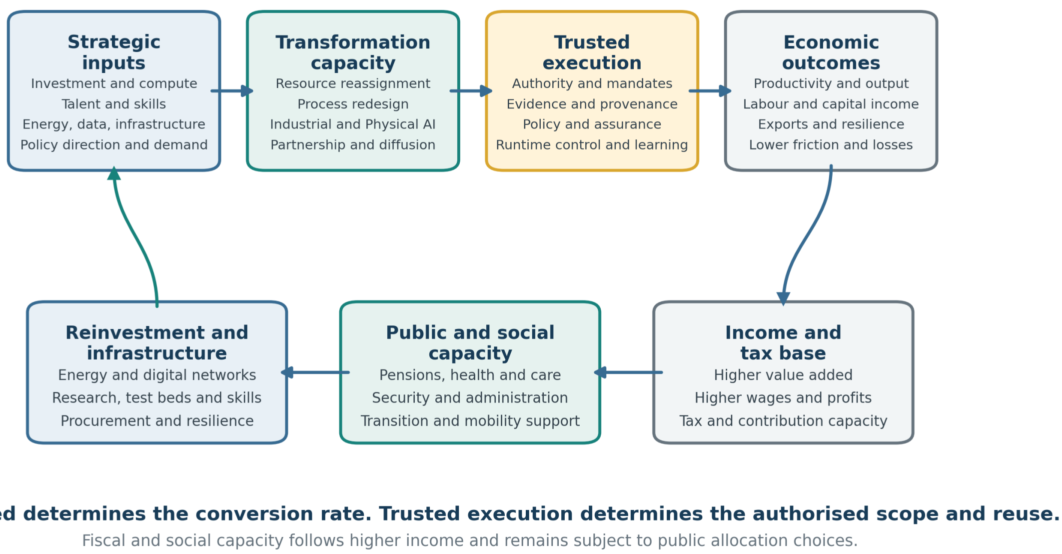

Figure 1: Macroeconomic levers, transformation mechanisms and public-capacity feedback. Policy direction and implementation speed determine how quickly strategic inputs become operational capability. Trusted execution determines the authorised scope and reuse of AI-enabled action.

Note: The feedback loop matters because higher income can support skills, infrastructure, research, security and social capacity, which in turn support the next cycle of transformation.

2 Trust as a production factor

Classical economics organised production around land, labour and capital. Modern growth theory and institutional economics broadened the picture to include technology, knowledge, human capital, institutions and other intangible assets. Transaction-cost economics showed that firms and markets also depend on the costs of finding partners, negotiating agreements, verifying performance and enforcing obligations [6, 7].

We use the term *production factor* in this broader managerial sense: an input that materially affects how productively people, capital, data and technology can be combined. Trust does not replace the established factors and is not proposed as a separate national-accounts category. It is an enabling complement. Without sufficient trust, otherwise valuable AI systems, data, machines and skills cannot be used fully.

2.1 Why trust now enters production directly

In conventional operations, managers, employees, contracts and established business relationships provide much of the context required for action. AI agents and connected machines change both the scale and speed of operations. They may discover suppliers, access data, commit resources, change production settings or initiate physical actions without a human checking every step. Cross-company autonomy therefore depends on verifiable trust at the moment of execution.

Digital trust authenticates companies, people, agents, workloads, machines and data. It protects integrity and applies Zero Trust Architecture: no actor or action is trusted solely because it operates inside a network. Legal trust connects an action to a legal person, a valid mandate, a defined scope and duration, revocation mechanisms and accountability. Semantic and evidentiary trust establish that participants refer to the same entity, product, contract and evidence relationship.

Verifiable evidence graphs connect claims to their sources, provenance, current status, dependencies and meaning. Runtime policies then determine whether a specific action is authorised at that moment and whether its execution can be monitored, restricted, interrupted and recovered.

2.2 Defensive controls as an economic requirement

AI also lowers the cost and increases the speed of producing plausible false evidence, deepfakes, social-engineering attacks and automated cyberattacks. As agents and machines become connected to payments, supply chains, production systems and physical assets, manipulated information can produce direct operational and financial consequences.

Defensive trust infrastructure therefore becomes part of productive capacity. Cryptographic identity, provenance, Zero Trust access control, least-privilege policies, status and revocation services, runtime monitoring and tested recovery can reduce the probability, scope and duration of incidents. These controls cannot eliminate risk. They can, however, reduce fraud losses, data compromise, unsafe actions, downtime and recovery costs.

