Presented by the MOEF, Republic of Korea

Knowledge Sharing Program

2024/25 KSP Policy Consultation Report

Poland

Strengthening Strategic Framework for SME Digital Transformation in Poland

Ministry of Economy and Finance

KDI Korea Development Institute

Ministry of Economic Development and Technology
Republic of Poland

Government Publications Registration Number
11-1051000-100111-01

Knowledge Sharing Program

2024/25 KSP Policy Consultation Report

Poland

Strengthening Strategic Framework for SME Digital Transformation in Poland

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

2024/25 KSP Policy Consultation Report

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 of Poland (MRiT)
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, KISDI
Authors	Chapter 1. Sangwon Ko, Senior Research Fellow, KISDI Sehoon Lee, Senior Research Associate, KDI Paulina Kiewicz, Chief Specialist, MRiT Chapter 2. Hyeshun (Melissa) Yoon, Professor, Hanyang University Katarzyna Colombel, Chief Specialist, MRiT Chapter 3. Hyungjong Kim, Professor, Seoul Women's University
English Editor	Korea Translation Co., Ltd.

Government Publications Registration Number 11-1051000-100111-01
ISBN 979-11-7566-029-8 95320
979-11-5932-164-1 (set)

2024/25 KSP Policy Consultation Report

Strengthening Strategic Framework for
SME Digital Transformation in Poland

Poland

Contents

Chapter 2

Strategy for Building an AI Innovation Ecosystem and Regulatory Innovation for SMEs' Digital Transformation in Poland

Chapter 3

Cybersecurity Innovation Ecosystem and Regulatory Reform for Polish SMEs

List of Tables

Chapter 1

Chapter 2

Chapter 3

List of Figures

Chapter 1

Chapter 2

Chapter 3

2024/25 KSP with Poland

Sehoon Lee (Korea Development Institute)

2024/25 KSP with Poland

Sehoon Lee (Korea Development Institute)

Polish SMEs account for 99.8% of all enterprises and generate 46.6% of GDP through their business activities, serving as the key driving force of the national economy. The adoption of digital technologies significantly enhances competitiveness by improving productivity and promoting innovation through automation and operational efficiency. As digital infrastructure expands and business processes become increasingly complex, discussions have also intensified on introducing AI applications (AX) and strengthening cybersecurity to support intelligent decision-making, demand forecasting, and secure management of digitalized data.

Nevertheless, Polish SMEs currently face challenges in digital transformation and AI adoption due to (1) low awareness and interest in digital technologies, (2) insufficient coordination between the public and private sectors, and (3) limited monitoring and evaluation framework for assessing digital transformation levels (KPMG, 2024). In addition, amid the growing number of cyberattacks targeting Poland as a neighboring country affected by the Russia–Ukraine war, there is a growing need to develop concrete measures to strengthen cybersecurity among Polish SMEs.

Against this backdrop, the Ministry of Economic Development and Technology of Poland (MRiT) applied for the 2024/25 Knowledge Sharing Program (KSP) to establish a mid- to long-term national strategy for SME digital transformation, by leveraging not only on European experiences but also on best practices from Asian countries such as Korea in digital transformation policies and support programs.

The KSP project with Poland, titled “Strengthening the Strategic Framework for SME Digital Transformation in Poland,” was conducted under three sub-topics: Establishing a mid- to long-term strategy for SME digital transformation, building an AI and cybersecurity innovation ecosystem, and promoting regulatory reform.

Project Title: Strengthening Strategic Framework for SME Digital Transformation in Poland		
ROK Institutes	Ministry of Economy and Finance (MOEF) Korea Development Institute (KDI)	
Polish Institute	Ministry of Economic Development and Technology (MRiT)	
	Sub-Topic	**Researchers**
1	Development of a Mid- to Long-Term Strategy and Action Plan for SME Digitalization (Ch1)	Sangwon Ko (KISDI) Sehoon Lee (KDI) Paulina Kiewicz (MRiT)
2	Strategy for Building an AI Innovation Ecosystem and Regulatory Innovation for SMEs' Digital Transformation in Poland (Ch2)	Hyeshun (Melissa) Yoon (Hanyang University) Katarzyna Colombel (MRiT)
3	Cybersecurity Innovation Ecosystem and Regulatory Reform for Polish SMEs (Ch3)	Hyungjong Kim (Seoul Women's University)
Major KSP milestones included: Launching Seminar and High-level Dialogue (Poland, 17-22 November 2024) Policy Seminar and In-depth Study (Poland, 23 February- 1 March 2025) Interim Reporting and Policy Practitioner's Workshop (ROK, 27-31 May 2025) Final Reporting Seminar and Senior Policy Dialogue (Poland, 20-25 July 2025)		

The project achieved notable outcomes at each implementation stage, as outlined below.

In November 2024, the KSP team, composed of Korean experts, held the KSP Launching Seminar in Warsaw. During the seminar, the team reaffirmed the policy consultation needs of the MRiT and finalized the scope of policy research in close collaboration with a Polish local consultant. The team also met with major public institutions supporting SME digital transformation in Poland, including the Ministry of Digital Affairs, Polish Agency for Enterprise Development (PARP), Polish Development Fund (PFR), and Research and Academic Computer Network (NASK), to assess the current policy environment and identify key challenges.

In February 2025, the KSP team revisited Poland to conduct additional meetings with key actors in the digital transformation process, such as Microsoft, Allegro, and Technosystem, gaining further insights for developing specific policy recommendations. Moreover, discussions with the Polish Chamber of Information Technology and Telecommunications (PIIT), Lodz Special Economic Zone (LSSE), and KOTRA Warsaw Office went beyond policy research, exploring potential business cooperation opportunities between Korean and Polish companies in the field of digital transformation.

In May 2025, MRiT officials were invited to Korea to participate in the KSP Interim Reporting Workshop, where the KSP team presented interim findings and gathered MRiT's feedback. During the visit, the Polish delegation held meetings with the Ministry of SMEs and Startups (MSS), Korea SMEs and Startups Agency (KOSME), Korea Internet & Security Agency (KISA), and Sejong Technopark (SJTP) to learn about Korea's ongoing SME digital transformation support policies, including the Innovation Voucher Program. They also visited leading Korean AI and cybersecurity companies such as NAVER, AhnLab, WINS Technet, and Bunjang, to discuss both their digital transformation experiences and potential collaboration with Polish enterprises.

In July 2025, the KSP Final Reporting Workshop was held in Poland, during which the KSP team delivered its final policy recommendations—including the Digitalization Voucher Program, AI

Regulatory Sandbox, and Local Digital Competence Centers—to Polish officials led by Secretary of State Michał Jaros. The workshop also featured a presentation on Bunjang's AI adoption case, highlighting a best practice of SME digitalization in Korea. Following the workshop, the KSP team visited Cyfronet AGH in Krakow to explore potential follow-up cooperation in the areas of AI ecosystem and supercomputing.

This project marked the first bilateral KSP with the Polish Ministry of Economic Development and Technology, providing timely policy recommendations that will contribute to the design of Poland's upcoming "Digital Transformation Programme for Enterprises" (to be announced in 2026). Beyond policy research, the KSP also strengthened cooperation networks between Korean and Polish governments and industries, paving the way for concrete follow-up collaborations.

Building on the outcomes of this year's KSP, it is expected that future cooperation in digital transformation, AI, and cybersecurity will further advance, leading to sustainable and substantive economic partnership between Korea and Poland.

01

Chapter

Development of a Mid- to Long-Term Strategy and Action Plan for SME Digitalization

Sangwon Ko (Korea Information Society Development Institute)
Sehoon Lee (Korea Development Institute)
Paulina Kiewicz (Ministry of Economic Development and Technology of Poland)

Keywords:
Digital Transformation, Small and Medium Enterprise (SME), Technology & Innovation Policy, Digital Economy

Development of a Mid- to Long-Term Strategy and Action Plan for SME Digitalization

Sangwon Ko (Korea Information Society Development Institute)
Sehoon Lee (Korea Development Institute)
Paulina Kiewicz (Ministry of Economic Development and Technology of Poland)

1. Introduction

Since joining the European Union in 2004, Poland has achieved rapid economic growth among Central and Eastern European countries by actively embracing economic liberalization, attracting substantial foreign direct investment (FDI), and significantly improving its transportation infrastructure, including highways. Leveraging its low labor costs and strategic geographical position, which links Western and Eastern Europe, Poland has become a major destination for multinational corporations. This has driven not only the development of manufacturing sectors such as automotive and electronics, but also accelerated the expansion of service industries, including finance and retail. As a result, Polish small and medium-sized enterprises (SMEs) have also experienced rapid growth in economic activity.

Despite these achievements, Poland continues to rank in the lower tier among EU member states in terms of digital transformation—an essential driver of productivity enhancement and innovation. In particular, Polish SMEs face significant barriers, including low awareness of the benefits of digital technology, high adoption costs, and shortages of skilled personnel. These challenges underscore the urgent need for an effective national strategy and support programs to promote the digital transformation of SMEs.

Recognizing these issues, the Ministry of Economic Development and Technology (MRiT)—Poland's lead ministry for enterprise policy—is in the process of designing a new national strategy titled "Digital Transformation Programs for Enterprises." This initiative aims to establish a more integrated and effective support system for SME digitalization.

Against this backdrop, this report seeks to support the Polish government in formulating effective SME digital transformation policies. It provides a comprehensive analysis of the current digital intensity of Polish SMEs, evaluates existing national policies and programs, and identifies areas for improvement and key policy implications. Drawing on Korea's representative support programs for SME digitalization—such as the AI Regulatory Sandbox, Smart Factory initiative, and Smart Service support scheme—this report offers actionable policy recommendations tailored to the Polish context.

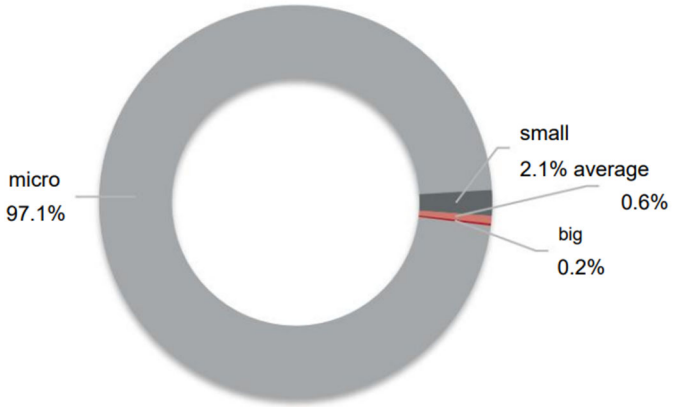
2. Current Status of Digital Transformation for SMEs in Poland

2.1. Overview of Poland's SME Sector

As of 2023, the total number of enterprises in Poland was approximately 2.31 million, with SMEs accounting for about 99.8% of all businesses. Among SMEs, micro-enterprises (those with fewer than 10 employees) made up approximately 97.1% of the sector. Polish SMEs make a significant economic contribution. In 2022, large enterprises accounted for 27.5% of Poland's enterprise-generated GDP, while SMEs contributed 46.6%. This shows that SMEs were effectively responsible for nearly half of the national economy produced by enterprises (PARP, 2025).

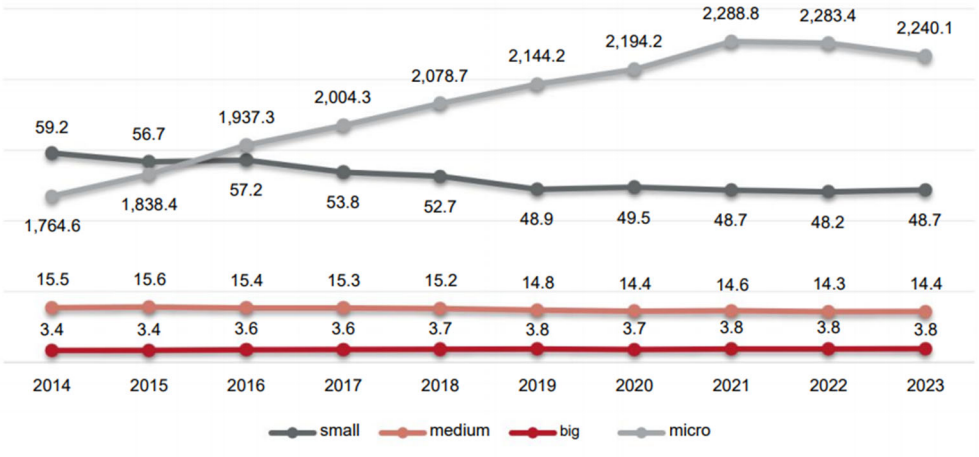
In particular, the steady increase in the number of SMEs in Poland suggests that a favorable business environment is being established for SMEs. Over the 10 years from 2014 to 2023, the number of SME business entities increased by approximately 464,300, representing a nearly 25% growth. Notably, the growth was most pronounced in the number of micro-enterprises with fewer than 10 employees.

[Figure 1-1] Types of Companies in Poland



Source: PARP (2025).

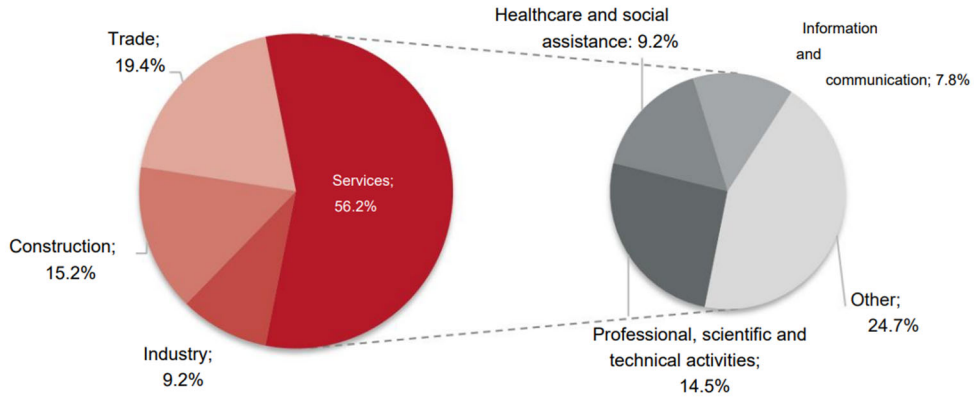
[Figure 1-2] Changes in the Number of Companies in Poland



Source: PARP (2025).

The distribution of SMEs by industry sector in Poland is as follows: services (56.2%), manufacturing (24.4%), and trade (19.4%). In the services sector, SMEs operating in the fields of science and technology (14.5%) and information and communication (7.8%) account for approximately 22.3% of the total. This indicates that a high level of digital capability is required in the services industry.

