Government Publications Registration Number
11-1051000-100106-01

Knowledge Sharing Program

Strengthening Strategic Framework for SME Digital Transformation in Poland

Poland

2024/25 KSP POLICY BRIEF

Presented by the MOEF, Republic of Korea

Ministry of Economy and Finance
KDI Korea Development Institute
Ministry of Economic Development and Technology Republic of Poland

Presented by the MOEF, Republic of Korea

2024/25 KSP POLICY BRIEF

Strengthening Strategic Framework for SME Digital Transformation in Poland

Poland

Ministry of Economy and Finance
KDI Korea Development Institute
Ministry of Economic Development and Technology Republic of Poland

Project Title: Strengthening Strategic Framework for SME Digital Transformation in Poland

Prepared for
The Government of the Republic of Poland

In Cooperation with
Ministry of Economic Development and Technology (MRiT), Republic of Poland

Supported by
Ministry of Economy and Finance (MOEF), Republic of Korea

Prepared by
Korea Development Institute (KDI)

Project Director
Jungwook Kim, Executive Director, Center for International Development (CID), KDI

Project Manager
Joonghae Suh, Visiting Senior Fellow, CID, KDI

Project Officer
Sehoon Lee, Senior Research Associate, CID, KDI

Senior Advisor
Hohyun Jang, Former Auditor, Bank of Korea

Principal Investigator
Sangwon Ko, Senior Research Fellow, Korea Information Society Development Institute (KISDI)

Authors
Sangwon Ko, Senior Research Fellow, KISDI
Sehoon Lee, Senior Research Associate, CID, KDI
Hyesun (Melissa) Yoon, Professor, Hanyang University
Hyungjong Kim, Professor, Seoul Women's University
Paulina Kiewicz, Chief Specialist, MRiT
Katarzyna Colombel, Chief Specialist, MRiT

English Editor
Korea Translation Co., Ltd.

Government Publications Registration Number 11-1051000-100106-01
ISBN 979-11-7566-024-3 94320
979-11-5932-110-8 (set)

2024/25 KSP POLICY BRIEF

Strengthening Strategic Framework for SME Digital Transformation in Poland

Poland

Preface

In recent years, the global community has faced an increasingly complex set of challenges, including geopolitical tensions, disruptions in global supply chains, and the accelerating impacts of climate change. These trends have placed significant pressure on the international development landscape, with a noticeable decline in overall development finance. At the same time, development cooperation is evolving toward a more reciprocal and strategic approach that emphasizes mutual learning and shared benefits. Despite these challenges, collaboration remains essential for achieving lasting progress. Sustainable development requires countries to work together toward shared goals and to build partnerships that foster shared prosperity. By drawing on the diverse knowledge, policy experiences, and innovations that each country offers, the global community can find practical solutions to today's challenges and create pathways toward inclusive and sustainable growth.

The Knowledge Sharing Program (KSP), launched by Korea's Ministry of Economy and Finance (MOEF) in 2004, has served as a vital platform for sharing Korea's development experiences globally over the past 20 years. In addition to embedding joint research outcomes into the policies of partner countries, the KSP has advanced various international projects and highlighted the value of knowledge sharing in tackling global challenges together. In recent years, the program has also broadened its horizons through collaboration with advanced economies, further expanding the scope and diversity of its partnerships.

Since its inception, the Korea Development Institute (KDI) has participated in implementing the KSP, collaborating with more than one hundred countries. As Korea's leading think tank, the KDI has addressed a broad spectrum of issues faced by partner countries, from industrial development to digital transformation. During the 2024/25 KSP cycle, the KDI has undertaken twenty-three policy consultation projects that reflect the needs of partner countries.

Among the notable projects, "Strengthening Strategic Framework for SME Digital Transformation in Poland," led by the Ministry of Economic Development and Technology of Poland, exemplifies the spirit of international cooperation. On behalf of KDI, I would like to extend sincere appreciation to the Government of Poland, especially Deputy Minister Mr. Michał Jaros, for his continued leadership and insight. I also wish to thank the KSP consultation team —Senior Advisor Mr. Hohyun Jang, Principal Investigator Dr. Sangwon Ko, researchers Dr. Hyesun (Melissa) Yoon, Dr. Hyungjong Kim, and Mr. Sehoon Lee—and the local consultants Ms. Paulina Kiewicz, Ms. Katarzyna Colombel, and Mr. Paweł Kostkiewicz

for their dedicated and constructive contributions throughout the project. Special thanks also go to the Center for International Development (CID) at KDI, particularly Executive Director Dr. Jungwook Kim, Project Manager Dr. Joonghae Suh, and Project Officer Mr. Sehoon Lee for their diligent and consistent coordination throughout the project.

This Policy Brief presents key findings and practical policy options developed through the 2024/25 KSP consultation process. It is designed to meet the needs of both decision-makers and implementers by providing clear, context-aware insights drawn from collaborative research. We hope it serves not only as a reference, but as a catalyst for informed policy action in our partner countries.

This year's KSP laid a solid foundation for future-oriented cooperation between Poland and Korea—promoting practical policy exchange, strengthening mutual trust, and advancing our shared commitment to sustainable development. We are confident that this partnership will continue to deepen and contribute meaningfully to the long-term partnership between the two countries.

Cho, Dongchul
President
Korea Development Institute

Contents

Tables & Figures

Tables

Figures

Summary

Poland's economic future hinges on accelerating the digital transformation of its small and medium-sized enterprises (SMEs) in key areas, including digitalization, artificial intelligence (AI) adoption, and cybersecurity. SMEs account for 99.8% of Polish businesses and nearly half of GDP, making their digital competitiveness a matter of national priority. However, Poland currently lags behind its European peers—ranking 28th out of 36 OECD countries in the World Digital Competitiveness Ranking (WDC). Polish SMEs are slow to adopt advanced technologies: as of 2023, only 4% of enterprises use AI and 19% use data analytics, far below leading digital nations. This digital gap poses a strategic risk to Poland's long-term growth, productivity, and alignment with the EU Digital Decade 2030 targets. The government recognizes the urgency; national strategies such as the Digital Decade Plan and Digitalization Strategy 2035 set ambitious goals (e.g., 90% of SMEs with basic digital intensity, 34% using AI by 2030). However, concrete actions are needed to turn these targets into reality.

Polish SMEs face multiple barriers on the path to digital transformation. According to a 2024 survey conducted by MRiT and KPMG, only 30% of SMEs are either "ready to act" or already digital leaders, whereas one-third remain uninterested in digitalization. Key obstacles include low awareness of digital benefits, scarce knowledge of available support programs, high costs of new technologies, and shortages of skilled IT personnel. Even when support programs exist, they often do not reach the smallest firms. Poland has promising initiatives through agencies such as PARP and NASK, but there is a "significant implementation gap, particularly for micro-enterprises." Institutional fragmentation further impedes progress, as responsibilities for SME digitalization are split among multiple ministries and agencies with limited coordination, thereby weakening policy coherence. Meanwhile, Poland's R&D investment remains around 1% of GDP, significantly below the OECD average, which constrains innovation and the talent pipeline. These challenges underscore the need for an integrated and well-resourced national support system.

This report provides a comprehensive analysis of Poland's current situation and recommends a policy agenda to strengthen the SME digital transformation ecosystem. Critically, it benchmarks Korea's best practices as a guide for Poland's policy design. Korea offers a compelling model, having achieved high rates of technology adoption among its SMEs through proactive government programs and public-private partnerships. For example, Korean SMEs have some of the world's highest adoption rates of advanced tools such as AI and Internet of Things (IoT), with minimal gaps between small and large firms. Korea's multi-faceted approach—from its Smart Factory initiative that modernized 30,000 manufacturing SMEs, to Data/AI Voucher programs that directly subsidize SMEs' technology projects,

to regional cybersecurity centers that assist local businesses—provides actionable models for Poland. Drawing on these insights, the report outlines tailored recommendations for Poland under three pillars:

1) Enhancing Governance and Strategy: Establish a more integrated governance framework to coordinate SME digitalization efforts across ministries and agencies, ensuring consistent policy direction and monitoring. Strengthen public–private and academic partnerships to leverage all stakeholders in the innovation ecosystem.

2) Scaling Effective Support Programs: Implement targeted programs based on proven Korean models—a National Smart Factory Initiative to drive Industry 4.0 adoption in manufacturing, a Smart Service Voucher scheme to digitalize service-sector SMEs, and data/AI voucher programs to fund SMEs' uptake of data analytics and AI solutions. Expand regulatory sandboxes beyond fintech to include AI, smart manufacturing, and other sectors, providing innovators with room to experiment under temporarily relaxed regulations.

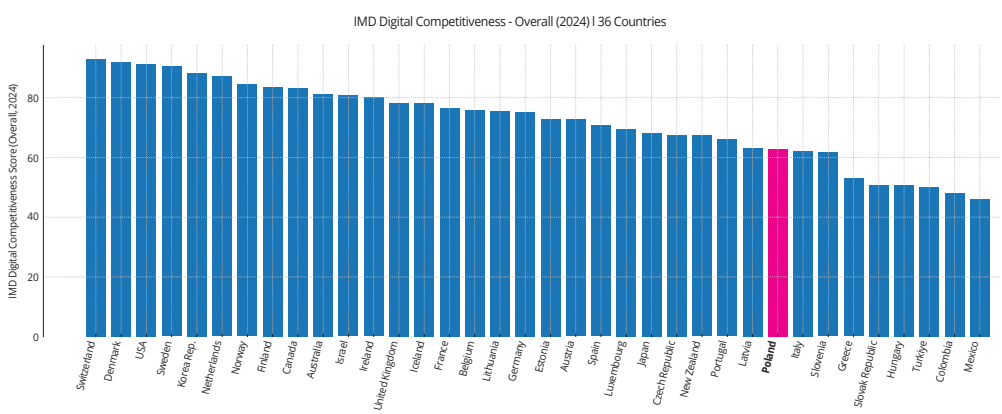
3) Improving Cybersecurity and Resilience: Develop a multi-layered SME cybersecurity support system. This includes setting up regional cybersecurity support centers to provide on-the-ground assistance, introducing simplified certification pathways to ease compliance burdens, protecting SME innovations through robust technology protection frameworks, and offering "security-as-a-service" solutions and turnkey packages that make it simple for resource-constrained firms to secure their operations.

By implementing these recommendations, Poland can significantly accelerate SME digital transformation in line with EU targets while tailoring support to its domestic context. In practical terms, the proposed measures will raise awareness and demand for digital tools among SMEs, lower the costs and risks of adoption, and build local capabilities (skills, solution providers, innovation hubs) that sustain progress. A conservative estimate is that these efforts could boost the share of Polish SMEs integrating advanced digital technologies from the current low levels into the double digits within the next five years, narrowing the gap with EU frontrunners. More importantly, they will enhance the competitiveness and resilience of Poland's SME sector, ensuring that even the smallest firms can thrive in the digital economy and contribute to Poland's growth. In summary, Poland's digital transformation journey for SMEs can be vastly accelerated by learning from Korea's success, improving coordination, and investing boldly in the necessary support systems. The time to act is now, before the digital divide widens further. The following report elaborates on these findings and lays out a roadmap for action.

1. Introduction

Digital transformation is no longer optional; it is a strategic imperative for Poland's economic development and competitiveness. Since joining the EU in 2004, Poland has enjoyed robust growth, becoming a major manufacturing and services hub in Central Europe. However, in recent years, productivity gains have slowed, and Poland's economy risks being left behind in the fourth industrial revolution. A key reason is the slow diffusion of digital technologies among Polish businesses, especially SMEs. Despite accounting for nearly half of GDP, Polish SMEs lag significantly in adopting digital tools and advanced technologies. Poland ranked 28th out of 36 OECD countries in the 2024 World Digital Competitiveness Ranking (WDC), placing it among the lower performers in digitalization. In particular, it scored relatively low on the Future Readiness Index, which assesses preparedness for digital transformation in areas such as adaptive attitudes, business agility, and IT integration (IMD, 2024).

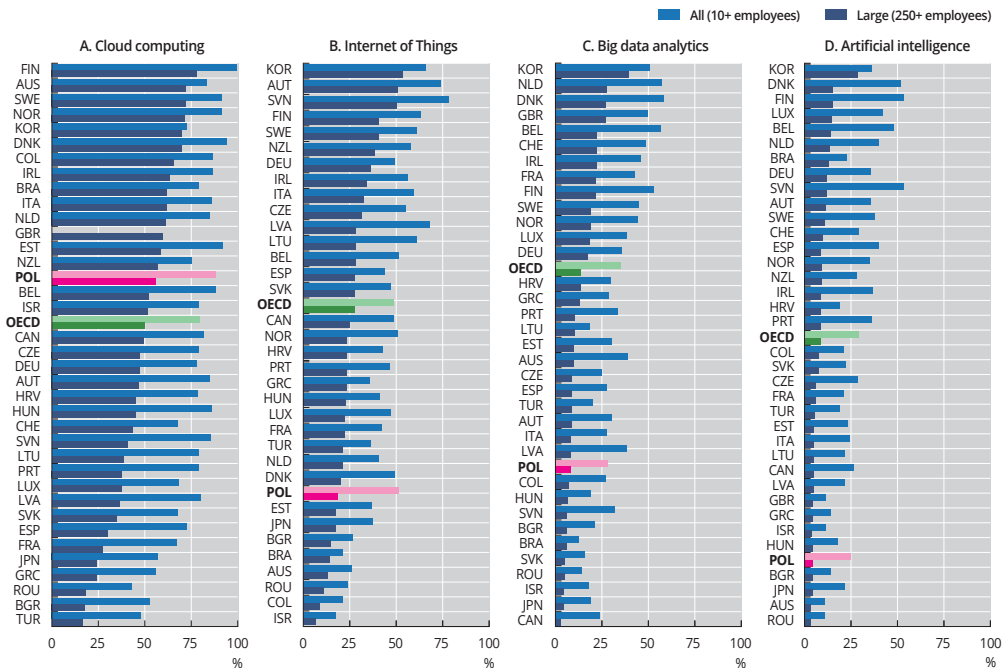
Figure 1.
IMD World Digital Competitiveness Ranking (OECD member countries)



Source: Author's compilation based on information from the World Digital Competitiveness Ranking (2024).