Their economic role extends beyond avoided damage. By lowering expected losses and containing failures, defensive controls allow boards, insurers, regulators and business partners to authorise forms of automation that would otherwise remain outside their risk appetite. They also help preserve confidence in digital transactions and automated systems. Defensive capacity is therefore not separate from productivity: it is one of the conditions under which greater autonomy can be deployed at scale.

2.3 How trust creates economic value

Trust enters production through four linked mechanisms.

- First, it reduces transaction and coordination costs by replacing repeated bilateral checks with reusable identity, mandates and evidence.
- Second, it expands authorised process depth: more steps can move from human-assisted preparation to accountable execution across organisational boundaries.
- Third, it raises risk-adjusted productivity by reducing fraud, error, unsafe action, expected loss and incident duration.
- Fourth, it creates infrastructure and network effects: once credentials, policies and evidence formats are widely accepted, additional transactions can reuse the same foundations.

For managers, the practical test is simple. Holding models, data, people and machinery constant, how many additional valuable actions can the organisation authorise, automate and reuse across counterparties when identity, authority, evidence and recovery are verifiable?

If the answer changes materially, trust is functioning as a production factor. Its contribution remains complementary: compute without reliable data, AI without authority, and automation without compliance evidence, safety and accountability cannot deliver their full economic value.

2.4 Why Europe has a leading starting position

Europe does not lead every layer of AI. It does, however, have a leading starting position for turning trust into an operational production factor. The Single Market combines a large cross-border transaction base with official registers, regulated industries, product-safety and cybersecurity rules, engineering standards and public authorities that can issue and verify authoritative evidence.

The European Digital Identity Framework (EUDIW) establishes a common legal and technical foundation for digital identity. The proposed European Business Wallet (EBW) extends this approach to companies and public bodies. It covers secure identification, attestations, document exchange and the management of representation rights and mandates [8, 9].

This foundation can support Zero Trust access control, secure supply chains, authenticated machines and assets, bounded mandates for AI agents and verifiable evidence graphs. European Business Wallets are an important component, but not the entire trust infrastructure. Issuers, authoritative sources, business registers, verifiable LEIs, trust registries, status and revocation services, shared semantics, policy engines and relying-party verification must work together [10].

Europe's advantage depends on cross-border implementation, mutual recognition and trust between jurisdictions, broad verifier coverage, open conformance mechanisms, usable standards and adoption in real production processes.

If these elements are connected, Europe can translate legal certainty and industrial quality disciplines into lower transaction costs, wider authorised automation and reusable capabilities for governed industrial and agentic systems. When accumulated and reused across organisations, sectors and jurisdictions, trust as a production factor becomes trusted execution capital.

3 Building Trusted execution capital

If trust is a production factor at the point of use, trusted execution capital is the accumulated stock that supplies it. The paper defines trusted execution capital as the stock of reusable technical, legal and organisational capabilities that allow digital and physical actions to be attributed, constrained, evidenced, monitored and corrected. Like other intangible capital, it requires upfront investment and creates value through reuse. Reusable organisational identity can shorten onboarding. Reusable mandates can reduce the cost of delegated action. Verifiable evidence can reduce repeated due diligence. Shared semantics can support automated interpretation. Machine-readable policy can enable straight-through processing. Runtime monitoring, interruption and revocation can reduce expected loss and incident duration.

3.1 Three complementary layers

AI Governance defines legitimate purposes, decision rights, responsibilities, oversight and remedies.

Trustworthy AI defines the context-appropriate qualities a system should achieve, including robustness, safety, security, transparency, fairness and effective human oversight.

Trusted AI makes selected claims and controls machine-verifiable for a specified actor, action, context and time. Trusted execution is the resulting authorised decision and action under those controls.

These layers should remain distinct and connected. Governance without operational enforcement may remain procedural. Trustworthy properties without current authority may still permit the wrong actor to act. A credential proves a claim; it does not by itself prove that a specific action remains authorised now. Current status, delegated limits, purpose, evidence quality, relying-party policy and runtime conditions determine actionability.

3.2 The six-question execution chain

1. Who or what is acting? Identity and attribution establish the subject.
2. For whom may it act? Mandate and delegation establish representation.
3. Which facts support the action? Verifiable evidence and provenance establish the basis.
4. What do those facts mean? Shared semantics and validation rules establish interpretation.
5. Is the action permitted now? Current status, policy and runtime authorisation establish actionability.
6. What happens if execution fails? Monitoring, interruption, recovery and accountability close the control loop.