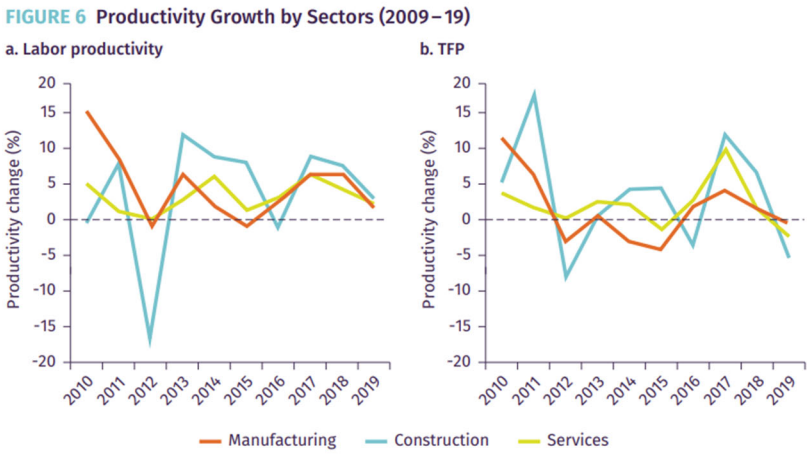
[Figure 1-3] Types of Companies in Poland



Source: PARP (2025).

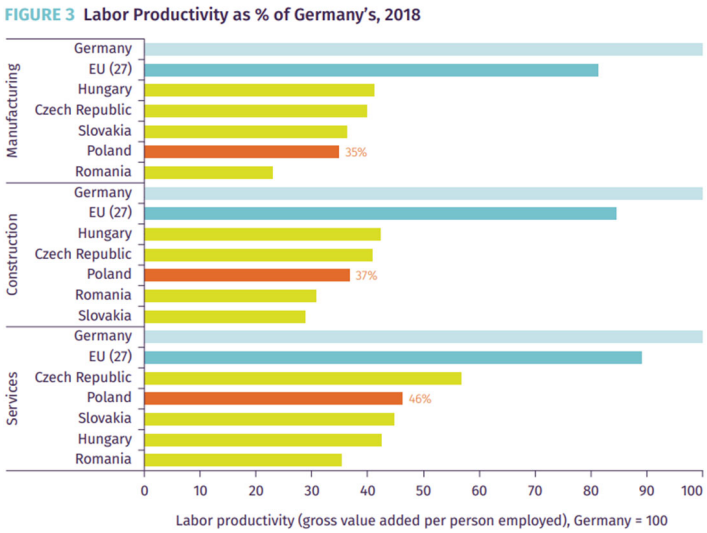
Poland has achieved significant growth in its SME sector through business-friendly policies and the attraction of FDI following its economic transition. However, the productivity of Polish companies remains relatively low. Between 2010 and 2019, Poland's labor productivity and total factor productivity (TFP) saw temporary improvements from 2015 to 2018 but declined sharply from 2019 onward. A comparison with major European countries highlights Poland's lagging labor productivity, particularly in the manufacturing sector. Given the substantial role of manufacturing in Poland's industrial structure, enhancing labor productivity in this sector is especially critical.

[Figure 1-4] Productivity Growth by Sectors in Poland



Source: World Bank (2022).

[Figure 1-5] Labor Productivity Growth by Sectors in Poland

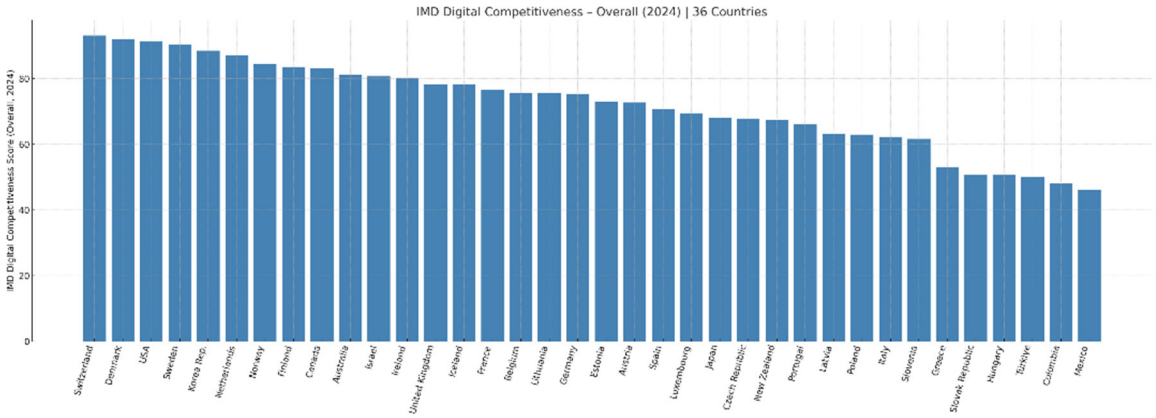


Source: World Bank (2022).

2.2. Current Status of Digitalization of Polish SMEs

Despite the quantitative growth of SMEs in Poland, labor productivity has continued to decline. A key factor contributing to this trend is the relatively low level of digitalization among SMEs. As of 2024, Poland ranked 28th out of 36 OECD member states in the World Digital Competitiveness Ranking (WDC), positioning it among the lower-performing countries. In particular, Poland scored relatively lower on the Future Readiness Index of the WDC indicators, which evaluates a country's level of preparedness for digital transformation in areas such as adaptive attitudes, business agility, and IT integration.

[Figure 1-6] IMD World Digital Competitiveness Ranking (OECD Member Countries)



Note: Elaborated by the author based on information from World Digital Competitiveness Ranking (2024).
Source: Author (2025).

An analysis of the key performance indicators (KPIs) for the digital transformation of Polish SMEs indicates that Poland demonstrates strengths in digital infrastructure, exceeding the EU average in areas such as Very High Capacity Networks (VHCN) and 5G. However, the country lags in the adoption of advanced digital technologies, such as AI, Cloud Computing, and Data Analytics, as well as in human capital development. In particular, Poland's growth rate in AI, basic digital skills, and digital public services for businesses is lower than the EU average.

One of the contributing factors to Poland's relative weaknesses in digital technology and human capital is its low R&D investment. From 2015 to 2022, Poland's R&D expenditure as a percentage of GDP remained around 1%, significantly lower than Germany (3%) and the OECD average (2–3%). This suggests that, given the limited R&D resources, improving efficiency—such as focusing R&D support on Poland's key industries and technology sectors—is essential to securing the necessary technologies and specialized workforce for SME digital transformation.

<Table 1-1> 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 (2025).

To identify key industries for digital transformation, it is crucial to assess the level of digitalization across various industrial sectors in Poland. According to the 2024 Eurostat survey, the digitalization gap between Poland and Western European countries, including Germany, France, Italy, the Netherlands, and Sweden, was most pronounced in industries with low levels of digitalization. When comparing the Digital Intensity Index between Poland and Western Europe, based on enterprises with at least a basic level of digital intensity, most industrial sectors in Poland exhibited lower digital intensity, except for computer programming, motor vehicles, and accommodation.

Overall, the digitalization gap was more significant in manufacturing than in services. In particular, within the manufacturing sector, the gap was wider in basic industries such as food, textiles, and basic metals rather than in advanced manufacturing. This suggests that, to achieve a more balanced improvement in SME digital transformation, a greater focus and support should be directed toward

traditional manufacturing industries. At the same time, efforts should also be made to enhance or sustain the competitiveness of the service sectors.

[Figure 1-7] Digitalization Gap by Industry Sector between Poland and Europe

Note: 1) Elaborated by the author based on information from Eurostat (2024).
2) 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: Author (2025).

2.3. Barriers to the Digital Transformation of SMEs in Poland

The digital transformation of Polish SMEs is a crucial factor in enhancing national economic innovation and competitiveness. However, many companies still face various obstacles in adopting new technologies. In 2024, the Ministry of Economic Development and Technology of Poland and KPMG Poland, a consulting firm, surveyed 650 Polish SMEs to analyze the current state of digital transformation and the challenges they encounter.

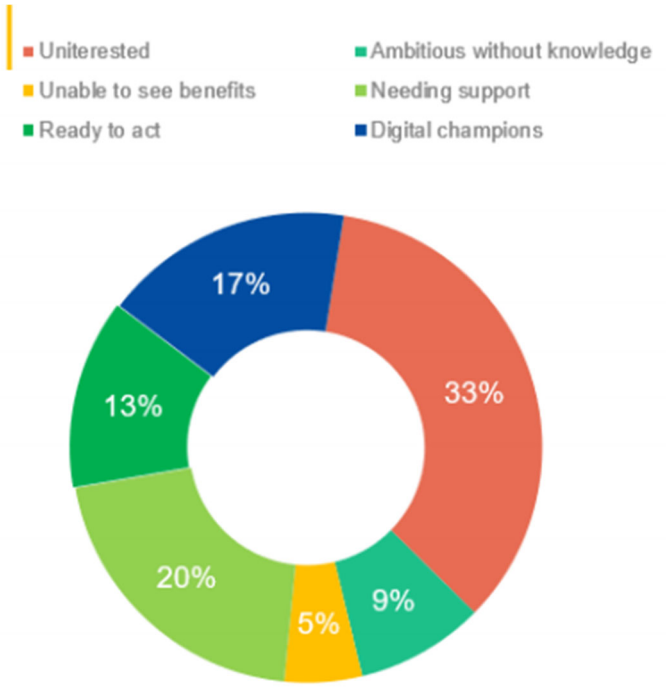
According to the survey results, only 30% of Polish SMEs had either already reached a certain level of digital transformation (Digital Champions) or were ready to act. Meanwhile, approximately

33% of respondents stated that they were uninterested in digital transformation. The primary barriers to digital transformation included low awareness of its necessity, a lack of knowledge about government support programs, financial constraints, difficulties integrating digital solutions with existing systems, and a shortage of dedicated personnel. The key challenges identified for each respondent group are summarized in <Table 1-2> below.

Regarding key areas of digital technology adoption, surveyed companies most frequently reported implementing digital solutions in financial management and accounting, document management, promotion, marketing, and customer outreach—all of which relate to internal business processes. This indicates a high demand for digital service solutions, such as cloud computing, CRM, and ERP, to optimize business processes. However, since approximately 70% of the surveyed companies operate in the service sector, the findings may not fully reflect digital transformation activities in small and medium-sized manufacturing enterprises.

These findings suggest that to accelerate the digital transformation of Polish SMEs, the Polish government must go beyond simple technological support and provide a combination of financial, educational, and institutional assistance. Policy interventions should encourage SMEs to view digital transformation not as a cost burden, but as a growth opportunity, while expanding tailored support programs that address the specific needs of SMEs at various levels.

[Figure 1-8] Survey Results of Polish SME Stakeholders on Digital Transformation



Source: KPMG Poland (2024).

<Table 1-2> Main Barriers and Limitations of SMEs in Each Group

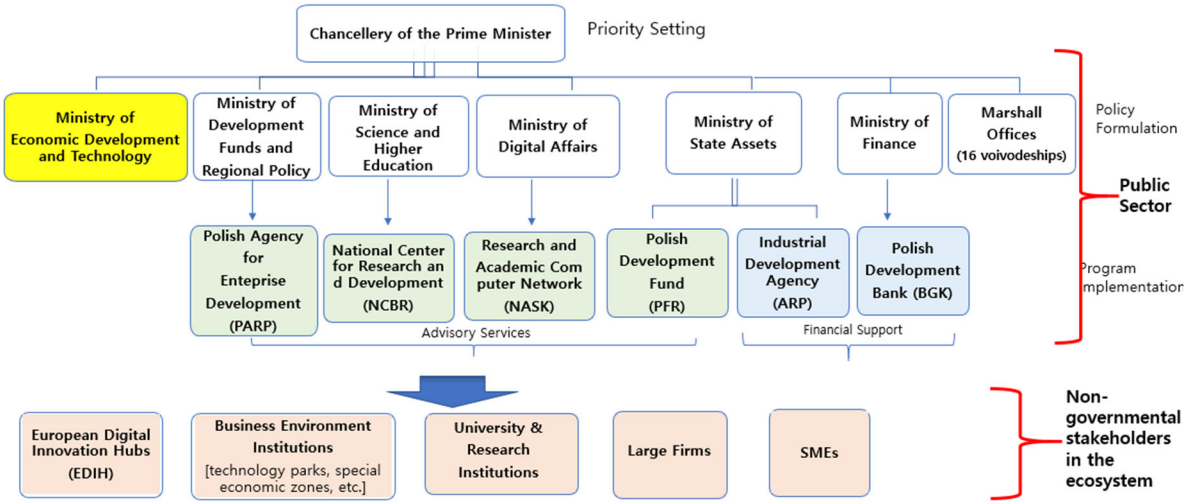
Uninterested	Ambitious without Knowledge	Unable to See Benefits	Needing Support	Ready to Act	Digital Champions
• Lack of identified need for digitization, lack of ambition for digital development • Approach to digitization focused only on implementing required solutions • Significant role of budgetary and competency limitations	• Insufficient knowledge about digital transformation • Significant role of cost constraints, lack of sufficient funds • Employees are not ready, mainly due to a lack of training and development opportunities	• Lack of identified benefits from further digital transformation, given a relatively high level of advancement compared to other segments • Digitization causes fear among employees	• Insufficient knowledge, especially regarding available administrative support • Resource constraints, lack of time to explore new opportunities • Perception of lack of intuitiveness in some digital solutions	• Lack of integration of appropriate infrastructure supporting digital transformation • Need for employee training and support during implementation	• A relatively high level of maturity of the digital transformation, which results in a further increase in solutions not being high

Source: KPMG Poland (2024).

3. Analysis of Existing Digital Transformation strategies and Support Programs for SMEs in Poland

3.1. Poland's Innovation System for SMEs' Digital Transformation

[Figure 1-9] National Governance System Supporting SME Digitalization in Poland as of 2025



Note: Compiled and organized by the authors.
Source: Author (2025).

Poland's national governance system for SME digital transformation comprises multiple central government entities and implementing agencies. However, the roles and support structures of these institutions are highly fragmented, making it difficult to implement integrated policies effectively, thereby reducing overall policy efficiency.

As of 2025, the Ministry of Economic Development and Technology's Department of Digital Economy serves as the lead ministry for SME digital transformation. This department is responsible for formulating mid-to-long-term action plans and developing efficient support programs to ensure the effective implementation of Poland's national digital decade strategic roadmap (as the national implementation framework of the EU's Digital Decade Program) and Poland's national Digitalization Strategy 2035.

The Ministry of Digital Affairs also plays a crucial role in the digital transformation of SMEs. Established as an independent ministry in 2015, it is responsible for developing national digital strategies, building infrastructure for the dissemination of digital technology—including AI and cybersecurity—and enhancing digital services for public institutions and businesses.

The Ministry of Funds and Regional Policy (MFiPR) oversees the allocation of EU cohesion funds to support SME digital transformation. The 16 Marshall Offices design and implement Regional Operational Programs (RPOs), tailoring measures to the digital needs of each voivodeship. Together, they connect EU funding with local SME priorities.