This digital deficit is particularly evident in cutting-edge areas: as of 2023, only about 4% of Polish enterprises use AI, and 19% use Big Data Analytics, highlighting a significant gap compared to leading economies. In Korea, by contrast, AI is adopted by 28% of businesses and Big Data Analytics by 40%, the highest adoption rates among OECD countries. Moreover, Korea demonstrates minimal digital adoption gaps between large firms and SMEs, underscoring a more inclusive and advanced digital transformation landscape (OECD, 2024).

Figure 2.
Adoption of Data-Driven Technology by Firms (2023)



Source: OECD (2024).

The message is clear: Poland needs to accelerate the digitalization of its SME sector or risk eroding its competitive edge in the global market. The strategic importance of SME digitalization, AI adoption, and cybersecurity cannot be overstated. Embracing these technologies will enable Polish firms to boost productivity, innovate in products and services, and expand into new markets. AI, in particular, has transformative potential. Poland's Digitalization Strategy 2035 emphasizes that it can "significantly improve industrial production capacity, efficiency, and the quality of services provided." Likewise, robust cybersecurity underpins trust in digital operations and protects the gains of digitalization from cyber threats. The Polish government recognizes these interconnections, and national strategic documents set out bold ambitions for the coming decade. The EU's Digital Decade 2030 goals, to which Poland has committed, include targets such as 90% of SMEs reaching at least a basic level of digital intensity and 75% of enterprises using cloud services by 2030 (European Commission, 2022a). Poland's Digitalization Strategy 2035 goes further, explicitly identifying SME digital transformation as a core priority and extending the vision to 2035. The strategy calls for comprehensive measures, including improved policy coordination, expanded support programs to stimulate SME demand for digital technologies, a focus on Poland's high-potential industries, stronger public-private collaboration, and enhanced cybersecurity for SMEs. In tandem, Poland's authorities are developing a new "Digital Transformation

Program for Enterprises" (expected around 2026) to operationalize these goals with specific actions and an integrated support system (MRiT, 2025). This flurry of planning suggests growing recognition at senior levels that SME digital transformation is important to Poland's future, and that changes to the current approach are increasingly seen as necessary.

Table 1.
Digital Decade KPI of Poland and the EU

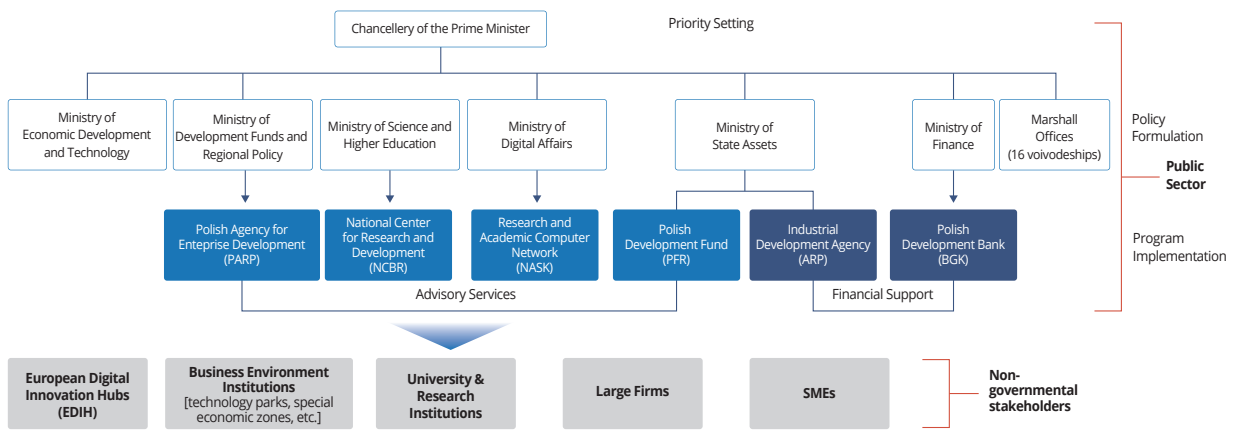
Digital Decade KPI[1]	Poland				EU		Digital Decade target by 2030	
	DESI 2024 (Year 2023)	DESI 2025 (Year 2024)	Annual progress	National trajectory 2024 (3)	DESI 2025	Annual progress	PL	EU
Fixed Very High Capacity Network (VHCN) coverage	81.1%	83.8%	3.4%	84.1%	82.5%	4.9%	100.0%	100%
Fibre to the Premises (FTTP) coverage	75.4%	77.8%	3.1%	84.1%	69.2%	8.4%	100.0%	-
Overall 5G coverage	71.9%	89.3	24.1%	98.3%	94.3%	5.9%	100.0%	100%
Edge Nodes (estimate)	42	82	95.2%	11	2257	90.5%	370	10000
SMEs with at least a basic level of digital intensity (2)	-	69.0%	6.4%	-	72.9%	2.8%	90.0%	90%
Cloud	46.5%	-	-	-	-	-	75.0%	75%
Artificial Intelligence	3.7%	5.9%	60.8%	4.3%	13.5%	67.2%	10.0%	75%
Data analytics	19.3%	-	-	-	-	-	35.0%	75%
AI or Cloud or Data analytics	51.8%	-	-	-	-	-	-	75%
Unicorns	10	11	10.0%	13	286	4.4%	20	500
At least basic digital skills	44.3%	-	-	-	-	-	80.0%	80%
ICT specialists	4.3%	4.5%	4.7	4.3	5.0%	4.2%	6.0%	~10%
eID scheme notification	-	yes	-	-	-	-	-	-
Digital public services for citizens	63.7	70.7	10.9%	81.5	82.3	3.6%	100.0	100
Digital public services for businesses	72.9	85.0	16.6%	87.4	86.2	0.9%	100.0	100
Access to e-Health records	90.0	91.8	2.0%	88.0	82.7	4.5%	100.0	100

Source: European Commission (2025a).

However, translating strategy into tangible results remains challenging. Poland's current support ecosystem for SME digitalization is not yet fully integrated, leaving many firms without adequate support. Key actors include MRiT's Department of Digital Economy (policy lead), the Ministry of Digital Affairs (national digital strategy, infrastructure, cybersecurity), and several implementing agencies: PARP (SME programs), NASK (digital skills and cybersecurity projects), NCBR (R&D and innovation funding), PFR and ARP (enterprise financing and training), and BGK (loans and guarantees). While each has a distinct role, their efforts operate in silos, with overlapping mandates and no central coordinating body. Frequent government reorganizations and shifting oversight responsibilities have further undermined continuity and coherence. As a result, the support landscape is difficult for SMEs to navigate and challenging for the government

to manage strategically. Many SMEs are unaware of the support available. A recent KPMG survey found that a significant share of Polish SMEs are unaware of existing digital transformation programs. Limited coordination also hampers evidence-based policymaking, as Poland lacks a unified monitoring framework to track SME digital adoption or program outcomes. The forthcoming Digital Transformation Program for Enterprises offers a timely opportunity to address these governance gaps by fostering an integrated innovation ecosystem with stronger coordination across public and private actors.

Figure 3.
National Governance System Supporting SME Digitalization in Poland



Source: Author.

Equally pressing are the on-the-ground challenges faced by SMEs themselves, which Poland's support system must help overcome. Surveys consistently highlight a mix of financial, informational, and human capital barriers. Many Polish SMEs, especially micro-firms, do not fully appreciate the benefits of digitalization; over 33% of SMEs in 2024 reported being simply uninterested in pursuing digital transformation. This points to an awareness and mindset gap; firms may fear that digitalization is costly with uncertain returns. Indeed, cost constraints are a top barrier: smaller companies often find the upfront investment in new IT systems, automation, or training prohibitive without external support (KPMG, 2024). Compounding this, Polish SMEs suffer from a shortage of digital skills and IT specialists. Only 44% of Poles have basic digital skills, compared with the EU average of 56%, and the share of ICT specialists in the workforce is below the EU average. SMEs struggle to hire or retain the talent needed to implement and maintain digital technologies. They also report difficulty in integrating new digital solutions into legacy systems and processes, as well as concerns about cybersecurity and data privacy when transitioning to digital (European Commission, 2024a). As of 2023, Poland's overall R&D and innovation capacity remains constrained

by relatively low R&D spending, which stood at 1.56% of GDP, below the EU average of 2.13% and significantly lower than Korea's 4.96% (OECD, 2024c). This underinvestment contributes to a limited supply of locally developed solutions tailored to the needs of SMEs. Moreover, the share of Polish firms innovating in products or processes remains below the EU average (European Commission, 2024b), with Polish businesses being half as likely to introduce product and business innovations compared to their European counterparts. Public investment in R&D has also lagged, amounting to just 0.5% of GDP. Innovation in SME manufacturing firms, especially those integrated into global value chains through multinational enterprises, faces high barriers—including excessive costs, limited access to public funding, and persistent skills shortages (OECD, 2025a; OECD, 2025b). Policy fragmentation on the supply side mirrors the SME perspective: support programs are viewed as complex and scattered, making it hard for a small business to find the right support at the right time. In summary, Polish SMEs face a combination of "knowledge and awareness barriers," "skill and resource constraints," and "technical and regulatory challenges" in digital transformation. The urgency for Poland is to address these hurdles holistically—raising awareness, subsidizing costs, building skills, simplifying regulations—to unlock SME digitalization at scale.

Crucially, Poland is not starting from scratch. The government has laid important groundwork through national plans and participation in EU programs. The National Action Plan for the Digital Decade (adopted October 2024) aligns Poland with EU-wide 2030 targets, committing to milestones such as 75% of enterprises using cloud, 35% using data analytics, and 34% using AI by 2030. Complementing this, the Digitalization Strategy 2035 provides a comprehensive domestic roadmap for digital transformation across infrastructure, skills, innovation, and cybersecurity, with SMEs featured prominently. Poland also channels substantial EU funding into digital projects: under the 2021–2027 EU budget and the Recovery and Resilience Facility, billions of euros are allocated to programs related to business digitalization, digital public services, and innovation (over half of the thematic funding areas touch SME digital competitiveness). For example, the previous Digital Poland Operational Program (2014–2020) invested in broadband and e-services. In the new EU financial perspective, separate funds target different needs: the European Funds for a Modern Economy (FENG) are earmarked for enterprises and R&D institutions, particularly to support SME technology adoption, while the European Funds for Digital Development (FERC) focus on public administration, including the financing of public e-services for citizens and businesses. Existing national initiatives include sectoral strategies (like an AI Development Policy and a Cybersecurity Strategy) and pilot support measures. PARP operates European Digital Innovation Hubs (EDIHs) that offer advisory services to SMEs, and grant programs (such as "Digital SME" in the past) have co-financed SME technology projects. NASK's "Fundamentals of Business Cybersecurity" certification program helps SMEs improve

cybersecurity awareness. Despite these efforts, the impact to date has been modest—Poland's digitalization metrics for SMEs remain well below EU averages. A criticism is that past initiatives were too broad and not sufficiently targeted at SMEs. Much of the focus has been on general digital infrastructure or e-government, rather than the specific digital transformation of SME business processes. For instance, funds have built networks and digital public platforms (important prerequisites). Still, fewer resources have been allocated to demand-side support that directly helps SMEs acquire new technologies or skills. Moreover, as noted, the plethora of programs would benefit from greater alignment under a common framework, as overlaps and gaps remain (for example, many micro-enterprises fall through the cracks between innovation grants geared toward larger SMEs and basic digital literacy programs that do not translate into tech adoption).

This report aims to support Polish policymakers in bridging these gaps by learning from international best practices, notably Korea's experience. The Republic of Korea transformed itself into a global digital leader through an orchestrated mix of policies that fostered SME innovation, from regulatory sandboxes enabling agile experimentation to massive programs upgrading SME manufacturing (the Smart Factory initiative) and services (Smart Service program). Korea's success was underpinned by strong government coordination and industry partnership—a model that holds valuable lessons for Poland. In the subsequent sections, we first provide a detailed comparative assessment of the current status and challenges of SME digital transformation in Poland versus Korea, to pinpoint specific areas for improvement. We then present actionable policy recommendations tailored to Poland's context, drawing inspiration from proven Korean programs and governance approaches, as well as relevant EU and international examples. By the end of this report, it will be evident that Poland has much to gain by adopting a more integrated support system: one that not only funds and guides SMEs in going digital, but also builds an ecosystem of technology providers, skills, and innovation-friendly regulations. Such a system can empower Polish SMEs to harness digital tools, boost their productivity, and compete on the European and global stage. Strengthening Poland's national framework for SME digital transformation has become both timely and necessary. In this context, Korea's experience presents an empirically grounded model from which valuable insights can be drawn.