3.3 Trust Algorithms and threshold-based control

NIST SP 800-207 defines a Trust Algorithm as the process used by a policy engine to grant or deny access to a resource [11]. Agentic, Industrial and Physical AI require this logic beyond access alone. A control-plane Trust Algorithm evaluates identity, mandate, asset or workload posture and policy. An evidence-plane Trust Algorithm evaluates provenance, authority, semantic validity, freshness, contradiction and fitness for purpose. An action-authorisation decision combines both with model state, environmental context, cyber-security posture, functional-safety limits and recoverability. Outputs can be permit, restrict, escalate or deny.

This infrastructure also supports defence against fraud, deepfakes, model attacks and cyber conflict. AI increases the speed and personalisation of social engineering, while agents create new attack surfaces through tools and physical systems. Content appearance is therefore insufficient. Organisations need verifiable sources, least privilege, tool restrictions, isolated execution, decision thresholds, continuous monitoring, rapid revocation and tested recovery.

4 Where Europe can create value

Europe's opportunity extends from administrative work to machines, infrastructure and scientific discovery. The common value mechanism is wider authorised process coverage: organisations can move from assistance at the edge of a workflow toward accountable execution in core processes. The economic value comes from redesigning the whole activity, including data capture, evidence, exceptions, authorisation, audit and recovery.

4.1 Administrative and agentic economy

Accounting, procurement, customer service, reporting, compliance, human resources and supply-chain administration contain repeated classifications and high verification loads. Task studies report faster completion and higher output in bounded settings, while firm evidence shows larger gains when AI is combined with process and capital investment [12, 13]. Trusted automation can also shift work away from data entry, reconciliation and administrative anxiety toward judgement, customer work, design, care and quality assurance.

B2B agentic commerce offers an immediate transaction base in procurement, logistics, financing, compliance and industrial services. Agents can discover suppliers, request quotes, verify company status, negotiate within approved ranges, check product evidence, place orders and monitor fulfilment. Reusable organisational identity, mandates, status and transaction evidence can replace repeated bilateral checks with shared infrastructure. B2C agents can reduce search and switching costs, provided that identity, delegation, spending limits, merchant claims, cancellation rights and redress remain enforceable.

4.2 Industrial and Physical AI

Industrial AI applies learning systems to engineering, planning, quality, energy, maintenance and supply networks. Europe holds process knowledge, installed machinery, equipment expertise and regulated product domains that general benchmarks capture only partially. High-value applications include generative engineering, predictive maintenance, quality inspection, digital twins, energy optimisation and coordinated industrial services. Runtime authority must remain bounded: a planning agent may recommend a production change, while release to a machine requires verified configuration, role authority, risk gates and a safe fallback state.

Physical AI connects perception, reasoning and action through robots, autonomous vehicles, laboratories, warehouses, drones, healthcare equipment, grids and critical infrastructure. It can address labour scarcity, hazardous work, inspection and high-mix manufacturing. It also expands the harm boundary. Safety cases, trusted sensor and asset identity, environment limits, software and configuration evidence, functional-safety controls, runtime monitoring and human takeover therefore form part of the economic architecture. Europe can create an export proposition in verifiably governed machinery and infrastructure rather than competing only on model scale.

4.3 Public-sector and scientific transformation

Business-to-government and government-to-government processes can create dependable demand. Public bodies can act as authoritative credential issuers, high-frequency verifiers, procurement customers, cross-border process owners and creators of recurring use. Candidate processes include licences, grants, tax, customs, public procurement, environmental reporting and inspections. Shared evidence can reduce burden, strengthen fraud detection and improve appeal and oversight. Autonomous laboratories add a scientific channel by shortening the loop between hypothesis, synthesis, measurement and learning, provided that provenance, calibration and reproducibility remain visible.

European Business Wallets are one component. The proposed framework can support organisational identification, authentication, attestations and electronic mandates. It should be treated as an access, custody, presentation and authority-management component within a wider trust infrastructure. Authoritative sources, issuers, trust registries, status services, semantics, policy engines and relying-party verification remain essential. Commission analysis modelled direct annual benefits between approximately EUR 58.4 billion and EUR 169 billion across assumptions. The estimate is ex ante. Realised value depends on adoption, credential supply, verifier coverage, current status, semantic alignment, actual usage and process redesign (European Commission, 2025a, 2025b).