Various implementing agencies, including PARP, NASK, NCBR, PFR, ARP, and BGK, implement support programs for SME digital transformation.

- **PARP (Polish Agency for Enterprise Development):** Operates under the Ministry of Funds and Regional Development, utilizing European Funds as a primary financial resource. It manages European Digital Innovation Hubs, provides financial support for SME digitalization, and offers consulting and training programs.
- **NASK (Research and Academic Computer Network):** A national research institution under the Ministry of Digital Affairs, supporting SMEs through ICT R&D, cybersecurity standardization, and certification programs.
- **NCBR (National Centre for Research and Development):** Primarily responsible for funding R&D programs for medium-sized and large enterprises, rather than SMEs.
- **PFR (Polish Development Fund)** and **ARP (Industrial Development Agency)**: These agencies provide indirect investment and training programs for SME digital transformation. ARP also manages Special Economic Zones (SEZs).
- **BGK (Polish Development Bank):** A national development bank under the Ministry of Finance, offering loans and guarantees to support SMEs investing in digitalization and innovation.

However, due to the fragmented governance structure, systematic coordination and monitoring of individual implementing agencies' activities remain inefficient. This has made it difficult for the Polish government to assess the current status of SME digital transformation, understand the needs of SMEs, and evaluate the effectiveness of support programs. The dispersed support system also weakens partnerships among key innovation stakeholders, including SEZs, universities, research institutions, large corporations, and SMEs, ultimately slowing the pace of digital transformation.

Frequent government reorganizations due to political transitions further exacerbate this issue. The supervising ministries of implementing agencies frequently change, making it challenging to maintain policy continuity and consistency in SME digital transformation efforts.

Lastly, large firms play a crucial role in driving SME digital transformation through value chain integration across industrial sectors. However, in Poland, multinational corporations dominate over local large firms, reducing the incentives for domestic companies to support SME digital transformation actively.

3.2. Analysis of Relevant National Strategies for SMEs' Digital Transformation in Poland

Poland's digital transformation of SMEs has traditionally been regarded as part of broader national economic growth and productivity enhancement efforts, rather than as an independent policy focus. However, in recent years, there has been a gradual shift toward the development of dedicated national strategies specifically targeting the digital transformation of SMEs.

In this context, the Polish government is actively participating in the EU's Digital Decade Program. On October 22, 2024, the Council of Ministers adopted the National Action Plan for the Digital Decade, which serves as Poland's official implementation document for the EU's Road to a Digital Decade program. This plan aligns with the EU's common digital transformation goals, aiming for full implementation by 2030.

The National Action Plan outlines key national measures to accelerate enterprise digitalization and ensure the adoption of advanced digital technologies at the levels specified in the strategy. The primary targets include:

- 75% of Polish enterprises utilize at least medium-advanced and advanced cloud computing services.
- 35% of Polish enterprises are conducting data analytics.
- 34% of Polish enterprises are implementing artificial intelligence (AI) solutions.
- 90% of Polish SMEs are achieving at least a basic level of digital intensity.

To successfully achieve these KPIs, sector-specific national strategies are being developed by relevant ministries. Among them, the Digitalization Strategy 2035, established by the Ministry of Digital Affairs, presents a comprehensive roadmap for Poland's national digital transformation, covering key areas such as digital infrastructure, AI development, cybersecurity enhancement, and governance improvement.

The Digitalization Strategy 2035 explicitly designates SME digital transformation as a core policy priority, outlining several key objectives:

- Formulating mid-to-long-term policies and a policy coordination framework for SME digital transformation.
- Implementing various support programs to stimulate SME demand for digitalization.
- Identifying key industries where Poland has competitive advantages and targeting digital transformation initiatives in these sectors.
- Strengthening public-private partnerships and collaboration between large enterprises and SMEs.
- Enhancing cybersecurity capabilities for SMEs.

To ensure the effective implementation and monitoring of SME digital transformation goals outlined in the EU Digital Decade Program and Poland's Digitalization Strategy 2035, the Ministry of Economic Development and Technology is currently designing the "Digital Transformation Program for Enterprises." Following a public consultation process, the program is expected to be officially announced in 2026. This program aims to increase the share of Polish SMEs that have successfully achieved digital transformation. Key policy components will include:

- Establishment of an innovation ecosystem through efficient coordination between the government, public implementing agencies, and the private sector to facilitate the deployment of digital solutions for SMEs.
- Expansion of financial and business consulting support programs.
- Enhancement of monitoring and evaluation systems for digital transformation outcomes.

Poland allocates funds in line with the EU's Multiannual Financial Framework (MFF) and develops policies and strategies that reflect the EU's overarching priorities. The European Funds for Modern Economy (FENG) (2021-2027) and various sectoral digital transformation strategies have been implemented within the framework of EU cohesion policy, demonstrating Poland's commitment to advancing digitalization across economic and social sectors.

However, rather than placing a strong emphasis on the digital transformation of SMEs, these initiatives have primarily focused on broad-based policy measures aimed at strengthening the overall digital capabilities of key stakeholders involved in transformation. This approach is also evident in Poland's utilization of funds from the Recovery and Resilience Facility (RRF) and the EU's 2021-2027 funding programs.

The Polish Ministry of Funds and Regional Policy is responsible for managing these funds, allocating them to implementing agencies through cohesion policies and tailored strategies. Notably, among the eight thematic areas designated under the 2021-2027 EU funding framework, more than half include provisions for business digital transformation, digital infrastructure expansion, and the enhancement of SME digital competitiveness.

<Table 1-3> Major National Policies for SME Digitalization in Poland

#	Policy / Program	Key Objectives in the field of SME Digitalization	Responsible Organization	Enacted Year
1	National Action Plan for the Digital Decade	• Achieving a basic level of digital technology adoption rate of over 90% for SMEs in the EU. • Increasing the participation of SMEs using the cloud, Big Data, and AI up to certain percentages nationally.	Council of Ministers	2024
2	Digitalization Strategy 2035	• Developing a national digitalization strategy for SMEs, ensuring clear goals, monitoring progress, and identifying technological needs • Promoting the use of Industry 4.0 technologies among SMEs, by supporting collaboration with technical institutions and establishing online knowledge-sharing platforms • Integrating SMEs into digital supply chains, ensuring that large enterprises' digital transformation efforts support SME inclusion • Strengthening SME cybersecurity awareness, providing training, certification systems, and linking cybersecurity compliance to insurance benefits	Ministry of Digital Affairs	In Progress (Public Consultation Phase)
3	Digital Transformation Program for Enterprises	• Increasing the proportion of digitally enabled enterprises in Poland, particularly within the SME sector, in alignment with the objectives of the Digital Decade. • Enhancing the efficiency of public instruments used to support and finance the digital transformation of enterprises. • Strengthening coordination within the business digitalization support ecosystem, while improving the quality of business consulting services and the competencies of public administration. • Ensuring broad and equitable access to comprehensive information on financing tools for digital transformation and provide effective support in accessing them. • Establishing continuous monitoring mechanisms for the implementation and effectiveness of digitalization support instruments.	Ministry of Economic Development and Technology	In Progress
4	Medium-Term Fiscal-Structural Plan for the Years 2025-2028	• Improving economic competitiveness by reforming industrial property rights and supporting SMEs in public procurement processes. • Enhancing digital transformation, including increasing high-speed internet coverage and promoting cloud computing and AI adoption in businesses.	Council of Ministers	2024
5	Cybersecurity Strategy of the Republic of Poland for 2025–2029	• To be Published	Ministry of Digital Affairs	In Progress (Public Consultation Phase)
6	Digital Competence Development Program	• Focusing on the development of digital competences for all citizens. • Indirect support for SMEs by creating a digitally competent workforce.	Ministry of Digital Affairs	2023
7	Productivity Strategy 2030 (2022)	• Improving the position of human capital from 22nd place in 2020 to 17th place by 2030 (DESI). • Increasing the number of robots per 10000 working in industry from 46 in 2019 to 135 in 2030. • Maintaining the position in the integration of digital technology at 25th place, to improve to 22nd place by 2030 (DESI). • Increasing the share of companies using Big Data from 8 % in 2020 to 16 % in 2030.	Council of Ministers	2022

#	Policy / Program	Key Objectives in the field of SME Digitalization	Responsible Organization	Enacted Year
8	National Recovery and Resilience Plan (2021-2027)	• Increasing the use of digital technologies in the public sector, the economy and society. • Improving access to high-speed internet. • Development and consolidation of e-services through appropriate reforms.	Ministry of Development Fund and Regional Policy	2021
9	Industrial Policy of Poland	• Digitizing industrial activity, from product design to changing business models. • Securing Europe's and Poland's production capacity, including pharmaceutical and medical devices. • Locating industrial production by shortening supply chains and diversifying sources of raw materials and intermediate products to ensure Europe's production stability.	Ministry of Economic Development, Labour and Technology	2021
10	Policy for the Development of Artificial Intelligence in Poland from 2020	• Supporting SMEs in digitalizing for better Competitiveness and efficiency. • Lack of specific goals for SMEs, but the policy supports their innovation through AI. • The overall objective is to stimulate SMEs to benefit from AI technologies.	Council of Ministers	2020

Note: Modified and updated by the author based on information from KDI (2023).
Source: Author (2025).

<Table 1-4> EU Cohesion Policy Funds Related to SME Digitalization in Poland (2021–2027)

#	Policy / Program	Key Objectives in the field of SME Digitalization	Budget (EUR)
1	European Funds for Modern Economy (EFME) (2021-2027)	• Encouraging entrepreneurs, mainly SMEs, to implement measures related to the green and digital transformation. • Raising awareness among businesses of the practical application of digital solutions. • Supporting research, innovation, and digitalization through a standalone fund separate from the MMF EU Fund (2021-2027). • Facilitating R&D, digital transformation, and innovation for SMEs. • Promoting technology transfer between enterprises to enhance competitiveness. • Assisting businesses in energy transition to improve sustainability. • Providing technical support for corporate participation, management, and promotion.	7,9 billion
2	European Funds for Digital Development (EFDD) (2021-2027)	• Expanding ultra-high-speed broadband internet and advanced e-services to enhance connectivity and digital accessibility. • Expanding financial support for projects for public e-services for citizens and enterprises • Strengthening cybersecurity and improving digital competence to ensure a secure and digitally skilled society.	2 billion
3	European Funds for Eastern Poland (EFEP)	• Enhancing the competitiveness of Eastern Poland by supporting business development and innovation. • Improving urban development in key cities within the Eastern region. • Providing financial support to major cities and businesses located in Eastern Poland.	2,65 billion
4	European funds for Regional Operational Programs (2021-2027)	• Implementation of digital technologies to improve operational processes. • Development of skills and implementation of technologies to increase the digital security of businesses. • Investing in education and training for employees to understand and make efficient use of new digital tools, which contribute to the company's productivity and innovation.	33.54 billion (16 voivodeships)

Note: Modified and updated by the author based on information from KDI (2023).
Source: Author (2025).

3.3. Support Programs for the Digital Transformation of Polish SMEs

Most support programs for the digital transformation of SMEs in Poland are implemented as part of EU-funded initiatives and are broadly categorized into advisory services and financial support.

In terms of advisory services, the flagship programs include European Digital Innovation Hubs (EDIHs) and Testing and Experimentation Facilities for AI (TEF AI). Financial support programs available to SMEs include Smart Pathway, Dig-IT—Digital Transformation, Guarantee Fund, and Technology Credit. Additionally, the Innopoint and STEP programs offer consulting services to help SMEs successfully access EU funding schemes. All these programs are funded under the Digital Europe Program and the European Funds for a Modern Economy 2021–2027 (FENG). The Ministry of Funds and Regional Policy supervises them.

<Table 1-5> Major SME Digitalization Support Programs in Poland

#	Category	Program Name	Implementing Agency
1	Advisory Services	European Digital Innovation Hubs (EDIHs)	PARP
2		Testing and Experimentation Facilities for AI (TEF AI)	EU
3	Financial Support	Smart Pathway	NCBR
4		Dig-IT—Digital Transformation	ARP
5		Technology Credit	BGK

Source: Author (2025).

3.3.1. Advisory Services

3.3.1.1 European Digital Innovation Hubs (EDIHs)

Polish EDIHs are regionally based digital innovation hubs established under the Digital Europe Program (DEP) of the European Union. Their main role is to support SMEs in adopting and utilizing digital technologies effectively. EDIHs allow companies to "test before invest," offering a one-stop-shop model for consulting, capability building, and technical validation services.

As of 2024, a total of nine EDIHs have been established across Poland since the program began in January 2023. Each hub specializes in a specific set of technologies (e.g., AI, IoT, robotics, cybersecurity, HPC), determined based on the region's industrial structure and smart specialization strategies (S3). Hubs are typically organized as consortia composed of over ten institutions, including universities, research institutes, private companies, and local governments.

EDIHs provide key services such as (1) digital maturity assessments, (2) access to testing environments for new technologies, (3) expert consultations and customized PoC support, (4) training and upskilling programs, and (5) investment advisory and public funding navigation. Most services are free or subsidized through EU and national funding, reducing the barrier to digital adoption. For instance, hub4industry EDIH, located in Kraków, not only the Kraków Technology Park but also research institutions such as AGH University of Science and Technology and the Kraków

Institute of Technology, together with large technology providers like T-Mobile and ASTOR, are jointly participating to carry out projects that support the digital transformation of SMEs.

Beyond service provision, EDIHs aim to act as long-term innovation partners in regional ecosystems. They engage with local industry clusters, startups, and municipalities to conduct demand assessments and develop practice-based joint projects. Hubs are also networked at the national level, coordinated by PARP.

EDIHs are closely linked with the EU's Digital Single Market strategy. As part of the pan-European EDIH network, Polish hubs collaborate with counterparts in other EU countries to share technologies, co-host workshops, and align with European regulatory and technical standards. The effective implementation of this integration enables Polish firms to achieve technological interoperability and enhance their credibility throughout the EU.

However, current EDIH programs face challenges. First, after the initial EU funding ends, many hubs lack sustainable revenue models, especially in smaller cities where matching national funds are not guaranteed. Second, variation in technical focus across regions leads to disparities in service quality. Some hubs are heavily skewed toward traditional industrial digitalization, which limits their support for more advanced technologies, such as AI. Lastly, a key weakness of EDIHs lies in their limited integration with other national support schemes; in some cases, service overlap further undermines synergy. This constraint results in non-standardized services and insufficient promotion among SMEs requiring support.

3.3.1.2 Testing and Experimentation Facilities for AI (TEF AI)

Testing and Experimentation Facilities for Artificial Intelligence (TEF AI), in which Poland participates, is a flagship initiative under the Digital Europe Program. At the same time, complementary support can be accessed via FENG. Its goal is to support the large-scale testing and validation of trustworthy and secure AI solutions. TEFs serve as advanced testbeds to verify AI technologies in real-world environments, beyond the R&D stage (Technology Readiness Level 5–9), just prior to market introduction.