2. Current Status and Challenges in SME Digitalization in Poland

2.1. Digitalization and AI Adoption: Gaps Between Poland and Korea

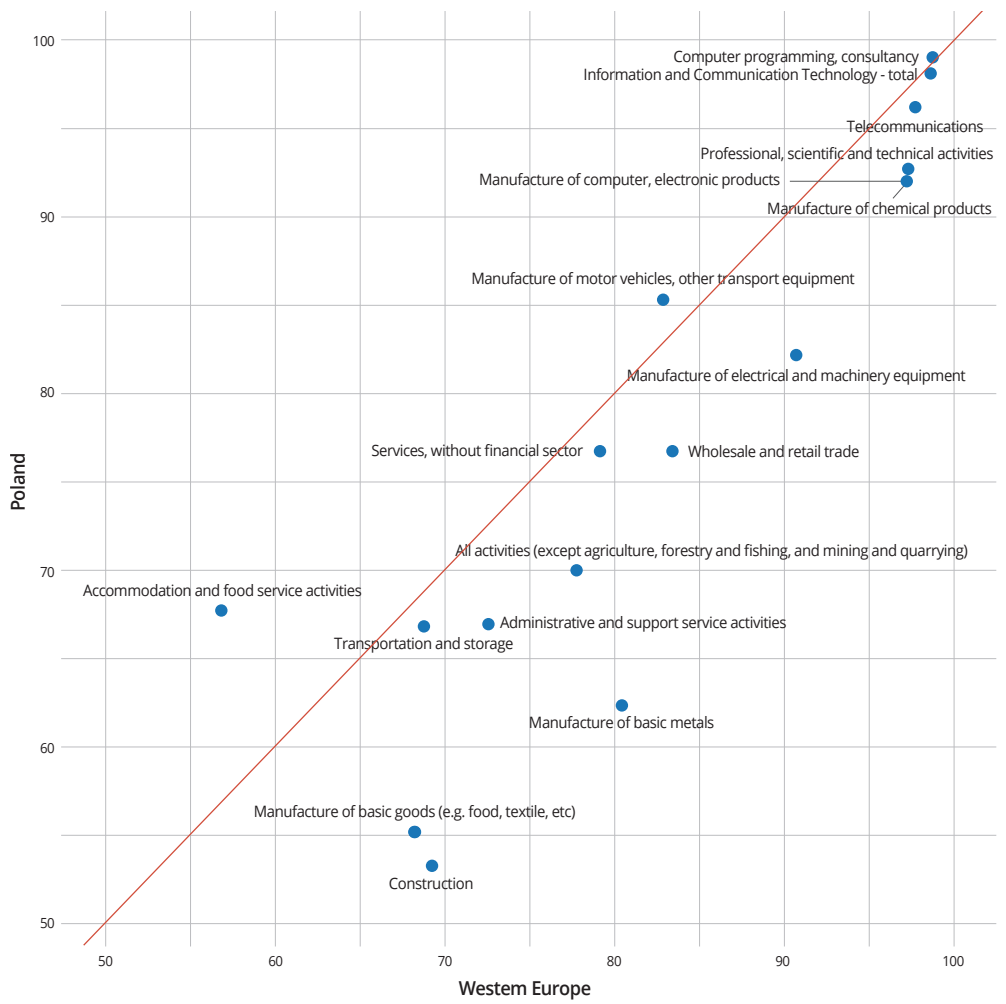
Polish SMEs demonstrate lower levels of digital maturity compared to their counterparts in Korea. This disparity is evident in both the overall diffusion of digital technologies and the degree of sophistication in their use. Poland ranks near the bottom among EU member states in SME digital integration, and Polish firms lag behind not only Western European countries but also leading countries including Korea. OECD data indicate that digital technology adoption in Korea is widespread across firms of all sizes, whereas in Poland, uptake is concentrated primarily among larger enterprises. For instance, cloud computing is used by 70% of Korean firms and 56% of Polish firms. Among large firms with 250 or more employees, however, the adoption rate is higher in Poland (88%) than in Korea (73%), suggesting that Poland's adoption is more concentrated at the top. At the same time, Korea exhibits broader diffusion across firm sizes, including SMEs (OECD, 2024).

In emerging technologies, discrepancies in measurement complicate direct comparisons, but the overall trend remains consistent. According to the European Commission, 4% of Polish firms have comprehensively adopted AI (European Commission, 2024c). Data from the Polish statistical office (GUS) place AI usage at 5.9% (Eurostat, 2025), while private sector research reports that 30% of companies indicate some degree of AI integration, with a 36% year-over-year increase (Amazon Web Services, 2024). Despite these variations, Poland remains well behind Korea, which reports the highest rate of AI adoption in the OECD and limited variation between large and small firms. Korea also leads in the adoption of Big Data analytics and Internet of Things (IoT) technologies. National programs such as Smart Factory and public digital platforms have contributed to this trend. In Poland, the use of these technologies by SMEs remains limited. The observed gap is not only quantitative but structural. In Korea, digital technology is adopted across the enterprise sector in a relatively balanced manner. In Poland, by contrast, adoption is concentrated among large firms, and the gap between large and small enterprises exceeds the OECD average.

Korea's digital infrastructure and adoption metrics are world-class. Korea ranks second in the OECD for broadband penetration, with one of the highest fiber-optic coverage rates, providing a strong foundation for digital business. It also leads in industrial automation—a telling proxy for digital technology adoption—with 1,012 industrial robots per 10,000 manufacturing workers, far above Germany (415) or Japan

(397). Poland, by contrast, has only 78 robots per 10,000 workers, ranking 28th globally and well below the global average (IFR, 2024). This indicates that the Polish industry, especially SMEs in manufacturing, has not widely adopted advanced automation and digital manufacturing techniques. The digitalization gap is also evident across sectors within Poland: highly digital sectors such as ICT or finance are closer to international norms, but traditional sectors (manufacturing of food, textiles, basic metals, as well as many service trades) have very low digital intensity. Indeed, the gap between Poland and Western Europe is largest in those industries with generally low digitalization, suggesting Poland's least digital sectors are falling even further behind as illustrated in Figure 4.

Figure 4.
Digitalization Gap by Industry Sector between Poland and Europe



Note: This analysis is based on the 2024 Eurostat Digital Intensity Index, specifically the indicator "Enterprises with at least a basic level of digital intensity." It presents the proportion (0–100%) of enterprises with at least a minimum level of digital capability, broken down by industrial sector. The figure for Western Europe refers to the average value across five countries: Germany, France, Italy, the Netherlands, and Sweden.

Source: Compiled and elaborated by the author based on information from Eurostat (2024).

The regulatory environment presents additional challenges for the adoption of AI. As an EU member implementing the Artificial Intelligence Act (Regulation 2024/1689), Poland faces substantial compliance burdens. Manufacturing SMEs in Poland incur annual regulatory costs of EUR 150,000 to EUR 400,000, compared to EUR 60,000 to EUR 150,000 in Korea (2.5 times higher). In contrast, service SMEs face EUR 110,000 to EUR 230,000 versus EUR 50,000 to EUR 130,000 (2 times higher). These costs stem primarily from EU AI Act compliance, GDPR complexity, and cybersecurity obligations. Poland is preparing its legislative response through the draft Act on Artificial Intelligence Systems (February 2025), which establishes KRiBSI as the national supervisory authority (Ministry of Digital Affairs, 2025). This approach, while ensuring EU compliance, creates additional coordination challenges compared to Korea's integrated approach.

The AI adoption landscape varies significantly across Polish industry sectors (Amazon Web Services & Strand Partners, 2024). Defense and aerospace lead with 71% adoption rates, primarily in quality control and cybersecurity applications. Manufacturing follows at 47%, focusing on predictive maintenance and process automation. Financial services achieve 40% adoption, particularly in credit analysis and fraud detection. E-commerce shows 38% adoption with emphasis on personalization and dynamic pricing. However, traditional service sectors lag significantly, with logistics at 25% and healthcare at 18%, indicating substantial opportunities for targeted intervention (Amazon Web Services & Strand Partners, 2024).

Polish SMEs can be categorized into six distinct digital maturity segments: (i) "Uninterested" (33%), meeting only basic requirements and resist change; (ii) "Ambitious without Knowledge" (9%), motivated but lack expertise; (iii) "Benefit Ignorers" (5%), not recognizing the value of digitalization; (iv) "Needing Support" (20%), willing but requiring assistance; (v) "Ready to Act" (13%) with high digital maturity; and (vi) "Digital Champions" (17%), having achieved the highest digitalization levels. This segmentation indicates that 42% of SMEs constitute priority targets for AI adoption programs (PARP, 2023b).

Encouragingly, Poland has shown clear improvements in several areas. The growth rate of SME digitalization in Poland between 2021 and 2023 was six times higher than the EU average, albeit from a low base. This indicates a strong catching-up momentum. Poland also demonstrates notable strengths. Very High-Capacity Network (VHCN) coverage reached 81.1% of households in 2023, surpassing the EU average of 78.8%, while 5G coverage reached 71.9%, showing steady expansion. However, advanced digital technologies remain a relative weakness. Only 3.7% of Polish enterprises have adopted AI (compared with the EU average of 8%), and 19.3% use data analytics (compared with the EU average of 33.2%). The Polish government has acknowledged these gaps. According to the Digital Decade Plan, the national targets are to increase AI adoption to 34% and data analytics usage to 35% by 2030. Achieving these goals

will require a significant acceleration in the adoption of advanced digital tools by SMEs (European Commission, 2024e).

Korea's experience shows what is possible with a concerted effort. Through initiatives such as the Smart Factory program (discussed later), Korea supported tens of thousands of SMEs in adopting sensors, automation, and AI in their production processes. By 2022, more than 30,000 production sites in Korea had been upgraded to "smart factories" equipped with digital systems. This modernization has extended even to mid-tier manufacturers. Importantly, Korea complemented quantitative expansion with a pivot to qualitative improvement after 2020, emphasizing data utilization and advanced applications in SMEs, rather than merely basic automation. As a result, Korean SMEs not only adopt more digital technologies but also use them more effectively. By contrast, Polish SMEs often remain at the entry-level of digitization—e.g., using basic office software or social media for marketing—rather than adopting integrated, data-driven systems. The gap in human capital compounds this challenge. In Poland, only 18% of enterprises provide ICT training to staff, and managers' low propensity to invest in upskilling is frequently cited as a barrier. In summary, Poland's SME sector lags significantly behind the digital frontier compared to countries such as Korea. This creates an urgent challenge: without intervention, Polish SMEs risk losing competitiveness not just to large firms domestically, but to foreign peers that are more digitally enabled.

2.2. Cybersecurity Readiness: Comparative Perspective

Cybersecurity is an integral component of digital transformation; without adequate security, SMEs are vulnerable to disruptions and may hesitate to digitalize further. Both Poland and Korea have established strong cybersecurity legal frameworks and agencies (Poland's Act on National Cybersecurity System aligns with the EU NIS Directive, and agencies such as NASK lead implementation; Korea has multiple laws and the Korea Internet & Security Agency, KISA. However, the on-the-ground cybersecurity readiness of SMEs in both countries reveals gaps, with interesting similarities and differences. A comparative study of SME cybersecurity practices found that, although the difference was marginal, Korean SMEs were more likely to have formal security policies in place—43% in Poland (KPMG Poland, 2024) compared with about 50% in Korea (MSIT & KISIA, 2024). While Poland's approach is based on EU-driven compliance requirements (e.g., GDPR prompting written policies), Korea's adoption rate reflects government-led financial support and policy assistance programs. Regarding dedicated security personnel, both countries show relatively low adoption rates—around 27.1% of Korean SMEs have staff focused on cybersecurity, compared to 16% of Polish SMEs (Kang, 2023; KPMG Poland, 2024). While there is a slight difference, both countries demonstrate that the vast majority of SMEs still lack dedicated cybersecurity staff, often assigning security tasks as additional responsibilities to existing employees due to resource constraints.

In terms of security measures, SMEs in both countries do well on basic practices but struggle with advanced ones. In terms of security measures, both countries show different patterns in basic protections. Polish SMEs implement basic practices such as password policies (86%) and regular software updates (83%) (KPMG Poland 2024), indicating awareness of fundamental cyber hygiene. Korean SMEs, on the other hand, primarily rely on antivirus software (275 out of 550 surveyed) and firewalls/network security (266 out of 550) (KISA, 2023). However, more complex practices are rare in both countries: very few SMEs in either Poland or Korea perform regular risk assessments, and security testing or audits remain uncommon. This points to a common challenge—while basic protective tools are adopted, limited expertise and budget prevent SMEs from undertaking comprehensive cybersecurity management. This points to a common challenge—limited expertise and budget prevent SMEs from undertaking comprehensive cybersecurity management. Interestingly, the cyber incident patterns differ between the two countries: Polish SMEs report a 16% attack rate in a given period (KPMG Poland, 2024), while in Korea, SMEs account for over 80% of all cyber incidents nationwide (Ministry of Science and ICT, 2024; BoanNews, 2024). This could mean Korean SMEs are more digital (hence more exposed to attacks and also perhaps better at detecting/reporting them), whereas some Polish SMEs might be "below the radar" simply because they are not as online yet. In both cases, SMEs express identical needs

for public support on cybersecurity: namely, more training programs for staff, financial subsidies to afford security solutions, and simpler regulatory requirements. They tend to view cybersecurity as complex and burdensome—something that can slow down digital adoption if not addressed. Polish experts have noted that while businesses often see cybersecurity as a regulatory cost, it is essential to reframe it as an enabler for safe digital growth.

Poland has initiated some SME-focused cybersecurity efforts. PARP's online Akademia PARP offers free cybersecurity e-learning for SMEs (covering phishing, secure remote work, GDPR, etc.), helping raise awareness. NASK launched "Firma Bezpieczna Cyfrowo" (Fundamentals of business cybersecurity) in 2022, a program where SMEs self-assess, get a tailored improvement plan, and work toward a cybersecurity certification with provided guidance. These are positive steps, lowering knowledge barriers and incentivizing SMEs to improve security. However, uptake remains limited relative to the sheer number of SMEs. Many micro and small firms in Poland still lack even basic cybersecurity policies or tools, such as VPNs, because they find them too costly or complex without assistance. Korea's approach has been to build regional support infrastructure—it set up regional Information Security Protection Centers that provide local SMEs with consulting, training, and even services such as vulnerability assessments, often free or subsidized. Poland currently lacks an equivalent local outreach mechanism; support is centralized in agencies and online platforms, which may not effectively reach SMEs outside major cities. Another area is certification and standards: Korea introduced a simplified certification regime for SMEs (e.g., a lighter ISMS information security management certification with reduced requirements by 50% for SMEs). Poland, following EU standards, requires certain sectors to implement ISO 27001 or national standards, which many SMEs find daunting. There is room for Poland to explore "right-sizing" cybersecurity standards for SMEs so that compliance is achievable and meaningful.

A critical challenge in Poland is that SMEs often lack incentives or pressure to improve cybersecurity until they experience an incident. Larger companies and multinationals tend to impose security requirements on their supply chains, but given Poland's economic structure, many SMEs are not integrated deeply enough to feel that pressure. Government procurement could serve as a lever: if public tenders required basic cybersecurity measures, SMEs would be more likely to adopt them to qualify for contracts. Korea has experimented with such incentives—for example, by granting SMEs with strong cybersecurity practices easier access to certain contracts. Additionally, technology protection is emerging as a need. Polish SMEs developing innovations—for instance, a startup with an AI tool—face risks of intellectual property theft or cyber espionage. Korea operates technology protection programs (through KISA and other agencies) that help SMEs secure trade secrets and respond to industrial espionage.

Poland's awareness in this area remains nascent. However, as Polish SMEs begin producing more valuable digital products, the need for technology protection will grow.

In summary, both Poland and Korea demonstrate the difficulty of extending robust cybersecurity to the SME sector. Poland's SMEs have partially formalized basic security measures, but they lag in dedicated resources and advanced preparedness. As a result, many Polish SMEs remain vulnerable; for instance, a significant share lack incident response plans or fail to back up critical data, as various studies indicate regularly. Cyber threats such as ransomware could therefore have devastating effects on unprepared firms. The challenge is compounded by low awareness: Many SMEs underestimate cyber risks or assume they are too "small" to be targeted, which is a dangerous misconception in today's digital environment. The Polish government has established a solid legislative framework and agencies in place; however, the implementation gap remains, particularly for micro-enterprises with limited contact with existing programs. Closing this gap will require more proactive outreach and support—a theme reiterated in our recommendations, which draw on Korean practices such as regional security centers, subsidy schemes (e.g., vouchers for cybersecurity tools), and simplified compliance regimes to better integrate SMEs into the national cybersecurity framework.