5 Three transformation regimes

The Trusted Execution Transformation and Diffusion Model, TETDM, is a transparent scenario instrument. It separates stakeholder acceptance from authorised process depth, and adoption readiness from effectiveness after deployment. It combines adoption, implementation velocity, complementary capability, resource reassignment, trust, transition cost and spillovers. The reference path begins at an index of 100 in 2026 and grows by 0.5 per cent annually. It embeds globally available digital technology and continuation of current productivity trends while assigning zero additional post-2026 growth to the transformation mechanisms modelled in TETDM.

Fragmented drift combines slow implementation, national fragmentation, vendor silos and pilot funding. Firms adopt assistants while core-process redesign and cross-border reuse remain limited.

Coordinated acceleration combines stable direction, faster implementation, common procurement cases, interoperable trust services and mission coalitions that redesign selected core processes.

Trusted industrial leadership treats execution infrastructure as a strategic European asset. Capability anchors connect strong firms, start-ups, research institutions, equipment makers and public users. Open interfaces and diffusion mechanisms carry successful components into adjacent sectors and regions.

Figure 2 shows how the three conditional transformation regimes diverge through 2040.

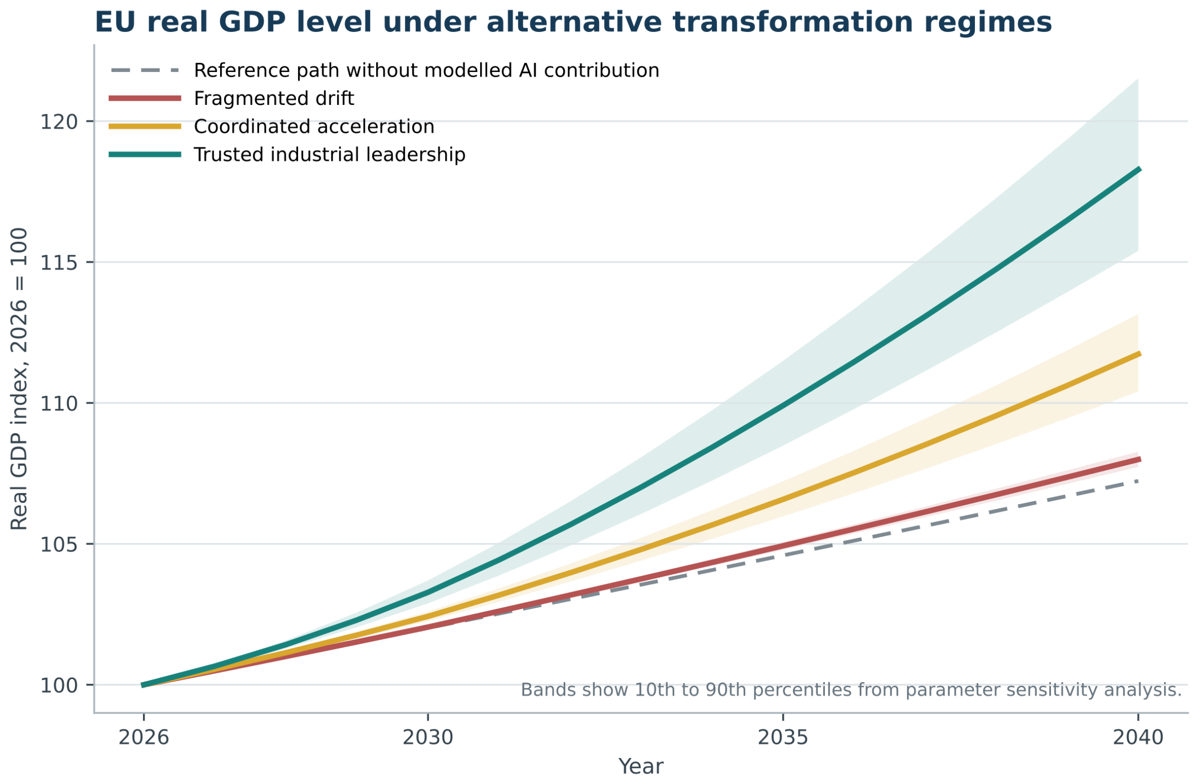

Figure 2: Modelled EU real-GDP level under alternative transformation regimes, 2026 to 2040. Lines are medians; bands show the 10th to 90th percentiles from 6,000 parameter draws.