TEFs are divided into four thematic areas: (1) Smart Cities and Communities (Citcom.AI), (2) Healthcare (TEF-Health), (3) Agriculture and Food (AgrifoodTEF), and (4) Manufacturing (AI-MATTERS). Each project is allocated between EUR 40–60 million in funding and is operated by multinational consortia over five years starting in 2023.

Poland is a key partner in Citcom.AI and AgrifoodTEF. In Citcom.AI, AI applications for smart mobility, energy, and urban services are being tested in Warsaw and other large cities. In AgrifoodTEF, drone-based crop monitoring and AI-enabled livestock management systems are being piloted. These projects align strategically with Poland's regional industrial priorities.

Core services of TEF include: (1) large-scale testing of AI in real conditions, (2) validation against EU AI Act requirements on transparency and trust, (3) evaluation of ethical, legal, and technical compliance, and (4) sandbox experiments in collaboration with sectoral regulators. Polish institutions participating in TEFs provide AI firms with advisory services, datasets, and certification assistance to facilitate EU-compliant commercialization.

TEFs aim not only to serve as testing platforms but also to shape standards and regulatory frameworks across the EU AI ecosystem. Participating firms gain access to cross-border test environments and contribute to EU-level policy feedback. Poland benefits from internationalizing its tech sector and positioning itself as a hub for AI trustworthiness certification.

Nevertheless, TEF is a multinational program with participation constrained by national priorities. Poland currently engages in only two of the four TEF domains, limiting full access. Moreover, since TEF focuses on regulatory validation for pre-commercial AI technologies, it may not align with the short-term commercial goals of most SMEs.

3.3.2. Financial Support

3.3.2.1 SMART Pathway

The SMART Pathway is a flagship R&D and innovation support scheme under Poland's FENG (European Funds for a Modern Economy 2021–2027), administered by the National Centre for Research and Development (NCBR). It succeeds the 2014–2020 Smart Growth Program and aims to strengthen the competitiveness of Polish firms through transformative innovation.

The program supports both SMEs and large enterprises; however, applicants must present projects with high national-level innovation potential, beyond incremental improvements or standard IT deployments. Game-changing technologies are emphasized.

SMART Pathway offers integrated project packages built from mandatory and optional modules. Mandatory modules include R&D and implementation (commercialization); proposals must include at least one. Up to five optional modules can be added, including R&D infrastructure, digital transformation, green transition, workforce development, and international expansion. This modular design allows firms to tailor integrated strategies across the innovation lifecycle.

With a total budget of approximately EUR 4.3 billion (PLN 20 billion), SMART Pathway is the largest innovation grant scheme in Poland and among the largest in the EU. Grant intensities vary by module, company size, and region; however, most support is typically direct subsidy-based. Some modules also offer financial instruments or indirect support.

The second call for proposals in March 2025 allocated PLN 1.3 billion. SME applicants are encouraged to form consortia with large firms, universities, or research centers to promote resource sharing and ecosystem development.

Strengths of SMART Pathway include its scale and its role in fostering collaboration among innovation stakeholders. However, the program presents high barriers for SMEs: large firms often outcompete SME consortia due to superior capacity, and the required innovation level may exceed what is realistic for SMEs pursuing local or internal improvements. The complexity of application design, requiring integrated multi-module plans, also burdens firms with limited in-house expertise.

3.3.2.2 Dig-IT—Digital Transformation

Dig-IT (Digital Transformation of Polish SMEs) is a financial support program under FENG, managed by the Polish Industrial Development Agency (ARP S.A.). It targets SMEs in the industrial processing or production service sector, helping them implement digital technologies such as process automation, data digitization, AI, and cloud solutions.

Subsequently, grants ranging from EUR 40,000 to EUR 200,000 per firm are provided, covering up to 50% of eligible project costs. An eligible project includes the purchase and implementation of software, machines and devices, consumables, and training in the field of digital transformation. Additional activities include seminars and workshops aimed at disseminating best practices, as well as research initiatives to analyze the impact of digital transformation on enterprises.

Scheduled to launch in the fourth quarter of 2025, the program aims to support 400 SMEs to raise their digital maturity level. Additionally, the project aims to enhance the digital transformation capabilities of 2,000 SME employees and promote the importance of digital transformation within the SME ecosystem.

Since the DIG IT project has not yet been fully launched, the detailed operational structure of the support program remains to be specified. However, as the program currently targets only the manufacturing sector, it will likely need to expand in the long term to support the digital transformation of the service sector. In addition, SMEs participating in DIG-IT are expected to independently purchase and utilize digital transformation equipment and software after receiving grants. To enhance the efficiency of grant support, it would be worth considering the involvement of technology providers that supply digital transformation solutions, thereby enabling tailored matching support.

3.3.2.3 Technology Credit

Technology Credit is a grant-linked loan support program managed by Poland's national development bank (BGK). It targets SMEs that take commercial bank loans to implement or commercialize new technologies. If project conditions are met, BGK repays part of the principal using EU funds—a mechanism referred to as the "technology bonus."

As of 2023, the program had a budget of PLN 763 million (approximately EUR 160 million) and had awarded bonuses to over 270 companies.

To qualify, firms must introduce new technology—either developed in-house or acquired externally—and use it to offer new or significantly improved products/services. Upon successful completion, BGK reimburses a portion of the bank loan, thereby reducing the financial burden.

Eligible expenses include: (1) acquisition of land and non-residential property (up to 10% of eligible costs), (2) machinery and fixed assets, (3) construction and materials (up to 50%), (4) IP assets (patents, licenses, expertise), (5) lease payments on fixed assets, (6) external consulting and technical documentation (up to 50%, maximum of EUR 2 million), and (7) patent-related costs (up to 50%, maximum of PLN 500,000).

The process begins with loan approval from a commercial bank. The SME then submits a technology bonus application to BGK. If BGK verifies successful innovation outcomes, it transfers the grant to the bank to reduce the loan balance.

The program reduces the cost of innovation by integrating EU-private financing and incentivizes performance-based investment. However, requiring loan approval excludes financially weak SMEs, and the bonus is only paid after project success—meaning SMEs must bear all upfront risk.

3.4. Main Challenges and Policy Implications

Based on a comprehensive analysis of the digital intensity of Polish SMEs, as well as government policies and support programs, the key challenges hindering digital transformation and the corresponding policy implications can be summarized as follows:

3.4.1. Financial Burden of Adopting Digital Technologies

As highlighted in prior empirical surveys, approximately one-third of Polish SMEs report not recognizing the need to adopt digital technologies. A major reason for this is the high perceived cost of digital adoption. While nearly 93% of SMEs express willingness to adopt digital technologies, survey results indicate that they must cover approximately 97% of the adoption cost from their own resources. Only 9% of firms reported having received any form of public support (KPMG, 2024).

As a result, many SMEs perceive digital transformation not as an opportunity for innovation but as a potential financial burden or risk. This perception is especially prevalent among micro-enterprises, which comprise approximately 97% of Polish SMEs and typically employ fewer than nine people, due to their limited access to financing.

Current government support programs, such as the Technology Credit scheme, mainly offer retrospective grants rather than low-interest loans, thereby discouraging participation from SMEs that are willing to invest but are constrained by repayment risks. Moreover, grant-based programs like EDIH and Innovation Vouchers are tied to EU funding cycles, and support is often discontinued once EU project periods end, thereby limiting access for SMEs that are already burdened by costs.

In this context, financial support schemes need to focus more on enhancing access to affordable financing for innovation-oriented SMEs, such as by expanding low-interest loan offerings.

3.4.2. Limited Coordination of Public and Private Institutions

Although various ministries and implementing agencies are involved in SME digitalization policy, their roles and responsibilities remain unclear, and inter-agency collaboration is limited. This institutional fragmentation undermines the effectiveness and coherence of support programs.

To address this issue, the Ministry of Economic Development and Technology is seeking to enhance its coordinating role through the "Digital Transformation Program for Enterprises." Given that SME support in Poland is broadly divided between financial support and advisory services, the Ministry must establish coordinated linkages between advisory programs led by institutions such as PARP, NCBR, NASK, and PFR, and financial instruments managed by BGK. In addition, the above program should closely cooperate with the MFiPR and the 16 Marshall Offices, contributing to the implementation and monitoring of tailored Regional Operational Programs that take into account the state of digital transformation across industries in each voivodeship.

In addition, policies should aim to foster collaboration between SMEs and large firms or technology providers. Since technology providers are better positioned to identify the digital solutions needed by SMEs, support programs that are based on SME-technology provider consortia can enable more tailored assistance. For such models to be effective, the government should also promote the development of a national base of digital technology providers that specialize in working with SMEs.

3.4.3. Need for More Customized Support Programs for SMEs

Most current SME support programs in Poland are generic and not sufficiently tailored to the specific industrial sectors or the digital maturity levels of individual firms. However, the types and levels of digital technologies needed by SMEs vary significantly depending on these factors. To address this gap, it is crucial to develop customized support programs that reflect the unique characteristics and needs of different SME groups.

Effective program design requires a robust evidence base. Poland should therefore establish a regular national monitoring system—such as an annual survey on SME digitalization—to assess the digital readiness, adoption barriers, and sector-specific demands of SMEs.

Furthermore, to accelerate the adoption of emerging digital technologies across diverse industries, it is vital to actively introduce and scale up regulatory sandbox frameworks tailored to sector-specific needs. At present, regulatory sandboxes in Poland are limited to the fintech sector. In the future, the scope should be broadened to include areas such as artificial intelligence and smart manufacturing, thereby establishing an institutional foundation for technology piloting and commercialization.

4. Benchmarking Best Policy Practices for SME Digital Transformation and Digital Ecosystem Development in Korea

The digital transformation (DX) of SMEs is a key driver of national competitiveness, innovation, and productivity. For Poland, where the SME sector plays a dominant role in the economy but faces chronic issues such as limited digital capabilities, fragmented governance, and slow technology adoption, identifying effective international policy benchmarks is crucial. Korea presents a compelling model, having achieved significant results in SME digitalization through an orchestrated mix of regulatory, technological, and market-based interventions.

This section aims to provide an in-depth review of Korea's leading policies that enabled the digital transformation of SMEs. The policies examined include the Regulatory Sandbox framework, the Smart Manufacturing Innovation Strategy, the Government Software Procurement Policy for SMEs, and private sector-led Digital Transformation Platforms, such as KoDTi. The Korean experience can offer practical lessons and insights to inform the design of Poland's mid- to long-term strategies under the Digital Decade 2030 and the Digitalization Strategy 2035.

4.1. Policy Dimensions Supporting SME Digital Transformation

This section outlines key international policy dimensions that support SME digital transformation, drawing on the OECD's (2023) analytical framework. It identifies six policy pillars—regulatory frameworks, market conditions, digital infrastructure, access to finance, skills development, and innovation support—and highlights representative programs implemented across OECD countries to inform Poland's policy design.

1) **Institutional and Regulatory Frameworks:** Countries have increasingly turned to regulatory innovation and ethics-based toolkits to guide SME digital transformation. Denmark's Digital Ethics Compass supports SMEs in implementing responsible data and design practices in the fintech and mobility sectors. Finland's AuroraAI connects public and private services via ethical AI platforms, promoting seamless access for SMEs. At the regional level, the EU General Data Protection Regulation (GDPR) plays a crucial role in ensuring secure data usage and compliance with privacy regulations (OECD, 2023). In Korea, a comprehensive legislative framework has been established to support the digital transformation of SMEs, guided by policy-specific statutes enacted or amended in recent years. These laws serve as pillars for enabling innovation, promoting convergence, and ensuring effective institutional coordination. The Act on Promotion of Smart Manufacturing Innovation for Small and Medium Enterprises (2023), proposed by the Ministry of SMEs and Startups (MSS), stipulates the implementation framework for the digital transformation of small and medium-sized manufacturers. It outlines detailed support mechanisms for the construction of smart factories and digitized production systems. The Act on the Protection and Support of Small Business Owners (2023), also led by

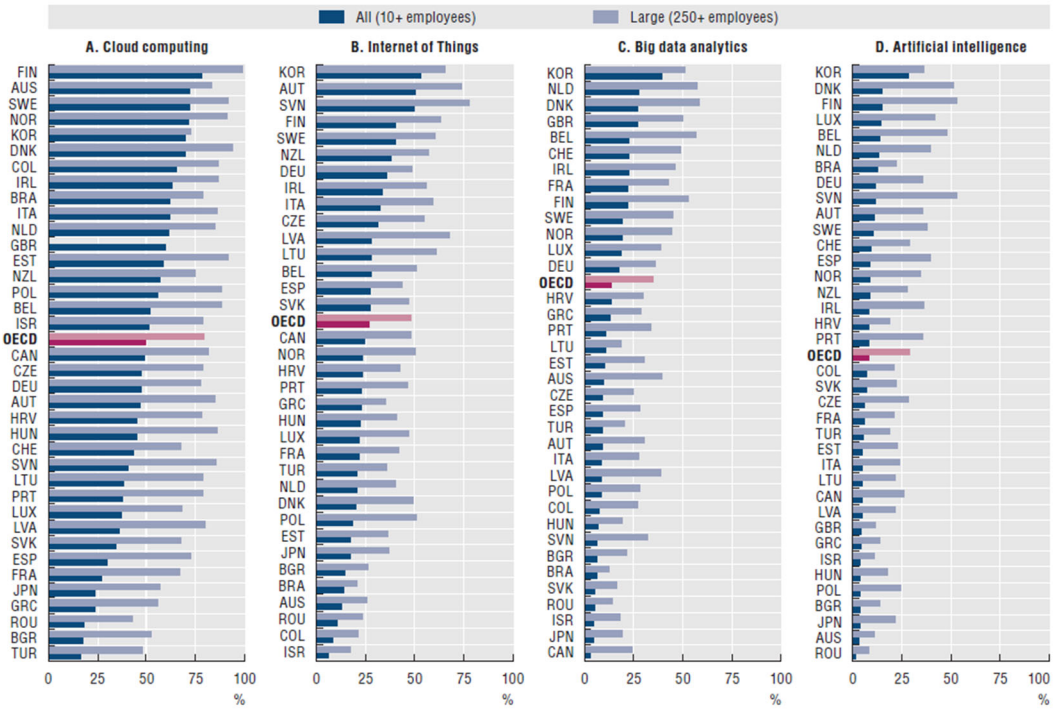
MSS, provides the legal foundation for digital transformation among microenterprises. It supports innovation dissemination projects, establishes dedicated organizations, and introduces a Digital Transformation Advisory Committee to coordinate policy execution. The Special Act on Promotion of Information and Communications Technology and Vitalization of Convergence (2013), proposed by the Ministry of Science and ICT (MSIT), emphasizes regulatory reform, talent cultivation, and support for technology convergence and venture creation. It lays a foundation for digital innovation ecosystems across industries. The Industrial Digital Transformation Promotion Act (2022), managed by the Ministry of Trade, Industry and Energy (MOTIE), promotes large-scale industrial digital transformation through the formation of an Industrial Digital Transformation Committee. It also supports regulatory reform, selection of strategic digital innovation projects, and the development of a skilled workforce. The Small and Medium Enterprise Cooperatives Act (2023) includes amendments to facilitate the use of digital transformation tools and data-sharing systems among SMEs and small businesses, encouraging collaborative innovation models.