2.3. Structural Barriers: Fragmentation, Funding, and Skills

Beyond specific technology adoption issues, Poland faces systemic challenges in its support ecosystem that hinder SME digital transformation. The fragmented governance structure, noted earlier, remains a fundamental issue. At present, multiple ministries—such as Economic Development and Technology, Digital Affairs, and Funds and Regional Policy—and their agencies run SME-related programs with digital components. This has created an overlap—for instance, two different agencies might offer duplicative grants for SME IT upgrades—and no single body tracks overall progress. This makes it challenging to evaluate which initiatives are most effective or to ensure that an SME's journey from awareness to implementation is consistently supported. Korea addressed similar multi-agency issues by establishing coordinating committees and enacting laws that assign clear institutional roles—for example, the Korea Basic SME Digitalization Act or the Smart Manufacturing Innovation Act—to institutionalize cooperation. Poland's forthcoming Digital Transformation Program for Enterprises offers an opportunity to establish a stronger coordination mechanism, possibly an inter-ministerial task force or a lead agency with authority to align others. At present, policy fragmentation reduces efficiency—resources are spread thin, and some important tasks fall through the cracks. For example, no agency in Poland currently provides the comprehensive on-site digital advisory services that many SMEs would benefit from. Moreover, frequent political

changes have led to shifting priorities and the rebranding of programs, interrupting continuity.

Fragmentation particularly affects AI adoption initiatives, where responsibilities are dispersed across multiple ministries and agencies without clear coordination. MRiT manages economic policy aspects, while the Ministry of Digital Affairs oversees the development of the AI strategy. NASK addresses cybersecurity dimensions, and NCBR directs R&D funding. Various other agencies handle additional components, all without integrated oversight (Amazon Web Services and Strand Partners, 2024; OECD, 2020). As a result, an SME seeking comprehensive AI implementation support or even basic digital solutions deployment must navigate multiple agencies with different application processes, eligibility criteria, and timelines (European Commission, 2024c). Korea addressed similar challenges by creating the National AI Committee and integrating governance structures to coordinate AI policies across ministries, thereby providing a single point of reference for SMEs seeking AI adoption support (Ministry of Science and ICT, 2024).

Funding constraints present another structural barrier. Polish SMEs heavily rely on EU funds and government subsidies for digital projects; however, these funds, although significant, are not always easily accessible or tailored to meet SME needs. For AI-specific investments, the funding landscape is particularly challenging. Traditional grant programs often demand substantial co-financing (50% or more), which can be prohibitive for AI projects that typically require significant upfront investments with uncertain returns (Amazon Web Services and Strand Partners, 2024). Korea's Data Voucher Program, which supported more than 2,000 projects in 2023, demonstrates an alternative approach. Vouchers cover up to 80% of AI implementation costs, directly paid to certified solution providers, thereby eliminating upfront financial barriers for SMEs (Korea Data Agency, 2023).

The EU's cohesion funds (2021–2027) allocate resources for SME digitalization, but these are often channeled through competitive projects that benefit only a fraction of SMEs. Domestic funding is limited; Poland's public R&D expenditure and innovation grant pool is smaller relative to GDP than in Western Europe. R&D spending accounts for 1.56% of GDP (compared to 3.11% in Germany), leaving less capital available to support cutting-edge SME innovation (OECD, 2025c). Many Polish SMEs, especially micro-enterprises, also struggle to obtain private financing for digital investments. Banks may not lend for "soft" assets such as software or training, and SMEs themselves often have limited collateral or retained earnings to invest. Some countries have introduced dedicated loan guarantee schemes or digital transformation loans; Poland's development bank, BGK, has offered loan programs—for example, a "Technological Credit"—but awareness and uptake by micro-SMEs remain low. As a result, there is a significant financing gap at the smallest firm level.

Additionally, existing grants often require co-financing (e.g., 50%), which can be a barrier for micro-firms that cannot raise even that portion. In comparison, Korea's voucher programs have provided significant direct support—often fully subsidized vouchers up to a limit—to lower financial barriers for SMEs. This difference in approach—between upfront vouchers and reimbursable grants or tax incentives—can be decisive in determining whether a microenterprise undertakes a digital project.

Beyond funding constraints, linkages between large and small enterprises present another structural challenge. Poland's national innovation system lacks strong connections between large corporations and SMEs. The dominance of multinational corporations means local SMEs are often suppliers to foreign companies that may not invest in their digital capacity, while domestic large firms are relatively few and may lack the capacity to support a broad SME base. This dynamic results in weaker technology spillovers from large to small companies in Poland's economy. In countries such as Korea, large corporations often mentor or assist SMEs in their supply chains to digitalize, sometimes incentivized by government-sponsored "win-win" programs. Moreover, collaboration between academia—including universities and technical institutes—and SMEs remains insufficient. Unlike in some countries, where universities operate extension programs or innovation centers that support SME digital projects, such linkages in Poland remain nascent or are limited to EU-funded pilot projects. Regional innovation hubs (such as science parks or the European Digital Innovation Hubs) are promising but require scaling and better integration with national efforts.

Human capital constraints constitute the most critical barrier to digital and AI adoption among Polish SMEs. Poland produces a sizable number of ICT graduates in absolute terms, but many are absorbed by large firms or emigrate to higher-paying markets abroad. Current data shows that only 44.3% of Poles possess basic digital skills compared with the EU average of 55.6% (European Commission, 2024c). At the same time, the shortage of AI specialists is even more acute (Amazon Web Services and Strand Partners, 2024). SMEs report particular difficulty attracting both general technology talent and AI expertise, as many lack the resources to compete with large enterprises for scarce skills. This skills gap necessitates a comprehensive approach, including digital literacy programs for business leaders, technical training for employees, and innovative mechanisms to provide SMEs with access to AI expertise through shared services or consulting programs (Amazon Web Services and Strand Partners, 2024). The challenge is compounded by the fact that only 18% of Polish enterprises provide ICT training to staff (Eurostat, 2025), and managers show low propensity to invest in upskilling (Amazon Web Services and Strand Partners, 2024).

Microenterprises face the greatest challenges in adopting digital and AI technologies. Representing 97% of all Polish enterprises, these firms—typically with fewer than 10

employees—are often family businesses or sole proprietorships with limited capacity to engage with government programs. Language barriers, bureaucratic complexity, and co-funding requirements can deter them from accessing support. Even well-designed programs often fail to reach this "long tail" of the smallest businesses. Microenterprises require highly simplified, turnkey solutions that can be implemented with minimal technical expertise. For general digitalization, this could include ready-to-use e-commerce platforms with minimal setup, basic cloud-based accounting services at near-zero cost, or one-time consultations to establish an online presence. For AI adoption specifically, they require AI-powered business tools integrated into existing software, such as accounting systems with AI analytics capabilities, or customer service platforms with AI chatbots that require no programming knowledge to deploy. Traditional policy tools are often too burdensome for them. For example, they are unlikely to apply for grants that require 30-page applications. The solution lies in low-friction support instruments, such as small vouchers, free tools, or embedding digital solutions onto services they already use, such as banking or accounting platforms. The challenge is to create AI solutions that are sufficiently automated and user-friendly to be adopted by non-technical business owners with minimal support (PARP, 2023b; Amazon Web Services and Strand Partners, 2024).

In conclusion, Poland's current SME digitalization landscape is characterized by low adoption of advanced technologies, significant firm-level barriers, and structural shortcomings in the support ecosystem. By comparison, Korea demonstrates higher SME adoption and a more mature support system, though even Korea faces challenges in encouraging the smallest firms to make additional progress in digitalization and cybersecurity. This comparative perspective highlights areas where Poland should focus its efforts: governance coherence, targeted funding, skills development, and inclusive program design. The next section builds on these insights to propose concrete policy recommendations, many of which draw on Korean models that have proven successful in addressing similar challenges.

3. Policy Implications (Conclusions)

To propel the digital transformation of Polish SMEs, a multifaceted policy package is required—one that strengthens governance, scales up effective support programs, and addresses specific gaps in technology adoption and cybersecurity. The following recommendations are designed as actionable measures for the Polish government, drawing inspiration from Korea's best practices and aligning with Poland's EU commitments. They are grouped into eight key strategic areas:

3.1. Establish an Integrated Governance and Coordination Framework

Poland should break down institutional silos and establish a unified national support system for SME digitalization. It should designate a clear coordinating body or mechanism to align the various ministries and agencies involved in digital transformation programs. One option is to establish an Inter-Ministerial Task Force on SME Digital Transformation, chaired by a high-level authority, such as the Prime Minister's Office or a joint committee of the Ministries of Economic Development and Digital Affairs. This body would oversee strategy implementation, ensure that programs complement rather than duplicate one another, and monitor progress toward the Digital Decade targets. Korea's approach to multi-ministerial collaboration provides a model. For example, its regulatory sandbox framework is coordinated by the Office for Government Policy Coordination, with eight ministries working under a common agenda. Poland could similarly empower a central unit to manage cross-ministry digital initiatives—for instance, by aligning PARP's enterprise programs with NASK's cybersecurity projects and BGK's financing tools.

In practice, this could involve creating a "Digital Transformation Steering Committee" that meets regularly, includes public and private stakeholders (e.g., chambers of commerce, SME associations), and reports annually on outcomes. Additionally, Poland should consider enacting a supportive legal framework— similar to Korea's statutes for SME digitalization—that mandates cooperation and ensures long-term policy continuity beyond political cycles. A law or government resolution could formalize roles—for example, designating MRiT as the lead on enterprise digital uptake and the Ministry of Digital Affairs as the lead on infrastructure and skills—with data-sharing agreements between agencies to track SME progress. A unified online portal for SME support should be developed, consolidating all digital transformation programs listed in one place. This portal could serve as the front end of an integrated system, providing SMEs with a one-

stop shop for information and applications across various support schemes.

Stronger coordination would also facilitate monitoring and evaluation. It is recommended to establish a national SME digitalization observatory—an annual survey or index to measure SME digital readiness, technology uptake, and satisfaction with support programs. This evidence base would help fine-tune policies. In line with the Digitalization Strategy 2035's call, Poland should launch a regular "SME Digital Transformation Barometer" by 2026. The coordinating body could use these data to identify lagging sectors or regions and adjust resource allocation accordingly.

3.2. Launch a National "Smart Factory" Program for Manufacturing SMEs

Poland should accelerate digital transformation in Poland's manufacturing sector by creating a dedicated Smart Factory initiative, modeled on Korea's highly successful program. Manufacturing is the backbone of Poland's economy (accounting for about 25% of SMEs and a large share of exports), yet productivity remains low, and automation levels are modest. Korea's experience demonstrates that a well-funded, targeted program can modernize thousands of SMEs. Since 2014, Korea's Smart Factory initiative has transformed more than 30,000 factories by equipping them with sensors, IoT devices, data analytics, and automation systems. Poland should aim to similarly upgrade its SMEs with Industry 4.0 technologies over the next decade.

Key components of a Polish Smart Factory program would include:

1) National Roadmap and Targets: Develop a Smart Manufacturing Roadmap 2030 that sets clear milestones—for example, the number of SMEs to reach "Industry 4.0 ready" status by 2027 and 2030. The government could, for instance, target 5,000 manufacturing SMEs to implement advanced automation and AI solutions by 2030. Responsibilities should be assigned across ministries (e.g., MRiT, the Ministry of Higher Education & Science, and the Ministry of Education) for related R&D and skills development, and industry bodies should be involved in co-writing this roadmap. Crucially, the program should be anchored with a legal or regulatory mandate to ensure continuity, similar to Korea's Smart Manufacturing Innovation Promotion Act of 2023, which provided a legal basis and accountability for its program.
2) Tiered Support by Maturity Level: Not all factories are starting from the same point. A tiered support scheme should be implemented to meet firms where they are. Basic-level firms with little automation could support small grants or equipment vouchers for first steps, such as sensor installation or digital quality control tools. For intermediate firms (some automation, no integration), co-funding could support more integrated systems such as ERPs, manufacturing

execution systems (MES), or IoT networks on the shop floor. For advanced firms ready to pioneer, could support larger grants or public-private co-investment for cutting-edge projects—e.g., AI-driven production optimization, digital twin simulations, or robotics—potentially creating a few "lighthouse" smart factories as demonstrators. This graduated model would ensure efficient use of funds by pushing each SME to the next level of digitalization without relying on one-size-fits-all subsidies.

3) On-site Consulting and Skills Training: Financial support should be paired with expert consulting services to maximize impact. Poland could fund a cadre of "industrial digital transformation coordinators"—independent experts or certified firms—to visit SMEs, diagnose their production processes, and recommend tailored digital solutions. This approach echoes the coordinator system in Korea's programs and could be integrated with PARP's advisory offerings. Providing three to five days of free consultancy per factory would help SMEs plan effective investments. Simultaneously, investments should be made in workforce upskilling: partner with technical universities, vocational schools, and private training centers to offer short courses in smart manufacturing—such as industrial IT, robotics maintenance, and data analytics for production. EU funds, such as the European Social Fund+, could be leveraged to finance training vouchers for SME employees. The goal should be to train thousands of workers and managers in new digital tools to ensure the sustainable adoption of technology.
4) Develop Domestic Solution Providers: The program should not only upgrade factories but also foster the growth of Poland's local technology ecosystem. Part of the budget should be allocated to support Polish providers of automation equipment, industrial software, sensors, and related technologies. This could be achieved through R&D grants for SMEs developing Industry 4.0 solutions, tax incentives for larger firms to partner with local suppliers, and a certification program for quality solution providers—as Korea did, increasing its certified smart factory vendors from 299 in 2016 to 1,969 by 2022. Creating testbeds or innovation hubs in collaboration with research institutes, where providers and manufacturers can trial new solutions, would foster collaboration. For example, "Smart Manufacturing Innovation Centers" could be established in industrial regions (perhaps by building on existing technology parks) where SMEs can witness demonstrations of digital technology and receive hands-on support. While European Digital Innovation Hubs (EDIHs) were originally designed to cover part of this support, it is essential that the program simultaneously reinforce domestic providers and embed them within these structures to secure long-term local capacity. By boosting domestic suppliers, Poland would ensure that resources spent on smart factories also strengthen local industry and expertise.