Note: Conditional scenarios, not forecasts. The median 2040 result is below one per cent above the reference path in fragmented drift, around four per cent in coordinated acceleration and around ten per cent in trusted industrial leadership. The regimes diverge gradually as adoption, complementary capital, authorised process depth, resource reassignment and spillovers accumulate. Early sensitivity bands overlap. The upper case requires exceptional institutional and corporate execution. Permitted interpretation: the model estimates outcomes under coherent transformation regimes in which trusted execution is one necessary complement. It does not identify an isolated causal coefficient for trust infrastructure and does not predict the distribution of gains among workers, firms and states. It does not address and predict economic damages from fraudulent actions, illicit behaviour or offensive cyber capabilities.

6 Systemic and holistic leadership

Bill Gates frames the current period as a simultaneous source of broad economic and social value and of structural risks to employment, community stability, security, equality and public trust [15]. His message to leaders is that they have a chance to act now, before disruption weakens communities and legitimacy. For Europe, this means managing opportunity creation and transition risk through one connected architecture rather than distributing responsibility across separate bureaucratic programmes.

Systemic and holistic thinking and execution require shared outcomes and decision rights across industrial, labour, education, fiscal, security, health, competition and public-service policy. They require cross-ministry ownership, public-private implementation organisations, participation by workers, regions and affected communities, shared evidence and metrics, and feedback from realised benefits and harms into policy adjustment. International coordination remains necessary where markets, model supply chains, cyber risks and information flows cross borders.

6.1 Capability anchors and engineered diffusion

Europe should assemble its strongest complementary teams around a limited portfolio of measurable missions. An industrial mission may combine a manufacturer, specialised Mittelstand suppliers, a robotics or equipment firm, an AI company, a systems integrator, a trust-infrastructure provider, a university, a vocational network, an insurer and a public deployment customer. The mission should specify the operational outcome, owner, budget, assurance boundary, dependencies and path to scale.

Concentrating capability at the frontier creates value only when diffusion is designed. Public support should therefore buy open interfaces, conformance artefacts, supplier participation, measurable milestones and transfer plans. Regional and sector nodes should provide shared engineering, managed trust services, data preparation, evaluation, cybersecurity, training and change support. Supplier academies, secondments, reference deployments and reusable credentials can move tacit knowledge and reduce uncertainty. Transparent admission, time-limited mandates and independent competition review protect contestability.

6.2 Public demand and corporate commitment

Public procurement can convert standards and pilots into recurring demand. Authorities should select high-frequency processes in which reusable organisational, professional and product evidence can reduce burden. Procurement specifications should require portability, auditability, security and open conformance. Public bodies should also improve authoritative credential issuance and verifier readiness so that market participants have real processes in which the infrastructure creates value.

Corporate leaders need to move from tool portfolios to transformation portfolios. A first horizon raises productivity in bounded tasks. A second redesigns end-to-end processes such as procure-to-pay, engineering change, maintenance and regulatory reporting. A third changes the operating model through agentic commerce, autonomous operations and outcome-based services. Boards should identify which legacy processes will be retired, simplified or rebuilt, and should join cybersecurity, legal, operations, finance and worker representatives before production gates.

6.3 Social transition is an adoption mechanism

Trusted automation can release people from repeated verification, data entry and reconciliation. It can support better work when skills, occupational mobility, participation and benefit-sharing are designed into the programme. These measures also improve adoption because employees hold essential process knowledge and bear transition costs. Higher productivity can support wages, a broader tax base and ageing societies when competition, bargaining, skills and fiscal institutions distribute the gains.

7 Leadership and implementation agenda

7.1 Priorities for policy makers

1. Establish a European Trusted Execution Infrastructure programme that aligns AI Governance, Trustworthy AI assurance, digital identity, organisational and asset identity, verifiable evidence, Trust Algorithms and runtime policy enforcement.
2. Create high-capability national public-private implementation units with accountable ownership, direct escalation routes and measurable time-to-capability targets.
3. Use public procurement and authoritative credential issuance to create recurring cross-border demand rather than isolated pilots.
4. Fund complementary capabilities, including data engineering, organisational redesign, cybersecurity, functional safety, skills, energy and systems integration.
5. Launch a small portfolio of Industrial and Physical AI missions with capability anchors, shared test facilities and open conformance requirements.
6. Integrate worker participation, portable training, occupational mobility, regional adjustment and benefit-sharing into the productivity strategy.