These laws demonstrate Korea's multi-ministerial commitment to digital policy design, enabling coordinated actions among MSS, MOTIE, and MSIT. This legislative ecosystem reflects best practices in agile governance and cross-sector alignment—elements that could be instructive for Poland as it refines its own regulatory frameworks to support SME digitalization.

2) **Market Conditions and Competition Environment:** Germany's GWB Digitization Act addresses the digital dominance of platforms by banning self-preferencing and other anti-competitive behavior. Italy's Digital Export Bonus offers EUR 4,000 grants to SMEs investing in digital tools to enhance their internationalization. Austria's Connecting Services program promotes innovation and international collaboration by matching SMEs with multinationals and investors. These initiatives help mitigate digital market concentration and create opportunities for fairer competition (OECD, 2023).

3) **Digital Infrastructure:** National platforms and public infrastructure play a pivotal role in enabling SME digital adoption. Denmark's national CSIRT enhances cybersecurity for all firms, including SMEs, through the use of scanning tools and support for GDPR compliance. These efforts are particularly crucial in the context of the rising cyber threats that have emerged since the COVID-19 pandemic. Investment in trustworthy and scalable infrastructure remains a common priority among OECD governments (OECD, 2023).

[Figure 1-10] Adoption of Data-Driven Technology by Firms (2023)

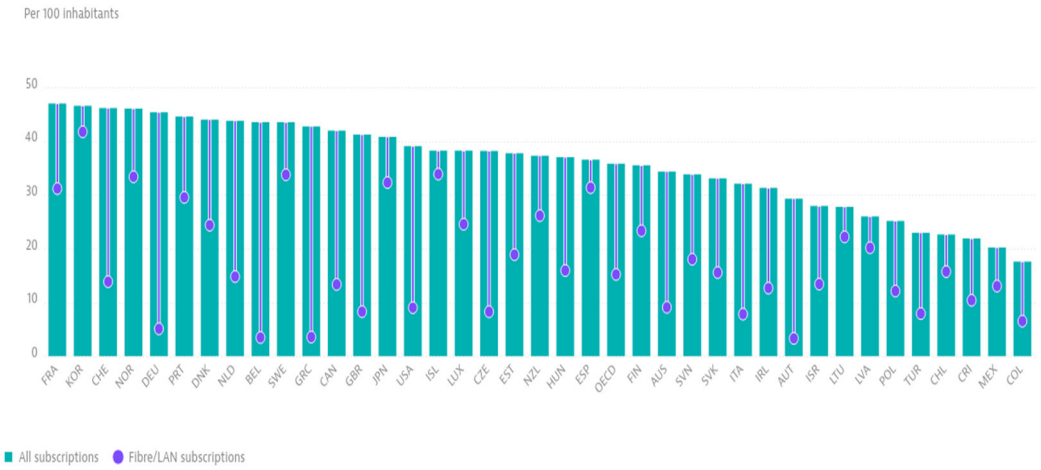


Source: OECD (2024).

The adoption of key digital technologies—Cloud Computing, Internet of Things (IoT), Big Data Analytics, and Artificial Intelligence (AI)—varies significantly across countries and between large firms and SMEs, as is shown in [Figure 1-10]. In the graphs, the dark blue bars represent adoption by large firms (with 250 or more employees), while the light blue bars indicate adoption by all firms (with 10 or more employees). The difference between these two serves as a proxy for SME adoption: a smaller gap implies that SMEs are adopting digital technologies at rates similar to those of large enterprises. Korea shows relatively high adoption rates of core digital technologies among businesses, particularly in relation to SMEs. According to OECD data, Korea ranks at or near the top among member countries in Cloud Computing, Internet of Things (IoT), Big Data Analytics, and Artificial Intelligence (AI). In each of these categories, the gap between adoption rates of large firms and all firms (including SMEs) is relatively small, suggesting that SMEs participate more actively in digital adoption compared to the OECD average. For example, Korea has the highest reported adoption of IoT and AI technologies, with minimal differences in adoption rates between firm sizes. Adoption rates for Big Data Analytics and Cloud Computing are also relatively high across Korean firms, which may reflect the influence of national programs such as smart factory initiatives, digital training, and data-sharing platforms. In contrast, Poland reports lower overall adoption rates in all four technology categories, with wider gaps between large firms and SMEs. While cloud adoption is moderate, SME engagement in IoT, Big Data Analytics, and AI remains limited. The OECD average indicates a general trend where digital technologies are more commonly adopted by large enterprises, with lower diffusion among smaller firms (OECD, 2024).

These observations highlight the importance of designing digital policy frameworks that account for firm size and that address specific barriers faced by SMEs—such as access to infrastructure, skills, and financing. Comparative data can support Poland in identifying policy areas where targeted interventions may be needed to expand SME participation in digital transformation.

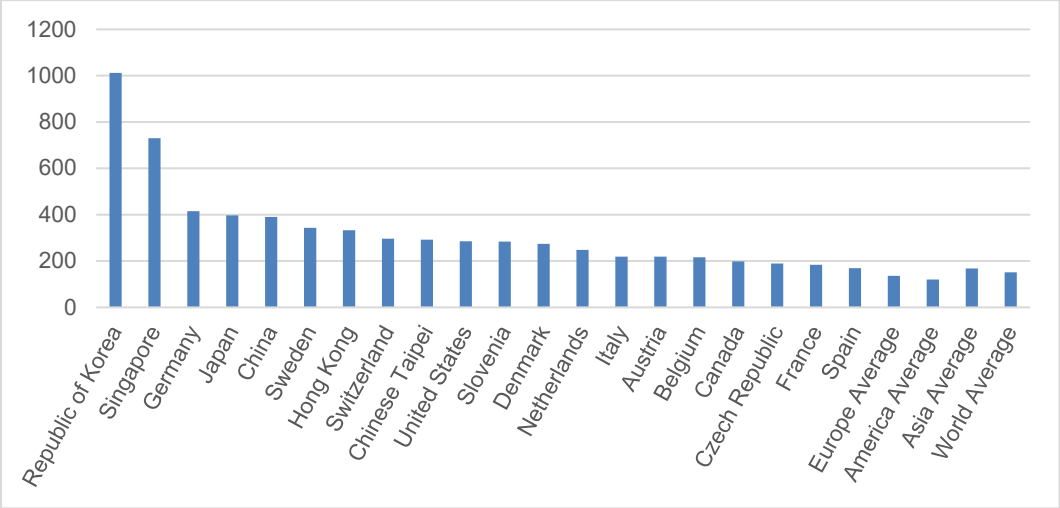
[Figure 1-11] Fixed Broadband, Fiber/LAN Subscriptions Per 100 Inhabitants (2023 Q4)



Source: OECD (2025).

Korea's relatively high adoption of digital technologies across firms, including SMEs, is supported by a strong foundation in digital infrastructure. As of Q4 2023, Korea ranks second among OECD countries in fixed broadband subscriptions per 100 inhabitants and shows one of the highest shares of fiber/LAN subscriptions. This extensive broadband penetration, especially through high-speed fiber networks, provides a reliable and scalable foundation for businesses of all sizes to adopt cloud computing, big data analytics, and other advanced digital tools.

[Figure 1-12] Industrial Robots for 10,000 Manufacturing Employees (2022)



Source: International Federation of Robotics (2024).

In addition to connectivity, Korea also leads globally in industrial robot density, with 1,012 robots per 10,000 manufacturing employees. This figure far exceeds those of other industrialized nations, such as Germany (415), Japan (397), and the United States (285). While robot density itself is not an infrastructure input, it reflects the maturity of Korea's digital manufacturing ecosystem and the degree to which advanced technologies have been integrated into production. This alignment of

physical infrastructure (such as broadband networks) with industrial technology adoption contributes to Korea's broader digital transformation outcomes (International Federation of Robotics, 2024).

These indicators suggest that Korea's policy efforts to expand both digital infrastructure and the deployment of advanced technology have contributed significantly to the widespread adoption of digital tools in the private sector. For countries like Poland, expanding broadband infrastructure and supporting industrial automation could serve as complementary strategies to enhance SME digital readiness and innovation capacity.

4) **Financial Accessibility:** Dedicated funding mechanisms have been developed to close the digital investment gap. Broader EU-level instruments complement Italy's Digital Export Bonus and Austria's innovation matching funds. These schemes reduce risk and stimulate SME participation in digital markets. The inclusion of non-repayable and hybrid finance options reflects a growing awareness of SME liquidity constraints and the need for long-term capital (OECD, 2023).

5) **Digital Skills Development:** Denmark, Slovenia, and Portugal exemplify countries that integrate financial and educational support to build SME digital competencies. While Denmark focuses on GDPR readiness and cybersecurity, Slovenia's Voucher for Raising Digital Competencies and Portugal's Digital Training programs provide accessible and certified learning pathways for SME staff and managers (OECD, 2023).

6) **Access to Innovation Assets:** Innovation platforms like Australia's Digital Solutions Program and France's France Num are instrumental in facilitating access to digital tools, consultants, and markets. These services help SMEs to adopt new technologies and integrate them into operations. The Netherlands' Commit2Data and Korea's KoDTi further demonstrate how public-private consortia can provide data access, sector-specific toolkits, and innovation support across industries (OECD, 2023).

These international programs offer valuable lessons for Poland as it refines its digital transformation policies for SMEs. Emulating cross-sector collaboration, ethical design, and targeted finance and training can boost SME productivity and resilience in alignment with the EU's Digital Decade 2030 goals.

4.2. In-Depth Review of Korea's Leading Policies Enabling SME Digital Transformation

4.2.1. Korea's Regulatory Sandbox: Enabling Innovation through Legal Flexibility

In January 2019, Korea launched its regulatory sandbox to shift the regulatory paradigm and support the development of emerging industries and innovative technologies. The system allows businesses to introduce and test new products and services by temporarily suspending or exempting them from existing regulations—either fully or partially—under defined conditions such as time, location, and scale. This enables early market entry and promotes data-driven regulatory reform. While the concept originated in the United Kingdom in 2016, primarily in the financial sector, Korea

has expanded its scope to encompass all innovative industries (Regulatory Reform Committee, 2023).

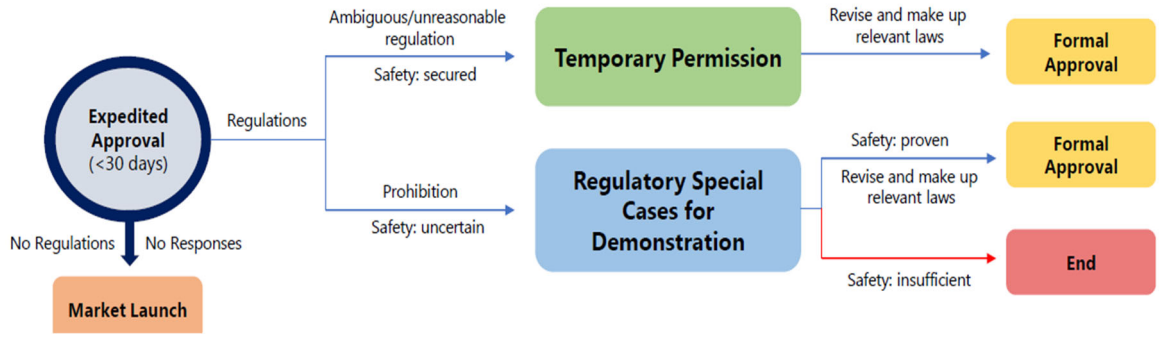
The Korean sandbox system consists of three key tracks:

(1) **Regulatory Special Cases for Demonstration:** Allows businesses to test and verify new technologies in areas where regulations are ambiguous or prohibitively restrictive, with relevant laws revised based on the results.

(2) **Expedited Approval:** Provides prompt confirmation on the existence of applicable regulations. If no response is received within 30 days, the product may proceed under the assumption that no relevant regulations exist.

(3) **Temporary Permission:** Grants conditional market entry for products facing unclear or unreasonable regulations, assuming safety is secured. Relevant laws are then revised based on operational outcomes (European Chamber of Commerce in Korea, 2023).

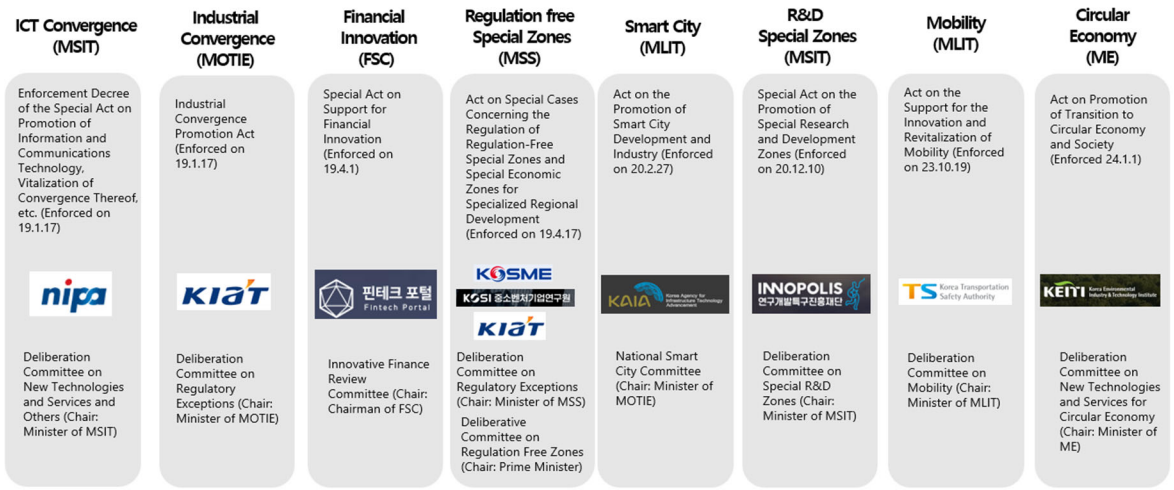
[Figure 1-13] Korea's Regulatory Reform Through Sandbox



Source: European Chamber of Commerce in Korea (2020).

To address concerns related to public safety, health, and environmental impact, Korea's sandbox system includes robust safeguards. Regulatory exemptions can be restricted or revoked if significant risks are identified or issues arise during implementation. Liability insurance is required in advance to ensure compensation, and the burden of proof for intent or negligence is shifted from the victim to the business operator (Regulatory Reform Committee, 2023).