With these elements, a Polish Smart Factory program could significantly enhance productivity. The initiative should be sizable. Korea scaled up to supporting approximately 4,000 factories per year at peak; Poland might aim for a few hundred per year initially, scaling to more than 1,000 as capacity grows. Funding could come from a mix of national budget—for example, via MRiT and national recovery funds—and EU structural funds earmarked for digitalization. Importantly, this program aligns with EU industrial policy goals—specifically the Digital Decade's aim to increase advanced technology adoption in SMEs—and should therefore be able to attract EU co-financing. By 2030, if implemented, Poland could see a transformation: SMEs equipped with real-time production data, predictive maintenance to reduce downtime, and agile manufacturing capable of delivering higher-quality outputs. In turn, this would contribute to closing Poland's productivity gap in manufacturing and to creating high-skilled jobs in both manufacturing and technology sectors.

3.3. Implement a "Smart Service" Voucher Scheme for Service-Sector SMEs

While manufacturing often receives greater attention, service-sector SMEs—from retail and tourism to logistics and professional services—are equally in need of digital upgrades. It is recommended that Poland introduce a Smart Service Support Program modeled on Korea's initiative, launched in 2025. The program would provide vouchers or matching grants directly to SMEs to adopt digital solutions—such as e-commerce systems, customer relationship management software, AI chatbots, or other ICT-based "smart services" — coupled with expert guidance. This would address the two primary barriers for service SMEs: lack of funding and lack of expertise.

Key Features of the Smart Service Voucher Scheme

1) Consortium-Based Applications: Each project should be a joint effort between an SME (the end user) and a technology solution provider. In practice, an SME would identify a digital solution it needs—for example, a data analytics system for a marketing firm or an inventory management system for a retailer—and partners with a vetted IT firm or software vendor to implement it. The SME and provider would then apply together for the voucher. This approach ensures the SME has a committed technology partner and a clear plan from the outset. It mirrors Poland's existing mechanisms under PFR—such as PFR Ventures and programs supported by the European Funds for a Modern Economy (FENG)—which channel capital into technology companies and often incentivize SME–provider collaboration, as well as Korea's model where consortium applications were mandatory. This ensures that the support is demand-driven (SMEs choose

what they need) but also guided by technological expertise.

2) Pre-Approved Provider Pool: A national registry of certified digital solution providers should be established from which SMEs can select partners. Korea's program required providers to register in a Smart Service provider pool in advance (Ministry of SMEs and Startups, 2025). Poland should adopt similar vetting criteria: for example, providers would be required to demonstrate technical capacity, quality references, data security standards, and GDPR compliance. Eligible providers could include software developers, cloud service providers, system integrators, digital marketing agencies, and other relevant organizations. This vetted pool would give SMEs confidence in the vendors and protect against unreliable operators. It would also streamline the application process, as vendors would not need to be evaluated each time if already certified. An online directory of certified providers should be maintained to ensure transparency. As a complementary action, Poland could build on its EDIHs to recruit top providers across regions, ensuring that even small towns have access to local IT companies in the pool.
3) Voucher-Based Co-Funding: Use a voucher mechanism to fund projects, which is simpler and SME-friendly. For instance, offer to cover 50% of the project cost up to a certain cap (similar to Korea's 50% matching approach). Based on Korea's scale, Poland could set caps, such as approximately EUR 35,000 for a single SME project (roughly equivalent to KRW 50 million) and higher (approximately EUR 150,000) for multi-SME consortium projects. The voucher means the SME does not need to pay the full cost upfront and then wait for reimbursement; instead, the government covers its share directly when the SME procures the service. This encourages participation and is compliant with EU procurement rules since SMEs choose providers in a competitive market. The government's payment can go either to the SME or directly to the provider as reimbursement—in either case, it lowers the SME's financial barrier to invest. We suggest designing the scheme such that even micro-firms can access it (possibly with a higher subsidy rate for the smallest firms or a lower required co-finance for micro enterprises).
4) Integration with Advisory Services: To ensure SMEs make good use of the voucher, integrate the scheme with digital advisory programs. For example, an SME that has undergone a free digital readiness assessment (through an EDIH or a consultant) could get extra points or priority in voucher selection. This incentivizes SMEs to seek advice first, resulting in more mature project proposals that truly meet their needs. Poland's EDIH program can be leveraged—EDIHs could act as outreach and initial assessment channels, referring prepared SMEs to the voucher scheme. The program can thus create a pipeline: awareness → assessment → voucher funding → implementation, with minimal gaps in between.

5) Administration and Scale: Task a national agency with managing the program—PARP is a natural fit given its experience, potentially in collaboration with industry associations. The scheme should align with funding from the EU's programs, such as FENG or the Recovery Fund, as those have allocations for SME digital uptake. A realistic pilot could support a few hundred projects in the first year (ensuring processes are smooth), scaling up thereafter. Korea in 2025 funded ~110 single-company projects and eight consortium projects for new digital services, as well as 25 enhancement projects. Poland could target similar numbers initially and grow if demand is strong. Rigorous monitoring (perhaps with random audits by independent firms) should be instituted to prevent misuse and ensure deliverables are met. Over time, this voucher scheme can significantly increase the scale and speed of SME digital adoption in services by lowering cost hurdles and letting SMEs choose solutions that fit them.

In essence, the Smart Service voucher program would be a flexible tool to inject resources and expertise into SMEs. A small retailer could, for example, get a EUR 10k voucher to set up an e-commerce and inventory management system with a local IT firm, paying only half the cost. A group of tourism SMEs could jointly implement a digital booking and marketing platform with a bigger voucher. By combining funding with a curated ecosystem of providers and consultants, the program mitigates risk for SMEs and drives a culture of digital innovation in the service sector. It would also stimulate Poland's digital solutions market—providers have motivation to innovate and tailor products for SMEs (knowing there is a pool of subsidies to help clients pay). This can create a virtuous cycle, as seen in Korea, where such programs helped data and solution providers flourish alongside uptake.

3.4. Expand Data and AI Voucher Programs to Spur Technology Adoption

To specifically accelerate the adoption of data-driven innovation and artificial intelligence among SMEs, Poland should implement dedicated Data Voucher and AI Voucher programs. These would be modeled on Korea's pioneering schemes that have demonstrated impressive results in recent years. The idea is straightforward: provide SMEs with cash-equivalent vouchers to obtain data sets, data analytics services, or AI solutions from approved providers, thereby addressing the cost and resource barriers that prevent SMEs from leveraging data and AI.

Data Voucher Program

This program would support SMEs in procuring data or data services. In Korea, since 2019, the Data Voucher program (run by K-DATA under the Ministry of Science and ICT) offers vouchers up to KRW 60 million (approximately EUR 40,000) per SME for purchasing datasets or data processing services. The program connects data "consumers" (SMEs needing data insights) with data "suppliers" (companies that have data or can analyze data). Poland can create a similar mechanism under a body such as PARP, focusing on key data needs of SMEs— with a focus on addressing the critical data needs of SMEs—for example, providing market intelligence for small manufacturers, customer analytics for retail businesses, or geospatial data to support logistics firms. By subsidizing the cost of acquiring high-quality data or hiring data analysts, SMEs can innovate their products and business models. For instance, a startup could utilize data to train an AI model, or a small healthcare company could conduct comprehensive big data analysis on patient trends.

Korea's program had three tracks: purchasing data (for companies that need data sets/APIs), general data processing (for basic analytics services), and AI-specific processing (for advanced AI use cases). Poland can adopt a similar multi-track approach to cover different needs, ensuring even non-tech SMEs can benefit (some may need a market research dataset) while also encouraging advanced projects (AI model development). The program should involve a process where SMEs apply with a defined data need, a committee evaluates and approves support, and then matches them with qualified data providers or experts, with transparency and quality control overseen by a coordinating agency. A key success factor from Korea was having a specialized agency (K-DATA) orchestrating this ecosystem—coordinating suppliers, ensuring standards, and measuring outcomes. Poland might consider empowering an existing entity or creating a small "Data Initiative Office" to perform this role.

Korea's experience demonstrates the program's potential impact. From 2019 to 2023, applications for data vouchers increased significantly (from 2,795 to 7,376 annually) and supported projects expanded to over 2,000 per year. Participating companies saw significant benefits: the combined revenue of those firms increased from KRW 330 billion in 2019 to KRW 12,636 billion in 2023, indicating that leveraging data had a direct economic payoff. The program also created nearly 29,000 new jobs and fostered a culture where companies that started as data consumers evolved to become data providers themselves, fueling a virtuous data cycle. Poland could achieve similar results by implementing its own data voucher program to stimulate its currently underdeveloped data market. Many Polish SMEs have data (like production data, sales data) but do not utilize it; others could improve operations or marketing if they had external data. With vouchers, a manufacturing SME could, for example, access sensor data analytics to optimize energy use, or a tourism SME might purchase mobility data to

understand tourist flows. The program also aligns with the EU's data strategy and could draw on sources such as European data spaces.

AI Voucher Program

Building on data vouchers, an AI-focused voucher would specifically help SMEs adopt AI solutions. Korea introduced an AI Voucher program in 2020, which by 2023 had supported over 1,500 companies in implementing AI across various industries. Poland's target in Digitalization Strategy 2035—to raise AI adoption from 5.9% in 2024 to 50% of companies by 2035—is very ambitious and likely unreachable without direct support. An AI voucher scheme can be a game-changer. It would work similarly: an SME identifies an AI use-case (such as predictive maintenance, customer service chatbot, or AI-based quality inspection), partners with an AI solution provider or developer, and applies for a voucher to cover a substantial portion of the project cost. Given that AI projects can be expensive, vouchers might be up to, e.g., EUR 50,000 or more per project, possibly with different tiers for simple vs. complex AI solutions.

The program should ensure that SMEs have access not only to funding but also to expert mentorship. In Korea, the success of vouchers was underpinned by robust support infrastructure (with K-DATA and the Ministry of ICT providing technical guidelines, maintaining a marketplace of AI solutions, etc.). Poland can collaborate with universities or AI institutes to create a panel of AI experts who can help SMEs scope their projects properly. The voucher could even cover some hours of consulting to design the AI solution before implementation. Additionally, Poland could leverage existing EU AI initiatives (such as the AI Testing and Experimentation Facilities or Horizon Europe projects) to complement national vouchers with expertise and tools.

Strategic Impact and Implementation

By implementing data and AI vouchers, Poland will directly address the financial and capability barriers holding back SMEs from these advanced areas. Many SMEs may be interested in AI—for example, using it for demand forecasting or automating a process—but assume it is out of reach. Vouchers send a signal that the government will share the risk and cost. Over a few years, this could lead to hundreds of SMEs actually piloting AI—creating local case studies that inspire others. It will also nurture a domestic AI service industry, as providers see increased demand from SMEs, similar to how Korea's program catalyzed a broader data ecosystem.

Poland's program should be coordinated with EU efforts—for instance, ensuring that any solutions developed align with EU guidelines on trustworthy AI, including ethics—and possibly co-financed with EU digital programs where applicable. Considering Poland's emphasis on human-centric and sustainable AI in its strategy, vouchers can be directed to projects that also have social or environmental benefits,

such as AI for energy efficiency and healthcare.

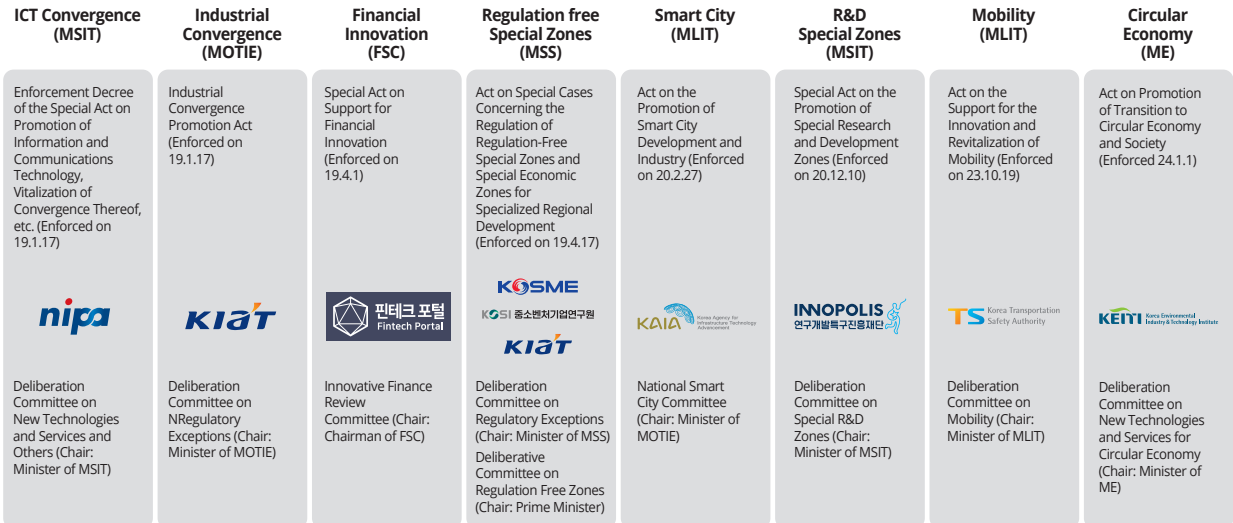
In summary, Data and AI vouchers are high-impact, relatively low-bureaucracy tools to infuse cutting-edge tech into the SME sector. The Korean case demonstrates their efficacy not only in bridging the gap but also in creating self-sustaining momentum within the digital ecosystem. Poland should adopt and adapt this model swiftly, focusing on local needs and ensuring inclusive access—such as reserving a quota or simplified process for small towns or less digitally mature regions to avoid only tech-savvy SMEs applying. This will help Poland's SMEs move from being digital laggards to fast followers in data and AI use.

3.5. Adopt Regulatory Sandboxes for Innovation in Emerging Technologies

Encouraging innovation often means allowing businesses to experiment with new technologies without being stifled by outdated or rigid regulations. Poland has so far used regulatory sandboxes in a limited way (primarily in the fintech or financial innovation sector under EU frameworks). It is recommended to expand the regulatory sandbox model to include AI, ICT convergence, industrial convergence, and smart cities, drawing on Korea's comprehensive, multi-sector approach that has demonstrated significant policy effectiveness. This expansion is particularly urgent, given the EU AI Act's requirement for member states to establish AI regulatory sandboxes by August 2026, as well as Poland's broader digital transformation goals.