7.2 Priorities for boards and executive teams

1. Select core processes for redesign, retirement or consolidation. Avoid funding AI beside every legacy activity.
2. Conduct risks analysis and set risk appetite by action. A drafting assistant, payment agent, physical actuator and critical infrastructure control system require different authority, evidence, safety and recovery thresholds.
3. Reassign capital, people and management attention toward deployment. Track the cost of delay and the productivity J-curve.
4. Build partnerships across models, data, equipment, integration, trust infrastructure, cybersecurity, assurance and public authorities. Preserve portability, evidence ownership and exit rights.
5. Measure time-to-capability: idea to approved production, source data to verified evidence, pilot to recurring operation, update to validated release, incident to containment and first deployment to external reuse.
6. Preserve evidence from failed projects, stop weak approaches and move resources quickly to stronger ones.

7.3 A 36-month sequence

- First 12 months: select missions, appoint accountable organisations, establish baselines, publish initial credential and evidence profiles, identify deployment owners and map core processes and action-level risk.
- Months 12 to 24: operate production deployments with large scale user bases, budgets and assurance. Open procurement frameworks, shared test facilities, managed trust services and supplier training to followers.
- Months 24 to 36: stop or redesign weak approaches, move strong components into recurring procurement and private investment, and diffuse them into adjacent sectors and jurisdictions.

7.4 Measures that matter

Leaders should track production-grade adoption, authorised process coverage, cycle time, quality, output, avoided loss, reusable credentials and mandates, verifier and Trust Algorithm coverage, incident rates, recovery time, external reuse and supplier upgrading. Activity counts, announcements and pilot volume are weak substitutes for operational evidence.

Selected references

[1] Draghi, M. (2024). *The Future of European Competitiveness*. European Commission. https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en

[2] Eurostat (2025). *Population structure and ageing*. Statistics Explained. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Population_structure_and_ageing

[3] Acemoglu, D. (2024). *The Simple Macroeconomics of AI*. NBER Working Paper 32487. https://www.nber.org/papers/w32487

[4] OECD (2026). *Foundations for Growth and Competitiveness 2026*. OECD Publishing. https://www.oecd-ilibrary.org/en/publications/foundations-for-growth-and-competitiveness-2026_40a7532f-en.html

[5] Aldasoro, I., Gambacorta, L., Korinek, A., Rees, D. and Stein, M. (2026). AI adoption, productivity and employment: evidence from European and US firms. *BIS Working Papers*, No. 1325. https://www.bis.org/publ/work1325.htm

[6] Coase, R. H. (1937). The Nature of the Firm. *Economica*, 4(16), 386–405. https://doi.org/10.1111/j.1468-0335.1937.tb00002.x

[7] North, D. C. (1990). *Institutions, Institutional Change and Economic Performance*. Cambridge University Press. https://doi.org/10.1017/CBO9780511808678

[8] European Commission (2024). Regulation (EU) 2024/1183 establishing the European Digital Identity Framework. https://eur-lex.europa.eu/eli/reg/2024/1183/oj

[9] European Commission (2025a). Proposal for a Regulation establishing European Business Wallets, COM(2025) 838 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2025:838:FIN

[10] GLEIF (2026). *The verifiable LEI (vLEI): Digital organisational identity for everyone*. Global Legal Entity Identifier Foundation. https://www.gleif.org/en/organizational-identity/lei-vlei/the-verifiable-lei-vlei

[11] NIST (2020). *Zero Trust Architecture*. NIST Special Publication 800-207. https://doi.org/10.6028/NIST.SP.800-207

[12] Noy, S. and Zhang, W. (2023). Experimental evidence on the productivity effects of generative artificial intelligence. *Science*, 381(6654), 187–192. https://www.science.org/doi/10.1126/science.adh2586

[13] Brynjolfsson, E., Li, D. and Raymond, L. R. (2025). Generative AI at Work. *Quarterly Journal of Economics*, 140(2), 889–942. https://academic.oup.com/qje/article/140/2/889/7990658

[14] European Commission (2025b). Analytical supporting document for the European Business Wallet proposal, SWD(2025) 837 final. https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2025)837&lang=en

[15] Gates, B. (2026). The Turbulent AI Era Is Here. The Choices We Make Now Are Critical. *Gates Notes*. https://www.gatesnotes.com/a-turbulent-ai-era-and-critical-choices-to-make

[16] European Central Bank (2025). The transformative power of AI. Speech, 24 November. https://www.ecb.europa.eu/press/key/date/2025/html/ecb.sp251124_1~c239fb4a7f.en.html

[17] European Commission (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Suggested citation. Harald, B. and Stöcker, C. (2026). *Europe's Fundamental AI Opportunity: Management Summary*. Spherity Research.