[Figure 1-14] Domains, Managing Ministries and Agencies of Regulatory Sandbox



Source: Regulatory Reform Committee (2023).

Korea's regulatory sandbox was first launched in January 2019 in the fields of ICT convergence and industrial convergence, followed by the financial innovation and regulation-free special zones in April 2019. Since then, the program has gradually expanded to cover smart cities (February 2020), R&D special zones (December 2020), mobility (October 2023), and the circular economy (January 2024), bringing the total to eight operational domains.

The regulatory sandbox system is managed through a collaborative framework among eight ministries, coordinated by the Office for Government Policy Coordination (OPC), which is responsible for overall planning and operation. Each ministry oversees sandbox implementation within its domain, in accordance with the eight corresponding legal acts:

(1) **ICT Convergence (MSIT):** Governed by the Enforcement Decree of the Special Act on Promotion of Information and Communications Technology, supported by NIPA and reviewed by the Deliberation Committee on Technologies and Services of New Industries (Chair: Minister of Science and ICT).

(2) **Industrial Convergence (MOTIE):** Based on the Industrial Convergence Promotion Act, supported by KIAT and reviewed by the Deliberation Committee on Regulatory Exceptions (Chair: Minister of MOTIE).

(3) **Financial Innovation (FSC):** Under the Special Act on Financial Innovation Support, supported by the Fintech Portal and reviewed by the Innovative Finance Review Committee (Chair: Chairman of FSC).

(4) **Regulation-Free Special Zones (MSS):** Governed by the Act on Special Cases Concerning the Establishment and Operation of Regulation-Free Zones, supported by KOSME and KIAT. Reviewed by the Deliberation Committee on Regulatory Exceptions (Chair: Minister of MSS) and the Deliberation Committee on Regulation-Free Zones (Chair: Prime Minister).

(5) **Smart City (MOLIT):** Based on the Act on the Promotion of Smart City Development and Industry, supported by KAIA and reviewed by the National Smart City Committee (Chair: Minister of MOLIT).

(6) **R&D Special Zones (MSIT):** Under the Special Act on the Promotion of Special Research and Development Zones, supported by INNOPOLIS and reviewed by the Deliberation Committee on R&D Special Zones (Chair: Minister of MSIT).

(7) **Mobility (MOLIT):** Governed by the Act on the Support for the Innovation and Revitalization of Mobility, supported by TS (Korea Transportation Safety Authority) and reviewed by the Deliberation Committee on Mobility (Chair: Minister of MOLIT).

(8) **Circular Economy (ME):** Based on the Act on Promotion of Transition to Circular Economy and Society, supported by KETI and reviewed by the Deliberation Committee on New Technologies and Services for Circular Economy (Chair: Minister of ME).

To address cross-ministerial issues or conflicts, the Regulatory Sandbox Related Ministries Task Force (TF), led by the Office for Government Policy Coordination, serves as a platform for coordination and resolution. This ensures that the system remains coherent and adaptable across sectors while leveraging the specialized expertise of each ministry.

As of 2023, Korea's regulatory sandbox program has approved a total of 1,139 projects across various types, sectors, ministries, and firm sizes. The majority of these approvals, 973 cases or 85%, were categorized as pilot programs, allowing companies to test new products and services under temporary regulatory exemptions. Another 111 cases (10%) were granted as temporary permits, which enable market entry for products facing ambiguous or outdated regulations, provided their safety is verified. Additionally, 55 cases (5%) were classified as proactive interpretations, in which regulatory authorities provided clarifications on whether existing rules applied to specific innovations. Annual approval numbers have grown steadily, starting from 195 in 2019 and reaching 279 by 2023, indicating a consistent institutional commitment to regulatory reform and innovation (Regulatory Reform Commission, 2023).

<Table 1-6> Regulatory Sandbox Approval Statistics by Year and Types

Total	2019	2020	2021	2022	2023	Pilot Program	Temporary Permit	Proactive Interpretation
1,139	195	209	228	228	279	973 (85%)	111 (10%)	55 (5%)

Source: Regulatory Reform Committee (2023).

In terms of sectoral distribution, the industrial convergence field accounts for the largest share, with 487 approvals, representing 43% of the total. This is followed by financial innovation, with 293 approvals (26%), and ICT convergence, with 200 (18%). Other sectors, including regulation-free special zones (84 approvals, 7%), smart cities (51 approvals, 4%), and R&D special zones (24 approvals, 2%), have shown gradual but steady participation. The expansion of the sandbox into

newer sectors demonstrates its flexibility and broad applicability across different industries (Regulatory Reform Commission, 2023).

<Table 1-7> Regulatory Sandbox Approval Statistics by Domains

Total	Industrial Convergence	Financial Innovation	ICT Convergence	Regulation Free Special Zones	Smart City	R&D Special Zones
1,139	487 (43%)	293 (26%)	200 (18%)	84 (7%)	51 (4%)	24 (2%)

Source: Regulatory Reform Committee (2023).

The sandbox program is implemented in collaboration with 36 government agencies, including eight local governments. A total of 1,376 regulatory approvals have been issued, accounting for cases where multiple regulations were involved in a single project. Among the leading ministries, the Financial Services Commission (FSC) approved 291 cases (21%), followed by the Ministry of Trade, Industry and Energy (MOTIE) with 234 cases (17%), and the Ministry of Land, Infrastructure and Transport (MOLIT) with 170 cases (12%). Other notable contributors include the Ministry of Food and Drug Safety (MFDS), Ministry of Health and Welfare (MOHW), Ministry of the Interior and Safety (MOIS), and the Personal Information Protection Commission (PIPC), alongside agencies such as NPA, ME, MSIT, MCST, KCC, and MAFRA, reflecting a whole-of-government approach to fostering innovation (Regulatory Reform Commission, 2023).

<Table 1-8> Regulatory Sandbox Approval Statistics by Ministries

Total	FSC	MOTIE	MOLIT	MFDS	MOHW	MOIS	PIPC
1,376	291(21%)	234(17%)	170(12%)	149(11%)	116(8%)	64(5%)	54(4%)
	NPA	ME	MSIT	MCST	KCC	MAFRA	ETC
	49(4%)	46(3%)	35(3%)	31(2%)	30(2%)	30(2%)	76(6%)

Note: A total of 36 government agencies (including eight local governments, with MOTIE including the Korean Agency for Technology and Standards) participated, with a total of 1,376 regulatory approvals (including duplicate counts)
Source: Regulatory Reform Committee (2023).

The program has been especially beneficial to SMEs, which account for 724 of the approved projects, or 64% of the total. Large firms received 343 approvals (30%), while public institutions and local governments were responsible for 72 projects (6%). This emphasis on SMEs underlines the sandbox's role in lowering entry barriers and enabling startups and smaller companies to pioneer new technologies.

<Table 1-9> Regulatory Sandbox Approval Statistics by Firm Size

Total	SMEs	Large Firms	ETC (Public Institutions□Local Governments)
1,139	724 (64%)	343(30%)	72(6%)

Source: Regulatory Reform Committee (2023).

By the end of 2023, 265 projects, representing 23% of total approvals, had resulted in follow-up regulatory actions, including amendments to laws and regulations or formal interpretations. Specifically, 201 cases resulted in legal or regulatory amendments, while 64 cases were resolved through authoritative interpretation. These outcomes underscore the sandbox's impact not only as a tool for testing innovation but also as a catalyst for systemic regulatory reform, informed by empirical results and real-world validation. A total of 180 applications were notified to companies as "no regulation" through the expedited verification system. This fast-track confirmation process determines whether existing regulations apply to new business models within 30 days. This mechanism enables businesses to proceed quickly when no legal or regulatory barriers are identified, thereby reducing delays in innovation and time-to-market (Regulatory Reform Committee, 2023).

In 2023, two notable cases exemplify the effectiveness of this expedited process. In the field of ICT convergence, a case involving a blockchain-based IoT video security enhancement solution raised the question of whether data collected from video devices—containing personal information—would be subject to privacy protection regulations. The result clarified that while personal data is involved and must comply with the Personal Information Protection Act, no separate regulatory barriers were preventing the service from proceeding. However, further legal clarity and insurance considerations remain important. In the industrial convergence sector, an application related to a remote vehicle electronic control system (remote OTA service) inquired whether providing alert services for issues such as system errors or vehicle malfunctions—without requiring a service center visit—would be permitted under the Motor Vehicle Management Act. It was confirmed that offering early warning alerts via remote OTA (over-the-air) updates was not subject to any prohibitive regulation, thereby enabling service implementation without additional legal amendment (Regulatory Reform Committee, 2023).

These cases demonstrate how the expedited verification system not only helps uncover regulatory blind spots but also reassures companies about compliance, fostering a more agile and innovation-friendly regulatory environment.

The Dog Nose Print Identification project is a novel regulatory sandbox initiative in Korea aimed at modernizing the country's animal registration system. Traditionally, animal registration in Korea has relied on implantable radio frequency identification (RFID) devices, which require physical insertion into the pet's body. However, this project explores an innovative alternative: identifying dogs using their unique nose print patterns, much like human fingerprints (Min, 2022). Under the current Enforcement Decree of the Animal Protection Act, local governments are required to equip registered pets with radio-frequency identification equipment and issue animal registration certificates accordingly. However, this regulation has been a barrier to adopting non-invasive, alternative identification methods—such as nose print scanning—prompting the need for regulatory exemption and testing under the sandbox framework (National Animal Protection Information System, n.d.).

To address this, two companies—iSciLab and Pet's Need—have been authorized to conduct real-world tests and verifications of their dog nose print identification technologies (Ministry of Agriculture, Food and Rural Affairs, 2024).

- iSciLab's Test Period: from May 19, 2023, to May 18, 2025
- Pet's Needs Test Period: from October 10, 2023, to October 9, 2025

During these test periods, both companies are exempt from existing legal requirements and are allowed to demonstrate the safety, technical reliability, and accuracy of their fingerprint-based identification systems. If the results prove favorable, the system may eventually be integrated into the national pet registration framework, offering a non-invasive and stress-free alternative to microchipping while promoting animal welfare. This initiative illustrates how the regulatory sandbox can facilitate innovation, enable data-driven policy refinement, and build public trust in novel identification technologies.

For Poland, adopting a similar model could address structural rigidities in its governance system. A regulatory sandbox could be introduced as part of a broader national digital strategy. To support its implementation, a cross-ministerial committee on digital innovation might be established to oversee applications, manage associated risks, and facilitate policy learning across different sectors. Key areas of focus could include emerging technologies, such as artificial intelligence, as well as digitally driven advancements in healthcare, mobility, and public services.

4.2.2. Smart Manufacturing Innovation: Digitalizing the Backbone of Industrial SMEs

Manufacturing is the cornerstone of Korea's economy, accounting for 27% of GDP in 2020—nearly twice the OECD average of 14%. Among the world's top 30 economies, only China (29%), Taiwan (31%), Vietnam (38%), and Ireland (36%) have a higher share of manufacturing in their national economies *(*Bank of Korea, 2024*)*. To strengthen industrial competitiveness, Korea launched its Smart Factory initiative in 2014, aiming to accelerate digital transformation across the manufacturing sector. Over the past decade, the policy has significantly modernized small and mid-sized manufacturers through the adoption of automation, data analytics, and AI-driven production systems.

By 2022, the initiative had supported approximately 30,000 smart factories—production sites equipped with sensors, digital infrastructure, and automated systems—substantially improving the technological capabilities of Korea's SME sector. However, in its early stages, the policy prioritized expansion in numbers over depth in digital maturity, as approximately 76% of supported factories remained at the basic level, with limited utilization of collected data. Since 2023, policy efforts have shifted toward qualitative enhancement, prioritizing standardized data models, fostering solution providers, and cultivating a sustainable smart manufacturing ecosystem (Relevant Ministries, 2023).

This section outlines the development of Korea's smart manufacturing strategy since 2014, focusing on key components, including the "4+7" strategic technology framework, SME support programs, data platforms such as KAMP, and regional AI manufacturing innovation centers. It also presents relevant implications for countries seeking to upgrade their industries through digital innovation.

4.2.2.1 Evolution of Korea's Smart Manufacturing Policy (2014–2022)

Launch and Expansion: Korea's national smart manufacturing initiative commenced in June 2014 with the introduction of the "Manufacturing Innovation 3.0" policy, reflecting a growing global

emphasis on digital transformation in industrial sectors. The goal was to shift the growth paradigm by integrating IT and software into traditional manufacturing to foster new industries. In July 2015, the government established a Public-Private Smart Factory Promotion Taskforce to accelerate the development and diffusion of smart factories nationwide. In 2017, the Ministry of SMEs and Startups (MSS) was launched and assumed overarching responsibility for the smart factory initiative, which had previously been managed by the Ministry of Trade, Industry and Energy (MOTIE). This shift signaled a growing emphasis on SME-led innovation. In 2018, the government introduced the Smart Factory Diffusion and Advancement Strategy and the SME Smart Manufacturing Innovation Strategy, aiming to build a private sector–led, government-supported smart manufacturing ecosystem centered on small and medium-sized enterprises (KDI Economic Information Center, 2021).

Early targets sought to establish 20,000 smart factories by 2022, later raised to 30,000 by 2022 as the urgency for SME productivity gains grew. This aggressive expansion was accelerated in 2018 by a new Smart Manufacturing Innovation Strategy, which linked factory upgrades with smart industrial clusters and workforce training. Annual deployments jumped from around 1,250 factories per year (2014–2017) to around 4,450 per year (2018–2022). By 2019, 12,660 cumulative smart factories had been implemented, and by the end of 2022, the target of 30,000 had been met (Ministry of SME and Startup, 2018; Ju, 2021; Relevant Ministries, 2023).

Role of MSS and Partnerships: MSS spearheaded funding and coordination efforts, working closely with large enterprises and regional agencies. Notably, by 2019, one-third of smart factories had been built with private sector or corporate assistance (e.g., voluntary upgrades or vendor programs), while two-thirds still relied on government support (Ju, 2021). To encourage large company involvement, Korea introduced win-win schemes—for example, crediting multinationals' mentoring of SME suppliers in performance evaluations. Local governments also co-financed projects, and a dedicated Smart Manufacturing Innovation Act (enacted 2023) now provides a legal basis for the program and accountability measures (Relevant Ministries 2023).

Outcomes and Challenges: The rapid scale-up dramatically broadened SME digital adoption, but many deployments were rudimentary. In 2021, a quarter of SMEs with smart factories reported low utilization of their systems. Common issues included limited data integration (most "smart" systems were basic production monitoring tools) and continued gaps in automation—e.g., 77% of root industry firms (e.g., metal, casting) still had less than 50% process automation as of 2022. Moreover, the rush to meet numeric targets led to some quality control problems, such as vendors "rubber-stamping" installations for subsidies. The government identified instances of fraudulent implementations (e.g., kickbacks of matching funds, overbilling of software workforce, etc.). These challenges exposed the need to shift from a purely government-driven, volume-centric approach toward a more sustainable, demand-driven ecosystem approach (Relevant Ministries, 2023).