A regulatory sandbox provides a controlled environment where companies (including startups and SMEs) can pilot innovative products or services under relaxed regulatory requirements or temporary legal exemptions, with oversight, before full legislation catches up. For Poland's SMEs, this approach addresses both general digitalization challenges (such as testing IoT sensor networks, automated production systems, or smart city data platforms) and AI-specific regulatory uncertainties under the new EU AI Act framework.

Figure 5.
Domains, Managing Ministries and Agencies of Regulatory Sandboxes



Note: MSIT (Ministry of Science and ICT), MOTIE (Ministry of Trade, Industry and Energy), FSC (Financial Services Commission), MSS (Ministry of SMEs and Startups), MLIT (Ministry of Land, Infrastructure and Transport), ME (Ministry of Environment)

Source: Regulatory Reform Committee (2024).

Korea's Comprehensive Sandbox System

Korea's Regulatory Sandbox System, operational since 2019, represents a coordinated multi-ministerial approach spanning eight domains: ICT Convergence (MSIT) covering AI and data applications; Industrial Convergence (MOTIE) for smart manufacturing and automation; Financial Innovation (FSC) for fintech solutions; Regulation-Free Zones (MSS); Smart Cities (MOLIT) for urban digital infrastructure; R&D Special Zones (MSIT); and Mobility Innovation (MOLIT) for autonomous systems. Performance metrics demonstrate substantial policy impact across all technology domains: 1,139 total projects approved with an 85% approval rate, with particularly strong results in AI applications (200+ projects achieving over 70% commercialization success) and industrial automation systems (Regulatory Reform Committee, 2024).

The Korean system offers three main tracks: pilot exemptions (Regulatory Special Cases) to test new technologies in ambiguous legal areas, expedited confirmations of regulatory status, and temporary permits for market entry of novel products under certain conditions. Crucially, Korea built in safeguards (e.g., mandatory insurance, clauses to revoke exemptions if risks emerge) to protect public safety while fostering innovation. These projects span a wide range of digital applications: new mobility services, smart manufacturing systems, healthcare AI applications, IoT-based urban solutions, and green technology innovations, with many led by SMEs.

Poland's Strategic Sandbox Design

For Poland, broadening sandbox use could have immediate benefits across multiple technology domains. In general digitalization, sandboxes could enable SMEs to test IoT sensor networks for predictive maintenance, implement fully automated production lines that do not fit current labor regulations, or deploy smart city data-sharing systems under temporary privacy exemptions. For AI specifically, sandboxes could allow SMEs to deploy AI solutions currently constrained by regulations—such as AI diagnostic tools in telemedicine, autonomous drones for logistics, or AI-powered quality control systems in manufacturing—under supervision while gathering evidence of safety and efficacy for regulators.

Poland's Digitalization Strategy acknowledges this need, noting that "regulatory sandboxes in Poland are limited to fintech... going forward, scope should be broadened to AI and smart manufacturing." This expansion aligns with both EU AI Act requirements and national development priorities (AI, Industry 4.0, cybersecurity, smart cities).

Addressing SME-Specific Challenges Through a Tiered Approach

Poland's regulatory sandbox design must address the unique challenges Polish SMEs face in innovation sharing and regulatory experimentation. Polish SMEs often express concerns about exposing proprietary information and trade secrets when participating in national-level programs alongside larger competitors. Many operate in specialized regional clusters with established business relationships and prefer familiar environments for initial experimentation. A tiered approach allows companies to begin testing digital and AI innovations in comfortable regional settings where trust networks are stronger and competitive pressures are reduced, before progressing to sectoral or national-level demonstrations.

3-Tier Sandbox Structure

Based on these considerations, Poland should establish a comprehensive 3-Tier Sandbox Structure addressing different scales and risk levels of digital innovation:

Tier 1: The National Digital Innovation Sandbox, under the direct operation of KRiBSI, would handle high-risk AI systems in healthcare, finance, and education, as required by the EU AI Act. It would also oversee large-scale digital infrastructure projects exceeding EUR 1M, national strategic technology development, and contribute to EU standard-setting. This tier focuses on technologies with national significance and regulatory complexity.

Tier 2: Sectoral Sandboxes with sector-specific operations would include Manufacturing 4.0 (covering both AI and general automation) with Ministry of Industry cooperation, Healthcare Digital Innovation (including AI diagnostics and telemedicine) with Ministry of Health cooperation, Fintech and Digital Financial Services with KNF cooperation, AgTech

and Smart Agriculture (IoT sensors, AI crop monitoring) with Ministry of Agriculture cooperation, and Smart Education Technologies with Ministry of Education cooperation.

Tier 3: Regional Sandboxes would establish technology hubs in major Polish cities: Warsaw Digital Innovation Hub as a comprehensive platform for all emerging technologies, Kraków Tech Valley focused on R&D and AI development, Gdańsk Maritime Innovation Hub for maritime digitalization and AI, Wrocław Industry 4.0 Center for smart manufacturing, and Poznań PIAST Center for AI infrastructure and digital services. These regional sandboxes enable local SMEs to experiment with both general digital tools and AI applications in familiar environments.

SME-Specialized Programs

To ensure accessibility for smaller companies, the sandbox system should include an SME Fast Track Program targeting companies with 50 or fewer employees and revenue under EUR 10M. Special benefits would include rapid review processes (reducing processing time from 6 months to 3 months), high support rates (80% demonstration cost support compared to the general 50%), dedicated mentors with 1:1 consultant assignment, legal support through free digital and AI legal consultation, and EU linkage support for market entry in other member states.

Operation procedures should follow four streamlined stages. Stage 1 involves submitting an Application over a period of one month, which includes a business plan, technical specification, regulatory conflict analysis, and a demonstration plan and safety review. Stage 2 covers Review and Evaluation over 2 to 3 months, including document review of technology, business viability, and social value, presentation review with committee face-to-face evaluation, and related ministry consultations. Stage 3 handles Approval and Agreement over a period of one month, including conditional approval decisions, demonstration agreement conclusions, and the establishment of a monitoring plan. Stage 4 encompasses Demonstration and Follow-up over 2 years, including quarterly progress reports, mid-term evaluation and consulting, and final performance evaluation.

AI Compliance Learning Sandbox

An AI Compliance Learning Sandbox should be established with the purpose of regulatory compliance learning for existing enterprises' AI adoption. This specialized program would include a stepwise learning process, comprising four levels: Level 1, covering GDPR basics and AI Ethics (2 weeks); Level 2, focusing on understanding and requirements of the AI Act (4 weeks); Level 3, addressing sector-specific AI regulations (4 weeks); and Level 4, involving practical application and testing (6 weeks).

The program would include risk simulation components such as mock regulatory environment testing, potential legal risk assessment, compliance cost prediction, and

best practices development. This addresses the significant regulatory burden that Polish SMEs face under the EU AI Act, where compliance costs can range from EUR 150,000 to EUR 400,000 annually for manufacturing SMEs and from EUR 110,000 to EUR 230,000 for service SMEs.

Implementation Framework

To implement this comprehensive sandbox system:

Create Legal Provisions: Enact or amend legislation to empower relevant ministries to grant time-limited regulatory exemptions or no-enforcement assurances for sandbox participants. This could be a horizontal "Innovation Sandbox Act" or sector-specific amendments. The law should outline the process, eligibility (likely innovative products that offer societal or economic benefit but face regulatory hurdles), and safeguards (e.g., participant must inform consumers of sandbox status, carry insurance, etc., similar to Korea's approach).

Coordination Unit: Given multiple sectors, a coordination unit (perhaps in the Prime Minister's Office) could manage the overall sandbox program, while sectoral ministries handle domain-specific applications. For instance, the Ministry of Digital Affairs might lead an AI sandbox with NASK or another agency providing technical evaluation, the Ministry of Economy might lead an industry sandbox with support from technical institutes, etc. Regular meetings of these bodies can ensure consistency and share lessons.

Outreach and Participation: Encourage SMEs and startups to apply by running calls for sandbox proposals. Work with industry clusters and tech hubs to identify innovative ideas hindered by regulations. Ensure that sandbox opportunities are well-publicized among the entrepreneur community. It might also help to offer government support to sandbox participants, such as advisory on regulatory compliance or even small grants to conduct the pilot (Korea often combined sandbox with other supports).

Use Sandbox Results to Reform Regulations: The ultimate goal is not to create sandboxes for their own sake, but to update laws. Institute a feedback mechanism: each sandbox project should produce a report on outcomes, which a regulatory committee reviews. If successful, regulators should draft amendments to make the exemption permanent, thereby scaling innovation into the mainstream. This way, sandboxes become a path to agile regulatory reform, ensuring Poland's legal environment keeps pace with technology. Korea has revised numerous laws after sandbox trials proved new concepts to be safe and beneficial. Poland can do the same, for instance, updating fintech rules, medical device approvals for AI, or mobility laws for autonomous vehicles, as sandbox pilots yield evidence.

Innovation Ecosystem Support Infrastructure

The sandbox system requires a robust institutional infrastructure, including a KRiBSI Sandbox Center in Warsaw, which provides central review and approval, national network coordination, EU sandbox linkage, and policy improvement feedback. Regional Demonstration Centers in five major cities should offer on-site support and mentoring, regional specialized expertise, local partnership building, and demonstration infrastructure for both digital and AI technologies.

Collaboration networks should establish multi-party cooperation systems, including university research institutes for technical consultation, law firms and consulting companies for legal support, VC and investment institutions for funding linkage, global enterprises for mentoring opportunities, and EU partners for cross-border market access.

The sandbox approach aligns well with EU innovation principles and can be done within EU law (the EU itself encourages sandboxes in areas such as AI under its forthcoming AI Act). By moving early, Poland can become a testbed for innovation in Eastern Europe, possibly attracting investments. Over time, a track record of sandbox projects will also signal to entrepreneurs that Poland is open for innovation.

In terms of metrics, Poland might aim to approve a certain number of sandbox experiments each year in various domains—even 10-20 meaningful projects annually could have ripple effects. These could include, for example, a few AI healthcare pilots, some advanced manufacturing process trials, and a couple of smart city data-sharing initiatives with privacy sandboxing, among others. This low-cost policy (it is more about regulatory flexibility than money) could unlock high-value innovations and give Polish SMEs a chance to pioneer new solutions rather than waiting for laws to change elsewhere.

This comprehensive regulatory sandbox framework positions Poland to exceed EU AI Act requirements while creating competitive advantages in Eastern Europe. By 2027, Poland could become the region's leading destination for testing digital and AI innovations, attracting both domestic SMEs and international companies seeking regulatory-friendly environments for breakthrough technologies.

3.6. Strengthen SME Cybersecurity Support and Simplified Compliance

To address the cybersecurity challenges identified, Poland should implement a dedicated package of measures to enhance cybersecurity for SMEs, learning from Korea’s multi-layered support system. Key recommendations in this domain include establishing regional cybersecurity centers, simplifying certification processes for SMEs, promoting security services, and protecting SME innovations:

1) **Regional Cybersecurity Support Centers:** Local Information Security Centers should be established across Poland's regions to provide hands-on assistance to SMEs. For example, Korea's KISA operates regional centers that deliver services such as security check-ups, on-site consulting, incident response support, and training workshops for local businesses. Poland could establish similar centers, perhaps within existing structures, such as voivodeship development agencies or in partnership with technical universities in each region. These centers should employ cybersecurity experts on staff (or have them available on call) who can visit SMEs or host consultations for them. Services could include vulnerability assessments of company IT systems, guidance on basic protections—such as firewalls and anti-malware—assistance in drafting security policies, and emergency response support in case of breaches. By being geographically accessible, these centers would lower the threshold for SMEs—a small firm in Podkarpackie could obtain support without needing to hire expensive consultants in Warsaw. Initially, a few centers could be piloted—for example, in five regions with high SME concentration—and then expand nationwide. Funding could come from a mix of national budget and EU funds—for example, the EU Digital Europe Program, which supports cybersecurity capacity building, could be tapped. Each center could also serve as a hub for awareness campaigns, organizing local seminars or "cyber hygiene" clinics for SMEs. Such efforts would not only improve SME defenses but also foster a community where businesses can share experiences and solutions. Ultimately, this network of centers would embed cybersecurity into the broader SME support infrastructure in Poland.
2) **Simplified Certification and Standards:** Cybersecurity compliance for SMEs should be simplified through staged or scaled-down certification frameworks. Many Polish SMEs are overwhelmed by comprehensive standards such as ISO/IEC 27001. Korea addressed this challenge by offering a lightweight version of its Information Security Management System (ISMS) requirements for SMEs, effectively reducing requirements by 50% for small businesses. Poland could work within EU frameworks—such as adapting the EU's upcoming cybersecurity certification schemes to include SME-friendly tiers—or create a national tiered standard. For example, a "Fundamentals of business cybersecurity" certification could require a manageable set of 10–15 key controls—such as regular backups, access controls, and an incident plan—while an "Advanced Secure SME" certification could align with more rigorous standards. Providing a clear pathway—such as bronze, silver, and gold levels—would encourage SMEs to reach at least the bronze level, which covers essential protections. The government could assist by providing templates, self-assessment tools, and subsidized audits for SMEs seeking certification. Simplified certification would help in two ways: it would provide

SMEs with a concrete target and guidance, and it would create trust marks that SMEs can display to partners or customers. It would also reduce the burden on small firms, where not all controls are applicable. Korea found that clarifying and reducing requirements increased SME participation in certification. Poland could coordinate this with European standards, ensuring that the simplified route still maps to core requirements of the NIS2 Directive for small operators of essential services, where relevant. Additionally, timeline flexibility—such as granting SMEs longer grace periods to comply with new regulations or allowing phased implementation—could be part of this simplification.

3) **"Security-as-a-Service" and Turnkey Solutions:** To lower implementation barriers, cloud-based security solutions and turnkey cybersecurity packages should be promoted for SMEs. Many SMEs cannot afford an in-house security infrastructure or dedicated teams. However, affordable cloud security services are available today—for example, managed firewalls, intrusion detection systems, and secure email gateways. The government could negotiate with providers to create SME-specific plans or vouchers for these services. For example, an SME could obtain a year of managed security services at half the normal price through a government subsidy. Security-as-a-service models allow SMEs to access professional-level security tools maintained by experts, without needing to manage them directly—a practice commonly used in Korea's approach to supporting SMEs. The government could also support the development of turnkey security packages—essentially preconfigured sets of hardware and software for, for example, a secure SME network, or a secure remote work setup, that can be deployed easily. This might involve partnering with IT companies to bundle antivirus, firewalls, VPN, and backup solutions with a simple installer and support line, offered at a discount for SMEs. By simplifying adoption—such as through a one-stop "SME cybersecurity kit"—even non-technical business owners could implement baseline protections.

4) **Technology Protection Mechanisms:** Measures should be implemented to protect SME innovations and sensitive technologies from theft or unfair exploitation. SMEs often fear that investing in innovation—such as AI algorithms, new designs, trade secrets—could be undermined if larger players or foreign actors appropriate their ideas. Korea has developed comprehensive technology protection frameworks, including legal support for SMEs in IP disputes, systems for registering critical technologies, and an industrial security consulting program. Poland should strengthen its support in this area—for example, by expanding the Patent Office or innovation agency programs to help SMEs patent their inventions or secure trade secrets. A rapid response team or hotline should also be established for SMEs that suspect cyber-espionage or IP theft, linking law enforcement, CERT

Polska, and legal advisors.

5) **Preventing Unfair IP Terms:** Policies should be considered to prevent large contractors from imposing unfair terms that claim IP from SME suppliers, which discourages SME innovation. Technology protection will become increasingly important as Polish SMEs advance up the value chain. Government-backed cyber insurance or indemnification for SME innovations could also be explored, to give firms confidence that if they invest in new technologies, they would have recourse in case of theft or breach.
6) **Incentives for Compliance:** Economic incentives should be created to encourage SMEs to improve cybersecurity. One approach is to integrate cybersecurity into public procurement criteria—for example, by awarding preference or additional points to bidders that hold a certain cybersecurity certification, either as a tiebreaker or small score in tenders. In this way, investing in security could help SMEs win contracts, transforming security from cost to an advantage. Another incentive could be tax credits for expenditures on cybersecurity hardware, software, or training for SMEs. This could be modeled on R&D tax credits but focused specifically on security investments. Such measures would reduce the effective cost and signal government support. Korea has used procurement and performance evaluations to incentivize larger firms to support SMEs—for example, giving credit to large companies that mentor SMEs in security. Poland could adapt that by making security a component of supplier evaluations. Additionally, insurance premium discounts could be considered, encouraging insurers to offer lower cybersecurity insurance premiums to SMEs that have taken recommended steps, much like safe driving leads to lower car insurance premiums. The government could partner with insurance associations to develop a scheme under which an SME with "Cyber Secure SME" certification receives a fixed percentage discount on cyber insurance premiums—a mutually beneficial arrangement, as it reduces risk for insurers too.

By implementing this set of actions, Poland would move toward a "culture of cybersecurity" among SMEs, where security is viewed not as a daunting burden but as an achievable and supported aspect of doing business. The ultimate goal is to substantially increase the number of SMEs with at least basic cybersecurity measures and to reduce the incidence of cyberattacks. If hundreds of SMEs receive direct support from regional centers each year, thousands utilize subsidized security services, and a growing number earn simplified certifications, the overall resilience of the SME sector would increase. This, in turn, would fortify Poland's digital economy, as cyberattacks often exploit the weakest links—typically small firms—thereby raising the baseline protection of supply chains and customer data nationwide.

3.7. Foster Industry–Academic Partnerships and Regional Innovation Hubs

Strengthening the ecosystem around SMEs is critical for sustainable digital transformation. Poland should invest in closer collaboration between industry—particularly SMEs—and academic and research institutions, while also bolstering regional innovation hubs that can diffuse knowledge and technology. Special emphasis should be placed on AI research collaboration and knowledge-transfer mechanisms. Korea's innovation success has been partly due to strong links between universities, research institutes, and businesses, as well as deliberate efforts to build regional innovation clusters —for example, Daegu's robotics cluster. Key actions for Poland include:

1) **Digital Innovation Hubs (DIHs) and Living Labs:** The network of European Digital Innovation Hubs in Poland should be expanded and strengthened, ensuring they have the capacity to serve more SMEs and cover all regions. These hubs provide test-before-invest facilities, training, and matchmaking services. Poland should support DIHs in acquiring the latest technologies—for example, small-scale Industry 4.0 demo lines, AI computing resources, including GPU clusters for machine learning, AI development environments, and specialized AI testing labs and cybersecurity labs—that SMEs can utilize. Additionally, the creation of Living Labs or sandboxes at the regional level should be encouraged, tailored to local industry strengths—for example, a fintech AI lab in Warsaw focusing on algorithmic trading and credit scoring, a healthcare AI lab in Kraków for medical imaging and diagnostics, an industrial AI lab in Wrocław for predictive maintenance and quality control, and an agricultural AI lab in Poznań for precision farming and crop monitoring. Poland should support DIHs to acquire the latest technologies—such as small-scale Industry 4.0 demo lines, AI computing resources, and cybersecurity labs—that SMEs can use.
2) **Living Labs and Regional Sandboxes:** The creation of Living Labs or sandboxes at the regional level should be encouraged, tailored to local industry strengths—for example, a fintech lab in Warsaw, a green energy tech lab in Gdańsk, an agricultural technology lab in Poznań. These labs, often hosted by universities or city authorities, enable SMEs, researchers, and users to co-create and test solutions in real-world settings. They can complement regulatory sandboxes by focusing on user-centered testing and feedback.
3) **University–SME Collaboration Programs:** Targeted programs should be introduced to connect SMEs with university expertise. For example, a "Digital Transformation Internship/Secondment" scheme could place ICT students or researchers in SMEs to work on specific digital projects—providing students with practical experience and SMEs with affordable expertise. The government could

fund stipends to make this attractive. Professors and academic labs could also be incentivized to partner with SMEs through grants—for example, by providing funding for applied research projects that require a university-SME team. Many SMEs face specific challenges—such as optimizing a process, developing a new product—that a university could help address through applied R&D. In Korea, for example, technical universities were linked to SME needs in the smart factory initiative, and programs such as KIAT were established to facilitate industry-academic projects. Poland's National Centre for Research and Development (NCBR) could earmark a portion of its programs specifically for SME partnerships with research units, with simplified application processes compared to large consortia projects. Additionally, Poland should establish specialized "AI for SMEs" collaboration programs. In this university, AI research centers partner with SMEs to develop practical AI applications. These could include AI graduate thesis projects addressing real SME challenges and joint AI pilot projects funded by government grants. Over time, these measures would build trust and facilitate knowledge flow between academia and the SME sector.

4) **Large–Small Enterprise Partnerships:** Larger companies—including state-owned enterprises and multinationals in Poland—should be encouraged to support SME digitalization across their value chains. The government could establish a "Digital Adoption Partnership" scheme, under which large corporations mentor or sponsor groups of SME suppliers to implement specific technologies—for example, a major automotive company assisting its parts suppliers in automating processes to meet just-in-time requirements. Incentives could include recognition awards—for example, an annual award for the best large SME collaboration—tax incentives, or, as mentioned, incorporating such mentorship into criteria, such as awarding extra credit in public procurement to large firms that have certified digitalized suppliers. Korea's win-win programs credited multinationals for mentoring SME suppliers. Poland could emulate this approach by working with its largest firms—many of which are global companies such as VW and LG operating in Poland. Such partnerships not only help SMEs but also benefit larger firms by creating more efficient supply chains.
5) **Regional Innovation Funds:** Regional funding instruments for innovation should be established or strengthened. While national programs are crucial, smaller regionally-managed funds can often be more accessible for local micro-SMEs or better tailored to local cluster needs. Voivodeships could operate digital innovation grant programs, co-financed by EU regional funds, that focus on their smart specializations—for example, robotics in one region and IoT in another. Ensuring alignment with national initiatives—through the coordination framework—would help avoid duplication. Additionally, public–private venture

funds could be considered to target digital startups and scale-ups in regions outside Warsaw, thereby spurring localized innovation and helping prevent brain drain to the capital or abroad.

6) **Continuous Skills Development Partnerships:** Educational institutions should work with government and industry to continuously update and deliver digital skills training for SME employees and owners. This should include not only IT skills but also managerial skills for digital leadership. Programs such as MBA or diploma courses in digital transformation for SME managers could be developed with subsidized tuition. Technical universities can offer certificate courses in data analytics, cybersecurity, and comprehensive AI literacy programs for SMEs. These could include "AI for Business Leaders" executive education courses and practical AI implementation workshops for technical staff, delivered with flexible scheduling or online formats. International examples include Slovenia's Voucher for Raising Digital Competencies and Portugal's SME digital training program, both of which fund SMEs to train their staff. Poland could adopt similar voucher schemes specifically for training, such as offering each SME a "training voucher" worth a fixed amount to spend on approved digital skills courses for their teams. This would help ensure that human capital development keeps pace with the adoption of technology.
7) **Leadership and Digital Literacy Development:** Recognizing that successful AI adoption requires strong leadership understanding, a comprehensive program targeting microenterprise owners and managers should be established. The program should begin with digital maturity assessments to help microenterprises understand their current readiness and identify personalized development pathways. Building on this foundation, it could include: (1) AI Leadership Bootcamps – short, intensive 2–3 day sessions designed to give micro-business owners a clear overview of AI basics, potential applications, and strategic implications for their business; and (2) peer-to-peer learning networks where early adopters share experiences and mentor others. The curriculum should remain streamlined to avoid overburdening participants and directly address one of the main barriers today—the fear of business downtime when implementing new solutions. Overall, the emphasis should be on practical business applications, decision-making capabilities, and strategic thinking about AI integration rather than technical complexity.
8) **AI Regional Specialization:** Poland should develop AI specialization strategies for major cities, building on their existing strengths. These strategies could designate Warsaw as a financial AI hub, Kraków as a hub for healthcare and research AI, Gdańsk as a hub for maritime and logistics AI, Wrocław as an industrial AI hub, and Poznań as a hub for agricultural and energy AI. Each region should host

dedicated AI innovation centers with specialized infrastructure, talent pipelines, and industry partnerships.

The combined effect of these partnerships and hub initiatives would be to embed SMEs in a supportive innovation ecosystem. Instead of operating in isolation, SMEs would have touchpoints with universities, large firms, and innovation centers that provide ideas, expertise, and opportunities for collaboration. Over time, this would foster regional clusters of innovation where SMEs, startups, academia, and corporates interact regularly—leading to knowledge spillovers and new business opportunities. For example, an SME might commercialize a university research prototype, or two SMEs introduced through a hub might jointly develop a digital product.

Poland's economy, with its strong regional cities and universities, could benefit from a more decentralized innovation approach—elevating not only Warsaw but also Kraków, Wrocław, Gdańsk, Poznań, and others as hotbeds of SME innovation. This approach would also align with EU cohesion goals aimed at reducing regional disparities.

3.8. Enhance Funding Instruments and Incentives for Microenterprises

To ensure inclusivity, special attention should be given to microenterprises, which constitute the vast majority of businesses in Poland. These firms—often family-run or sole proprietorships—typically have very limited capital and capacity, yet collectively they employ a large share of the workforce. Without tailored measures, many of the programs above may not reach them. It is recommended that funding instruments be created or adapted specifically for micro-SMEs:

- **Micro-Grants for Digital Start:** A micro digitalization grant should be introduced, offering small amounts (for example, EUR 5,000–EUR 10,000) to the smallest firms to adopt their first digital solutions. This could cover expenditures such as purchasing a computer and accounting software for a small retail shop, or setting up a basic website and online ordering system for a local restaurant. The grant should be easy to apply for, ideally through a short online form with minimal paperwork, and quickly disbursed. It could be positioned as a "Digital Starter Kit" for microenterprises. These grants should be integrated into a structured progression pathway, ensuring that recipients complete digital foundation requirements before advancing to more sophisticated AI solutions. Because the amounts are small, the risk of misuse is low, and monitoring can be simplified—for example, through proof-of-purchase submissions. By offering micro-grants, the government would signal that no business is too small to go digital. Even if each grant is small, across thousands of microenterprises, it could make a significant difference in bringing them online.

- **Low-Interest Micro-Loans and Guarantees:** The availability of micro-loans earmarked for digital investments should be expanded, with partial guarantees to encourage banks to lend. Poland's BGK (national development bank) could launch a program in partnership with commercial banks under which microenterprises could obtain loans of up to EUR 20,000 at subsidized interest for purchasing digital equipment or software, or for hiring IT services. BGK could guarantee the loans up to 80% to mitigate bank risk. A micro-consortium matching system could also be implemented, in which small technology providers are prequalified and matched with microenterprises based on sector, location, and specific needs. This would enable three to five microenterprises to jointly procure AI solutions, sharing costs and learning experiences while creating peer support networks. As with green investment loans in some countries, digital transformation loans could be offered with preferential terms. It is essential to ensure that microenterprises are aware of and guided through the application process by local chambers or business support centers, as many micro-owners find bank processes daunting.
- **Structured Digital-to-AI Progression Pathway:** A clear three-stage development framework should be implemented. Stage 1 (Digital Foundation) focuses on basic digitalization, including transitioning from paper-based to digital record-keeping, establishing an online presence, and implementing basic accounting software. Stage 2 (Data Readiness) would involve introducing data collection and basic analytics capabilities, customer relationship management systems, and digital payment processing. Stage 3 (AI Integration) would introduce AI-powered tools—such as automated customer service, predictive inventory management, or personalized marketing—only after the previous stages are completed. Each stage should include specific completion criteria and dedicated support mechanisms, ensuring that microenterprises build solid foundations before advancing to more complex technologies.
- **Tax Incentives for the Smallest Firms:** The tax system should be used to encourage micro and small businesses to invest in technology. For example, micro-SMEs could be allowed full depreciation in the first year for digital assets, enabling them to write off the expense immediately. Alternatively, an enhanced tax deduction—such as 150% of expenses—could be introduced for spending on approved digitalization activities, including software, hardware, and training. Given that many microenterprises may pay minimal tax if profits are low, this would not address all challenges, but for those that do pay, it would reduce net cost. Poland could also consider offsetting some social security contributions or providing a one-time tax credit for microenterprises that complete a recognized digital upgrade. For example, firms that obtain a certain digital certification or implement a specified level of technology could receive a fixed tax credit. Although more complex, such

measures could provide strong incentives for digital adoption.