Growth of the Ecosystem: One positive byproduct was the growth of a domestic smart manufacturing supply industry. The number of certified smart factory solution providers—firms offering related software, equipment, and integration services—increased from 299 companies in 2016 to 1,969 by 2022, driven by booming demand (Relevant Ministries, 2023). By 2024, this had further increased to 2,460 specialized providers, an 8.2-fold jump since 2016 (Relevant Ministries, 2024). However, most remained small enterprises; over 81% had an annual revenue of under KRW 5 billion (approximately USD 4 million), with many focusing on reselling basic solutions (e.g., off-the-

shelf MES software) rather than developing advanced technologies. This fragmentation and limited R&D capacity in the supply base prompted the government to launch new measures to foster high-quality solution providers and filter out subpar actors, including a “Two-Strike-Out” policy to ban vendors engaged in repeated fraud (Relevant Ministries, 2023).

4.2.2.2 Recent Policy Upgrades (2023–2024): Towards a Smart Manufacturing Ecosystem

By 2023, Korea recognized that “quantity-first” strategies had reached their limits and pivoted to emphasize quality, utilization, and ecosystem-building. In September 2023, the government announced the “New Digital Manufacturing Innovation Strategy” (MIDAS, 2027), setting a vision for “a world-class manufacturing powerhouse through digital manufacturing innovation.” Key goals include cultivating 5,000 advanced-level smart factories by 2027 and inducing an additional 20,000 SMEs to undergo digital transformation via private and regional initiatives. Rather than the government directly subsidizing basic systems for all, the new approach focuses on providing tailored support, integrating data, leveraging private-sector leadership, and developing solution providers (Relevant Ministries, 2023).

In October 2024, MSS followed up with the “Smart Manufacturing Innovation Ecosystem Enhancement Plan”, which, for the first time, treats smart manufacturing as an industry. This plan balances continued diffusion of smart factories with dedicated measures to grow the smart manufacturing industry (equipment, software, and service providers), aiming for “balanced development of all sub-sectors.” It introduced a formal classification of smart manufacturing technologies into four domains and 14 sub-fields and identified seven strategic technologies to prioritize national support. The following pillars now define Korea’s upgraded strategy (Relevant Ministries, 2024):

Technology Focus: “4+7” Classification of Smart Manufacturing

To guide R&D and industry development, Korea redefined the scope of smart manufacturing into four key domains and selected seven strategic subfields for intensive fostering. The four domains encompass the full stack of a digital factory: (1) Automation equipment—e.g. industrial robots, automated machines, machine vision systems; (2) Connectivity devices—sensors, control systems and industrial network equipment linking machines and IT systems; (3) Informatization solutions—software to manage production, logistics, and enterprise operations (MES, SCM, ERP, etc.); and (4) Intelligence services—advanced solutions like AI, big data analytics, digital twins, cloud platforms, and AR/VR for manufacturing. Within these, seven priority technologies have been designated based on strategic importance and technology readiness (Relevant Ministries 2024) :

(i) Identification systems & Machine vision (Automation domain)—vision inspection and sensor systems for smart perception

(ii) Industrial network equipment (Connectivity)—high-reliability wired/wireless communication devices for factories

(iii) Control systems (Controllers)—intelligent controllers/PLC units for precision monitoring and control of processes

(iv) Production Management Systems (Informatization)—integrated MES (Manufacturing Execution Systems) and related shop-floor solutions to optimize production scheduling, quality, and energy use.

(v) Logistics Management Systems (Informatization)—solutions like SCM/WMS (Supply Chain and Warehouse Management) for end-to-end supply chain visibility.

(vi) Virtual Modeling (Digital Twin) (Intelligence)—simulation and cyber-physical systems that mirror real-time production processes for optimization and testing.

(vii) Manufacturing Big Data & AI (Intelligence)—data analytics platforms and AI applications tailored to manufacturing (predictive maintenance, process AI, etc.).

By concentrating resources on these seven areas, the government aims to nurture globally competitive expertise. For example, MSS plans to certify 500 "Smart Manufacturing Specialist" firms by 2027 that excel in these fields and elevate the technological level of SMEs by at least 5% through the diffusion of such advanced solutions. This focus also informs R&D programs, testbeds, and import substitution efforts (some gaps, like sensors and industrial software, have been historically filled by foreign suppliers—an issue the policy highlights for improvement (Relevant Ministries, 2024).

Tailored Stage-Based Support for SMEs

Korea has transitioned from one-size-fits-all grants to a stage-based support system tailored to each firm's digital readiness. Rather than pushing unprepared firms to adopt systems they cannot fully use, the new strategy segments SMEs into three tiers and provides graduated support (Relevant Ministries 2023):

(i) High-capability SMEs: Technologically advanced manufacturers that are ready to implement cutting-edge solutions. These firms receive support to build "autonomous factories" leveraging AI and digital twins, and to serve as exemplar smart plants that collaborate with suppliers (so-called digital collaboration factories linking value chains). Approximately 50 leading factories will be selected for this top-tier assistance in 2024.

(ii) Moderate-capability SMEs: Firms that have some basic automation or data systems in place but have not achieved integration or real-time control. The program helps these companies upgrade from basic to advanced smart factories, for example, by adding IoT sensors, real-time data analytics, and manufacturing AI to existing operations. The government set a target to upgrade roughly 1,050 such factories by 2024 as part of this tier. These projects focus on making data accessible and actionable on the shop floor (moving from simply collecting data to using it for automated control and decisions).

(iii) Low-capability SMEs: Small manufacturers with minimal automation (often labor-intensive operations) that face resource and skill constraints. For these, the policy emphasizes foundational upgrades—deploying affordable industrial robots or simple digital tools to relieve labor shortages and improve safety/quality. Rather than heavy central subsidies, Korea is leveraging local governments and policy finance (loans from the Korea SME Bank and credit guarantees) to encourage voluntary adoption at this basic level. In other words, regional industry programs and concessional loans help these firms take the first steps, while central funds focus on the higher tiers of innovation.

This tiered model ensures “companies get the right support at the right stage,” improving the effectiveness of public investment. It also addresses past issues where unready firms installed systems they did not use. Now, only SMEs that meet specific readiness criteria proceed to advanced-stage projects, often with guidance from experts. Five hundred “SME DX mentors,” drawn from retired engineers and technical institutes, assist companies on-site (Relevant Ministries, 2023).

Developing Solution Providers and Industry Ecosystem

A central plank of the new strategy is to cultivate a robust smart manufacturing industry ecosystem—the cluster of solution vendors, system integrators, software developers, and equipment makers that supply digital solutions to factories. This marks a shift in treating this domain as an independent industry with growth potential, rather than just an ancillary to factory automation. According to a global market study, the smart manufacturing market is expected to reach approximately KRW 438 trillion (USD 330 billion) by 2028, growing at an annual rate of approximately 22%. Korea sees an opportunity to boost domestic suppliers’ global competitiveness (Relevant Ministries, 2024).

Key measures include strengthening solution provider capabilities through certifications, growth-stage financing, and performance disclosure. Starting in 2024, MSS is introducing a “Smart Manufacturing Specialist Enterprise” designation for qualified suppliers, streamlining their participation in government projects and reducing administrative burdens. The aim is to elevate promising firms into globally active players via scaled support. Providers are offered consulting to improve in-house management and technology (assessing them on 37 capability criteria and advising on gaps. The government is also increasing transparency by publishing each vendor’s track record (projects delivered, client satisfaction, technical domains) to help SMEs identify reputable partners (Relevant Ministries, 2024; Relevant Ministries, 2023).

At the same time, authorities are clamping down on market misconduct. In July 2023, the Smart Manufacturing Innovation Act took effect, allowing the recovery of the full government subsidy from any project found to have been implemented falsely, and barring repeat offenders from any future programs (“two-strike-out”). These strict penalties, alongside the new quality bar for certified specialists, are intended to “self-cleanse” the market of unqualified suppliers, thereby encouraging fair competition and consolidation around capable firms (Relevant Ministries, 2023).

Another facet of ecosystem-building is networking and collaboration. The policy encourages the formation of regional industry alliances; for example, local Smart Manufacturing Associations are being established to connect solution providers, manufacturers, and experts within each province. A national “Manufacturing DX portal” is also under development to match SME solution demand with the right suppliers and consultants across the country. This reflects a lesson from countries like Germany, which supports 18 regional SME competence centers and nine sectoral digital centers to reach SMEs at the local level. Korea is adopting a similar approach to decentralization, shifting away from a Seoul-centric, government-only initiative to a broader coalition that includes regional governments, industry groups, and large anchor companies (Relevant Ministries, 2023).

Data Infrastructure and AI in Manufacturing

To fully leverage digitalization, Korea is focusing on the use and sharing of manufacturing data. Earlier phases revealed that installing sensors and software is not enough if data remains siloed or in proprietary formats. Thus, a major push is underway to establish data standards and a common platform, enabling SMEs, large firms, and solution providers to securely share and utilize manufacturing data.

Data standardization: The government is developing a "Korean Manufacturing Data Reference Model", benchmarking international standards like the Asset Administration Shell (AAS) from Germany. By 2024, standard data models for 50 key manufacturing processes/equipment will be defined and piloted. These standards specify how machines and sensors represent data (names, units, formats for things like temperature, pressure, etc.), ensuring interoperability. Once standards are in place, guides and training will help equipment makers and IT providers adopt them. The goal is to make it far easier to integrate systems—e.g., if a factory switches machine vendors or adds new software, the data can flow in a common format without costly rework (Relevant Ministries, 2023).

KAMP—AI Manufacturing Platform: Korea has built a central data platform called KAMP (Korea AI Manufacturing Platform) to aggregate and utilize SME manufacturing data. KAMP provides a cloud-based repository of manufacturing AI datasets and analysis tools, intended as an "AI navigator" for SMEs. As of 2023, KAMP offered 50 pre-built AI data sets and 13 AI solution tools (for anomaly detection, predictive maintenance, etc.), but actual data contributions from companies have been limited so far. To boost engagement, the government is revamping KAMP with new features. By 2027, 500 curated manufacturing datasets (up from 100 in 2024) are expected to be accumulated, and an online data marketplace will be launched, enabling companies to securely upload, search, and trade manufacturing data. Subsidies will support SMEs in collecting and anonymizing their shop-floor data, so they can contribute to and benefit from shared AI models. KAMP essentially serves as a national data commons and AI-as-a-service hub for manufacturing—a critical resource for smaller firms that cannot develop these capabilities alone (Relevant Ministries, 2023).

AI Manufacturing Centers: To complement digital infrastructure, Korea is also establishing physical and organizational support for SMEs to adopt advanced technologies like AI. This includes setting up "Digital Transformation Hubs" (one-stop support centers) in industrial regions. For example, in 2024, the MSS Minister hosted a forum at the Gyeonggi Technopark Digital Conversion Hub with SME CEOs to discuss scaling AI and data use. Such centers provide hands-on guidance, training on AI use cases, and connections to tech experts from top institutes (Korea is leveraging its science and tech universities like KAIST as part of an AI support network). Through these hubs, SMEs can experiment with technologies like AI vision or digital twin simulations on pilot lines before investing in their own facilities. In addition, the government is funding AI solution co-development projects—e.g., matching AI startups with manufacturing SMEs to solve specific production problems, thereby creating reference use-cases in sectors like food processing or textiles. By embedding AI expertise into the ecosystem and lowering adoption risk, Korea hopes to accelerate the transition from basic automation to AI-driven smart factories across its SME base (Relevant Ministries, 2023; Relevant Ministries, 2024).

4.2.2.3 Recommendations for Poland: Adapting Lessons from Korea's Experience

Poland's manufacturing SMEs can greatly benefit from a coordinated approach to smart manufacturing, drawing on Korea's successes and lessons learned. Key strategic recommendations include:

Build a National Smart Manufacturing Roadmap: Establish a clear multi-year roadmap for SME digitalization, backed by top-level government commitment. Poland should define targets (e.g., number of SMEs to reach "Industry 4.0" readiness by 2030) and coordinate across ministries (economy, digitalization, education) to align resources. A dedicated program—akin to Korea's smart factory initiative—can focus policy attention on SME needs. Setting ambitious but realistic goals will signal long-term support to firms and technology providers alike.

Develop a Tiered Support System: Not all SMEs are equal in digital maturity, so adopt a stage-based support model similar to Korea's. For example, offer basic automation grants or loans for micro-manufacturers taking first steps (installing their first sensors or semi-automated equipment). For more advanced mid-sized firms, provide larger co-funding for integrated "model factory" projects (ERP/MES, IoT sensors, and robotic cells) that can showcase returns. Tie funding to performance and utilization—ensure companies get expert coaching so that new systems are actually used. This tiered approach maximizes impact and avoids one-size-fits-all solutions.

Strengthen SME Digital and Automation Capabilities: Beyond funding equipment, prioritize capability-building for SMEs. This includes sponsoring digital assessments and consulting for factories (to help them identify process bottlenecks and suitable technologies), as well as providing training vouchers to upskill workers and managers in digital competencies. Korea's example of training 100,000 smart manufacturing workers underlines the scale of skill development needed. Poland can expand vocational and continuing education programs focused on industrial IT, data analytics for production, and maintenance of automation equipment. By enhancing human capital, SMEs will be better equipped to absorb new technologies.

Foster a Domestic Innovation Ecosystem: Encourage the growth of local solution providers and tech startups in the industrial digitalization sector. Poland can create accreditation or support schemes for providers of automation solutions, IIoT (Industrial IoT) devices, software integrators, etc. This might involve grants for developing new solutions (e.g., AI quality inspection for food processing lines) or tax incentives for SMEs to purchase local tech. Public-private innovation centers can bring together academia, startups, and manufacturers to collaborate on pilot projects. Over time, a strong homegrown ecosystem ensures that SMEs have affordable, nearby sources of technology and support, much as Korea invested in building up its network of suppliers.

Incentivize Industry Participation and Collaboration: Leverage the expertise of larger industrial players to pull SMEs forward. Poland can introduce "large-small alliance" programs where big manufacturers or multinational plants mentor smaller local suppliers in adopting digital tools (for example, an automotive OEM helping its parts vendors implement real-time production monitoring). Offer recognition or tax benefits to large firms that actively assist SME modernization. Industry associations should also be engaged to promote awareness and aggregate demand for smart solutions (e.g., group purchasing of IoT systems to lower cost). The government might consider performance metrics (similar to Korea's co-growth index) that reward corporations for supporting SME digital upgrades.