- **AI-Specific Tax Incentives:** Microenterprises should be allowed to depreciate AI investments in the first year fully, or enhanced tax deductions —such as 150% of expenses—could be introduced for spending on approved AI activities, including software, training, and consulting. For microenterprises that pay minimal tax, alternative incentives could include offsetting social security contributions or providing one-time tax credits for completing recognized AI implementations or certifications.
- **Leveraging EU Microfinance:** Poland should work with EU-funded microfinance programs—such as the EU's InvestEU or predecessors that had microfinance windows—to channel more funds to Polish microenterprises for digital projects (European Commission, 2022b). Microfinance institutions could be mobilized to include an ICT lending component. Additionally, programs such as Slovenia's digital skills voucher or other small-scale EU initiatives should be studied and potentially replicated (European Commission, 2024d).
- **Turnkey AI Solutions and Education:** AI solutions should be developed specifically designed for microenterprises, requiring minimal technical expertise to implement and maintain. These could include AI-powered business tools integrated into existing software already used by microenterprises, such as accounting systems with AI analytics capabilities. Examples include customer service platforms with AI chatbots that require no programming knowledge, or inventory management systems with AI forecasting capabilities. Partnerships with AI vendors could be established to create "Micro-AI Packages"—preconfigured, affordable AI solutions tailored for specific microenterprise sectors such as retail, hospitality, crafts, and services. Additionally, basic AI literacy programs should be provided through local chambers of commerce, focusing on practical applications rather than technical complexity.
- **Targeted Outreach and Simplified Processes:** All of the above instruments should be accompanied by outreach specifically tailored to microenterprises. This could involve partnering with local governments, trade associations for craftspeople, and other relevant organizations to disseminate information. It is also crucial to simplify application and reporting procedures for these small amounts—potentially using a trust-based approach with random audits rather than extensive paperwork for every applicant. Digital tools could be used to manage these schemes—for example, a user-friendly app for micro-grant applications—which would also encourage microenterprises to engage digitally in the process itself.
- **AI-Focused Outreach:** Since microenterprises often need basic AI solutions, outreach should focus on ready-to-use AI tools that integrate seamlessly with services they already use. "AI for Microenterprises" workshops could be organized

in local communities, demonstrating simple AI applications such as automated customer responses, basic data analytics, or smart scheduling tools. Local business associations and chambers of commerce could be engaged to build trust and provide peer-to-peer learning opportunities.

- **Performance Monitoring and Ecosystem Learning System:** A comprehensive but streamlined monitoring framework should be established, incorporating: (1) Digital Maturity Tracking—regular assessments of participating microenterprises' digital capabilities using standardized, easy-to-apply metrics; (2) Business Impact Measurement—tracking revenue growth, customer satisfaction, and operational efficiency improvements; (3) Program Adaptation Mechanism—quarterly reviews of program effectiveness with adjustments based on participant feedback and observed outcomes; (4) Knowledge Sharing Platform—a digital repository of success stories, best practices, and lessons learned, accessible to all microenterprises; and (5) Annual Impact Assessment—a comprehensive evaluation of program effectiveness, including cost-benefit analysis, and recommendations for scaling or modification.

By providing microenterprises with accessible resources, Poland would help ensure that the benefits of digital transformation extend to even the smallest firms. This has social importance—by preventing a digital divide that excludes nano-enterprises—and economic significance, as incremental improvements at the micro level can generate meaningful macroeconomic impact. An additional benefit is that once microentrepreneurs begin using basic digital tools—such as transitioning from pen-and-paper to digital bookkeeping— they are often encouraged to adopt further technologies, creating momentum for continued self-driven digitalization. The structured approach outlined above would help ensure that this momentum is channeled effectively through a systematic progression pathway, supported by strong leadership development and comprehensive ecosystem support.

References

#CyberMadeInPoland. Raport z Inicjatywy #CyberMadeInPoland – 2023 [#CyberMadeInPoland Initiative Report].Warsaw: Klaster Cyberbezpieczeństwa, 2023.

Amazon Web Services. "AI Adoption in Poland Grew by 36% over the Past Year." Press Release, October 11, 2024. https://www.aboutamazon.eu/news/empowering-small-business/ai-adoption-in-poland-grew-by-36-over-the-past-year.

Amazon Web Services and Strand Partners. Unlocking Poland's AI Potential in the Digital Decade – Phase II.Luxembourg: Amazon Web Services, 2024.

BoanNews. 82.5% of Cyberattack Damage in Korea Targets SMEs, Yet Security Budgets Slashed [*한국 사이버공격 피해 82.5%가 중소기업…예산은 대폭 삭감*]. https://m.boannews.com/html/detail.html?idx=133399, 2025.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union L 333, December 27, 2022.

EDIH CyberSec. Katalog usług 2024 [2024 Service Catalog]. Warsaw: European Digital Innovation Hub (CyberSec), 2024.

European Chamber of Commerce in Korea (ECCK). Guide to the Regulatory Sandbox. August 2020. https://ecck.or.kr/wp-content/uploads/2020/08/Guide-to-the-Regulatory-Sandbox.pdf.

European Commission. Digital Economy and Society Index (DESI) 2022: Poland. Brussels: European Commission, 2022a.

European Commission. Framework Operation #3 Microfinance and Social Enterprises. InvestEU Programme. https://investeu.europa.eu/investeu-operations-0/investeu-operations-list/framework-operation-3-microfinance-and-social-enterprises_en, 2022b.

European Commission. "Poland 2025 Digital Decade Country Report." https://digital-strategy.ec.europa.eu/en/factpages/poland-2025-digital-decade-country-report, 2024a.

European Commission. European Innovation Scoreboard 2024 – Country Profile: Poland. Luxembourg: European Commission, 2024b. https://ec_rtd_eis-country-profile-pl.pdf.

European Commission. Poland – Digital Decade Country Report 2024. Brussels: European Commission, 2024c.

European Commission. "Available Funding in Slovenia." Digital Skills and Jobs Platform. Last modified July 30, 2024. https://digital-skills-jobs.europa.eu/en/latest/briefs/available-funding-slovenia, 2024d.

European Commission. Poland 2024 Digital Decade Country Report. Brussels: Directorate-General for Communications Networks, Content and Technology, 2024e. https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-country-reports.

European Union. "Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)." Official Journal of the European Union L 1689, June 13, 2024.

Eurostat. "Use of Artificial Intelligence Technologies by Enterprises." Statistical Release, March 2025.

Financial Services Commission (FSC Korea). FSC Regulatory Sandbox (Dubbed). YouTube video. https://www.youtube.com/watch?v=wjBp8MnJh20, 2025.

International Federation of Robotics (IFR). World Robotics 2024: Industrial Robots – Statistics, Market Analysis, Forecasts and Case Studies. Frankfurt: IFR Statistical Department, 2024.

K-DATA (Korea Data Agency). 2023 Data Voucher Project Results Report [in Korean]. Seoul: Korea Data Agency, 2023.

Kang, E. S. "Measures to Strengthen Information Security for Small and Medium Enterprises." Issues and Focus, no. 2156. National Assembly Research Service, November 3, 2023.

KDI (Korea Development Institute). Sharing Knowledge, Sharing the Future 2023: Country Case Study. Sejong: KDI, 2023.

KDI Economic Information Center. Global Smart Factory Trends: International Developments in Smart Manufacturing (Issue 2021–04). Sejong: Korea Development Institute, 2021. [in Korean]

Korea Internet & Security Agency (KISA). Press Release on Information Security Survey Results for SMEs and Venture Companies in Gyeonggi Region [경기지역 중소·벤처기업 정보보호 보안실태조사 결과 발표]. Press Release, August 9, 2023.

Korea Internet & Security Agency (KISA). Regional Information Security Support Center [지역정보보호센터]. https://risc.kisa.or.kr/.

Korea Ministry of Science and ICT. AI Framework Act Implementation Guidelines. Seoul: MSIT, 2024.

Korea SME Technology Market. Korea SME Technology Market [중소기업기술마켓]. https://www.techmarket.kr/.

Korea Technology and Information Promotion Agency for SMEs (TIPA). Technology Protection Support Services for SMEs [중소기업을 위한 다양한 기술보호 지원 서비스]. https://www.ultari.go.kr/portal/ptm/main.do.

KOSMO (Korea Smart Manufacturing Office). "What Is a Smart Factory?" https://smart-factory.kr/eng/smartFactory.do?menuId=03.

KOSMO Smart Manufacturing Innovation Promotion Group. 2025 Smart Manufacturing Innovation Support Project Briefing Session. YouTube video, February 2024. https://www.youtube.com/watch?v=QU4RXDmOMGc.

KOSMO Smart Manufacturing Innovation Promotion Group. Leap to a Global Manufacturing Powerhouse! Advancement Plan for the Smart Manufacturing Innovation Ecosystem. YouTube video, February 2024. https://www.youtube.com/watch?v=EOKPBdXKDzI.

KPMG Poland. Advancing the Digital Transformation of Polish Enterprises. Warsaw: KPMG, 2024.

Kwon, Inhyuk. "Korea's Institutional Framework on SME Digitalization." PowerPoint presentation, OECD Workshop, May 11, 2022.

MC (Ministerstwo Cyfryzacji). Polityka rozwoju sztucznej inteligencji w Polsce do 2030 roku. Warsaw: Ministry of Digital Affairs, 2025.

Ministry of Digital Affairs, Poland. "Draft Act on Artificial Intelligence Systems." Draft dated February 10. Warsaw: Ministry of Digital Affairs, 2025.

Ministry of Science and ICT and Korea Information Security Industry Association (KISIA). 2024 Survey on Information Security in Korea [2024 정보보호 실태조사]. December 2024.

Ministry of Science and ICT, Korea. "Press Release: National AI Committee Established." Seoul: Ministry of Science and ICT, February 2024.

Ministry of SMEs and Startups. Smart Manufacturing Innovation Strategy for SMEs (Joint Government Initiative). Press Release, December 13, 2018. Sejong. [in Korean]

Ministry of SMEs and Startups. Press release: Recruitment of participating companies for the "SME Smart Service Support Project" to promote digital transformation (DX) in the service sector. April 3, 2025. Ministry of SMEs and Startups, Republic of Korea. [in Korean]. https://mss.go.kr/site/smba/ex/bbs/View.do?cbIdx=310&bcIdx=1057801&parentSeq=1057801

MRiT (Ministerstwo Rozwoju i Technologii). Program transformacji cyfrowej przedsiębiorstw, 2025. Unpublished draft. Warsaw: Ministry of Development and Technology, 2025.

NASK. Firma Bezpieczna Cyfrowo – Dokumentacja Programu [Digitally Secure Company – Program Documentation]. Warsaw: NASK, 2023.

OECD. Digital Government Review of Poland: Bridging the Digital Gap. Paris: OECD Publishing, 2020.

OECD. SMEs and Entrepreneurship Outlook. Paris: OECD Publishing, 2023.

OECD. Survey of Economic Policy: Poland. Paris: OECD Publishing, 2023.

OECD. Digital Economy Policy Outlook. Paris: OECD Publishing, 2024.

OECD. OECD Economic Surveys: Poland 2025. Volume 2025/2. Paris: OECD Publishing, February 2025a.

OECD. Strengthening FDI and SME Linkages in Poland. Paris: OECD Publishing, 2025b.

OECD. Main Science and Technology Indicators (MSTI) Database. March 2025. https://www.oecd.org/en/data/datasets/main-science-and-technology-indicators.html, 2025c.

Polish Agency for Enterprise Development (PARP). Cyberbezpieczeństwo – Materiały Szkoleniowe dla MŚP[Cybersecurity – Training Resources for SMEs]. Warsaw: PARP, 2023a.

Polish Agency for Enterprise Development (PARP). Monitoring of the Digital Transformation of Enterprises – 2023.Warsaw: PARP, 2023b.

Polish Agency for Enterprise Development (PARP). Report on the Condition of the Small and Medium-Sized Enterprise Sector in Poland (2024). Warsaw: PARP, 2024.

Regulatory Reform Committee. Regulatory Reform Book 2023. [in Korean], 2023.

Regulatory Reform Committee. 2023 Regulatory Reform Annual Report. March 29, 2024. [in Korean].

Relevant Ministries (Republic of Korea). Plan to Advance the Smart Manufacturing Innovation Ecosystem through the Fostering of Specialized Smart Manufacturing Enterprises. October 2, 2024. [in Korean]

Skwarczynska, Barbara Maria, et al. Poland Structural Policies for Competitiveness: Position Paper on Regulatory Policy. Washington, D.C.: World Bank Group, 2023.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa [Act of 5 July 2018 on the National Cybersecurity System]. Dziennik Ustaw 2018, poz. 1560.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 [Act on Promotion of Information and Communications

Network Utilization and Information Protection, etc.]. Amended to Act No. 18787, effective January 2024.

중소기업 기술보호 지원에 관한 법률 [Act on Support for Protection of Small and Medium Enterprise Technology]. Law No. 14821, effective from October 2017.

Related materials

Ju, Hyeon. Smart Factory Policies and SMEs' Productivity in Korea. KIET Occasional Paper No. 111. Sejong: Korea Institute for Industrial Economics and Trade, 2021.

Korea Industrial Technology Association (KOITA). "DT Council." https://www.koita.or.kr/conts/104006001001000.do.

2024/25 Knowledge Sharing Program

This publication summarizes the key findings of the Knowledge Sharing Program (KSP), funded by the Ministry of Economy and Finance (MOEF) of the Republic of Korea. The views expressed are those of the authors.
The KSP is a policy-oriented development cooperation program designed to share Korea's development experience and knowledge. Its goal is to support the institutional and capacity building of partner countries through collaborative research, policy consultations, and technical assistance on key policy issues.

For more information:
https://www.ksp.go.kr

Ministry of Economy and Finance (MOEF)
Sejong Government Complex, 42, Doum 6-ro, Sejong-si 30112, Republic of Korea
Tel. 82-444-215-7742
www.moef.go.kr

Korea Development Institute (KDI)
263, Namsejong-ro, Sejong-si 30149, Republic of Korea
Tel. 82-44-550-4114
www.kdi.re.kr

Ministry of Economic Development and Technology (MRiT), Republic of Poland
Pl. Trzech Krzyży 3/5 00-507 Warsaw
Tel. 48-22-250-0123
www.gov.pl/web/development-technology

Knowledge Sharing Program (KSP)
www.ksp.go.kr

9 791175 660243 94320
ISBN 979-11-7566-024-3
ISBN 979-11-5932-110-8 (set)