Invest in Digital Infrastructure and Shared Platforms: Ensure that foundational digital infrastructure is in place. This includes expanding high-speed internet coverage to industrial and rural areas, deploying 5G/edge networks for smart factories, and possibly developing a manufacturing data platform in Poland. A platform analogous to KAMP could allow Polish SMEs to securely share data and access AI models (for instance, AI algorithms for predictive machine maintenance trained on pooled data from many companies). Government and industry could collaborate to populate such a platform with relevant datasets (like production parameters from food processing or metal fabrication) and analytics tools in the Polish/European regulatory context. This lowers the barrier for SMEs to use advanced analytics without having to build from scratch.

Bridge Sector-Specific Needs: While a national strategy provides an umbrella framework, implementation can be tailored to key sectors of Polish industry. For instance, food and beverage manufacturers (a significant SME segment in Poland) may focus on traceability systems and sensor-based quality control. Textile and apparel producers could explore automation in cutting and RFID tracking in logistics. Metalworking and machinery SMEs can benefit from advanced CNC machines with IoT connectivity and energy management systems. Poland can launch pilot programs or innovation clusters for these verticals, demonstrating how Industry 4.0 tools apply in each context. Sharing success stories from these sector-specific pilots will build momentum and help diffuse best practices across all industrial SMEs.

By taking a holistic approach—combining a clear vision, tailored support, ecosystem nurturing, and inclusive outreach—Poland can accelerate its manufacturing sector into the digital era. Korea's experience shows that political will and consistent policy frameworks can transform thousands of SMEs, but also highlights the need to continually adapt strategies to improve effectiveness. Poland can now leapfrog, avoiding early pitfalls (such as purely quantitative goals) and focusing on sustainable, inclusive, and smart manufacturing growth. With coordinated action, Polish industry can enhance its productivity and innovation capacity, ensuring competitiveness in the evolving global market.

4.2.3. Smart Service Support Program

The Smart Service Support Program, launched by the Korean government in 2025, aims to assist SMEs in developing and adopting ICT-based "smart" service solutions. The program aims to drive innovation in the service sector by applying advanced digital technologies, including big data and artificial intelligence. Participating SMEs receive both financial support and expert consulting to implement digital tools customized to their specific business needs (Ministry of SMEs and Startups, 2025).

Program Structure and Types of Support:

The program offers flexible forms of support to accommodate different types of business projects. Individual SMEs seeking to develop new digital services tailored to their operations can obtain co-financing for projects lasting approximately six to eight months, with the government covering up to KRW 50 million (approximately EUR 35,000), or 50% of the total project cost. In 2025, around 110 such single-company projects were funded (Ministry of SMEs and Startups, 2025).

For larger collaborative efforts, the program also supports consortia of five or more companies developing shared smart service solutions. These joint projects, typically of the same duration, are eligible for up to KRW 250 million (approximately EUR 175,000) in matched funding. Due to their scale, about eight consortium-based projects were supported during the year. In addition to fostering new development, the program provides support for enhancing or expanding previously implemented digital tools. SMEs upgrading their existing smart services can access up to KRW 100 million (about EUR 70,000) under the same 50% co-financing structure. In 2025, approximately 25 such upgrade projects were carried out (Ministry of SMEs and Startups, 2025).

Beyond financial support, the program emphasizes expert guidance through its “Coordinator” system. These government-funded consultants assist SMEs at every stage of their project—from initial planning and development to deployment—by offering up to two fully subsidized consulting sessions per phase. Coordinators help firms navigate challenges, ensure that chosen technologies align with business goals, and increase the effectiveness and sustainability of implementation. Overall, the Smart Service Support Program integrates funding with specialized consulting to enable Korean SMEs to adopt digital solutions that enhance their competitiveness. By reducing financial barriers and providing hands-on expertise, the initiative plays a key role in accelerating service sector innovation and building a more digitally capable SME ecosystem.

Implementation Procedure: The Smart Service Support Program operates through a well-defined, multi-stage implementation process involving several stakeholders. It begins with a public call for applications announced by the Ministry of SMEs and Startups (MSS). Once the call is issued, proposals from interested SMEs are collected and processed by the designated program administrator, the Technology and Information Promotion Agency for SMEs (TIPA), along with selected implementing organizations.

Following the application phase, an evaluation committee, comprising subject matter experts and representatives from both TIPA and the implementing agencies, reviews the submissions and selects the projects that will receive support. Once the evaluation is complete, MSS and TIPA formally confirm the list of approved SMEs and projects.

At this point, a tripartite agreement is signed between the program administrator, the implementing organization, and the participating SME, along with its chosen solution provider. With agreements in place, the project officially begins. Throughout implementation, an independent auditing firm, working in coordination with TIPA, monitors the use of funds and ensures compliance with project requirements.

As each project nears completion, the auditing body, in conjunction with TIPA and the implementing organizations, conducts a final review to assess outcomes and verify that all deliverables have been fulfilled. The process concludes with the program administrator officially closing the project and compiling performance data for overall program evaluation and future planning.

Eligibility and Selection Criteria: Eligible applicants are those who meet Korea’s SME definition (as outlined in the SME Framework Act) and participate in a consortium of at least two parties: an adopting SME (from the service industry) and a technology-supplying firm. The technology provider must be registered in the government’s Smart Service Provider Pool (a list of pre-approved digital

solution vendors). New providers not yet included in the pool are required to register at least two weeks before applying.

To encourage thorough preparation, proposals receive bonus points if the SME has already completed a prior consulting engagement with a program coordinator (+2 points) or if the project plans to deploy the solution on a CSAP-certified cloud platform (+3 points).

Certain applicants are excluded to avoid overlap and ensure effective targeting. These include:

- Companies that have already received new smart service support between 2020 and 2024 (they may only apply for enhancement support, not a second new project);
- Firms currently benefitting from similar digitalization programs (such as smart factory initiatives);
- Companies without a clear plan for service implementation;
- Entities that are inactive, bankrupt, or under sanctions.

Governance and Delivery Mechanism: The Smart Service Support Program is managed through a multi-tier governance framework. The Ministry of SMEs and Startups provides overall policy direction and funding.

TIPA (Technology and Information Promotion Agency for SMEs) serves as the central Program Administrator, with responsibilities that include detailed program design, budgeting, oversight of project evaluations, and performance monitoring. TIPA also supports the Ministry in policy planning and ensures the program evolves—for example, by planning new support initiatives or refining existing ones.

Selected Implementing Organizations carry out on-the-ground implementation. These intermediary agencies (such as industry associations or development foundations) are chosen for their capacity to reach SMEs and support project execution. Their functions include identifying enterprise needs, facilitating coordinator consulting services, assisting in the evaluation of project proposals, and supervising day-to-day project management. They also create networking opportunities for participating firms to share best practices and learn from one another.

In 2024, the Ministry selected four Implementing Organizations through a competitive call, including SME industry associations (e.g., MAINBiz, Innobiz) and a smart technology consulting association, to run the program across different regions and sectors. Their mandate spans 2024–2026.

In summary, Korea's Smart Service Support Program provides an integrated approach that combines matching grants, vetted solution providers, and expert consulting to drive SME digital transformation. By funding projects on a cost-share basis and involving industry intermediaries, the program mitigates financial risk for SMEs and builds an ecosystem of service providers. For Poland, this case provides a useful reference on how the government can catalyze SME digitalization through structured support and multi-stakeholder governance. Poland may draw on elements of the Korean model—such as the use of digital technology vouchers, coordinator-led advisory services, and certified provider pools—as it refines its own SME support strategies.

5. Policy Recommendations

International experience, particularly from Korea, offers valuable insights into how targeted programs can accelerate SME digital transformation and address systemic barriers. Three Korean initiatives—regulatory sandboxes, smart factory programs, and smart service vouchers—stand out for their measurable impact and relevance to Poland's situation.

Regulatory sandboxes in Korea have enabled companies to pilot innovative solutions without fear of breaching existing regulations, thereby reducing time-to-market and facilitating responsive policy updates. These sandboxes have supported hundreds of trials in fintech, mobility, and healthcare, fostering innovation ecosystems and attracting investment. For Poland, such a mechanism could reduce legal uncertainty for SMEs experimenting with AI-driven manufacturing, digital health, or logistics automation, thus unlocking innovation currently constrained by rigid or unclear regulations.

Smart factory programs have transformed Korean manufacturing SMEs by providing tiered support—from basic automation to full Industry 4.0 integration—resulting in productivity gains of up to 30%, significant defect reduction, and faster delivery times. The programs also nurtured a domestic ecosystem of solution providers, reinforcing industrial competitiveness. In Poland, where many SMEs lag in automation and data integration, a national smart factory initiative could systematically raise technological maturity, improve supply chain resilience, and stimulate growth in local tech industries.

Smart service vouchers in Korea have empowered service-sector SMEs to adopt tailored digital tools through co-funding with certified solution providers. This approach lowered financial barriers, maintained quality standards, and promoted competition among suppliers. For Poland, such a voucher system could particularly benefit the vast base of non-manufacturing SMEs, enabling them to access market-ready solutions that align with their operational needs. Linking voucher access to advisory programs such as EDIHs or a Digital Transformation Coordinator service would ensure that adoption is well-planned and effective.

By adapting these proven tools to Poland's context and embedding them in a unified, centrally coordinated framework, policymakers can directly target the key obstacles to SME digitalization: regulatory rigidity, low technological capacity, and cost barriers. This alignment of Korea's best practice with domestic priorities provides a strong foundation for the policy recommendations that follow.

The proposed framework consists of five mutually reinforcing pillars. First, regulatory sandboxes in priority sectors will enable SMEs to test innovative digital solutions under controlled conditions, reducing uncertainty and accelerating adoption. Second, a Digital Transformation Coordinator Program will deploy trained advisors to guide SMEs through the full transformation process—from readiness assessment to implementation. Third, a Smart Service Voucher scheme will lower financial barriers by co-funding SME purchases of certified digital solutions, creating market-driven demand. Fourth, a Digital Solutions Provider Registry and Innovation Network will provide SMEs with reliable access to vetted technology partners, while fostering knowledge exchange. Ultimately,

a National Smart Factory Initiative will enable manufacturing SMEs to adopt Industry 4.0 technologies through a tiered support model, targeted training, and the development of domestic solution providers.

This chapter outlines key policy recommendations for accelerating the digital transformation of Polish SMEs. These recommendations are informed by international best practices (including the Korean experience discussed earlier) and are tailored to Poland's economic context and strategic goals. Each proposal aligns with broader EU initiatives, such as the EU's Digital Decade targets and Poland's FENG program (European Funds for a Modern Economy), to ensure consistency with Europe's digital strategy. The recommended measures cover regulatory facilitation, capacity building, direct financial support, ecosystem development, and a dedicated push for smart manufacturing.

5.1. Introduce Regulatory Sandboxes for Digital Innovation

To complement existing SME support programs (e.g., the "Smart Pathway" and "Dig-IT" initiatives under FENG, as well as regional support provided through EU-funded regional programs managed by the Marshall Offices), Poland should establish targeted regulatory sandboxes that allow companies to pilot innovative digital solutions in a controlled environment. A regulatory sandbox provides a temporary relaxation or customization of certain legal requirements under the supervision of regulatory authorities, allowing new technologies to be tested without violating regulations. This tool can spur innovation in sectors where rigid regulations might otherwise impede experimentation.

Scope of Sandboxes: Sandboxes should be introduced in priority domains where current regulations may inadvertently hinder innovation— for example, digital health services, smart manufacturing, or intelligent logistics (given that fintech sandboxes already exist). These areas are aligned with national development priorities and EU-level digital agendas (including the EU Digital Decade goals)- Focusing on such sectors ensures sandbox trials address high-impact innovations while remaining coherent with Poland's and Europe's strategic objectives.

Design and Oversight: A multi-agency governance model is recommended for sandbox programs. Sector-specific regulators (e.g., finance, health) would jointly administer each sandbox alongside innovation agencies. For instance, the Ministry of Development and Technology (MRiT), in coordination with bodies like BGK (the state development bank) and ARP (Industrial Development Agency), could lead program design and oversight. Lessons from Korea suggest that involving multiple regulators facilitates the testing of cross-sector innovations—such as solutions that span data protection and industrial automation—without legal ambiguity. MRiT can convene relevant regulators to define the parameters of a sandbox. In contrast, each regulator retains authority in its domain. All sandbox experiments should be time-bound, limited in scale, and subject to monitoring and reporting requirements to manage risks-

Building on the Existing Ecosystem: The sandbox mechanism should complement Poland's ongoing digitalization funding programs by providing a space for projects that push the boundaries of current law. For example, an SME developing an AI-driven service with a Dig-IT grant might face uncertainty regarding data protection rules; a sandbox would allow it to test the service under temporary regulatory relief while authorities observe outcomes. Similarly, a manufacturing firm

implementing an IoT-enabled production line via the Smart Pathway could use a sandbox to ensure compliance with technical standards before full deployment. In this way, sandboxes become an extension of the FENG toolkit—enabling high-innovation companies to progress despite regulatory hurdles.

Pilot Initiatives and Scale-Up: It is advisable to launch one or two pilot sandboxes quickly to demonstrate commitment and learn from initial trials. For instance, Poland could introduce a FinTech Sandbox under the financial supervisor (KNF), and an Industry 4.0 Sandbox under MRiT's purview, as early examples. Implementing a few pilots requires limited public funding (mostly to cover administrative and compliance oversight costs). Still, it can yield substantial benefits. Successful cases from these sandboxes would encourage more SMEs to innovate and provide evidence for any needed regulatory adjustments. Over time, the sandbox program could expand to other sectors, creating a flexible regulatory innovation environment in line with EU best practices (many EU countries have launched fintech sandboxes, for example).

5.2. Launch a Digital Transformation Coordinator Program

Even with funding available, many SMEs struggle to navigate digital transformation due to limited expertise. To address this gap, Poland should establish a national "Digital Transformation Coordinators" service—a program that deploys certified advisors to guide SMEs through the entire process of adopting new technologies. This recommendation builds on Korea's successful coordinator model and complements existing Polish support structures, such as the Smart Pathway and the network of European Digital Innovation Hubs (EDIHs), while also filling the gap left by the discontinuation of consultancy services under Dig.IT.

Program Design: The Coordinators program would train and certify a cadre of digital transformation advisors (perhaps drawing from technology consultants, industry experts, or experienced managers) who can provide hands-on assistance to SMEs. The program can be administered through institutions such as ARP or PARP (the Polish Agency for Enterprise Development), or in partnership with regional EDIHs, ensuring national coverage. Each participating SME would be matched with an advisor and receive a structured package of support, typically spanning 5 to 6 consulting sessions over a few months. The content of these sessions would include:

Digital Readiness Assessment: The first step in the Coordinator Program involves conducting a comprehensive diagnostic of the SME's current level of digital maturity. This assessment should use standardized, methodologically sound tools—such as ADMA or the Digital Starter Kit for Enterprises developed by PFR, alongside methodologies previously applied under the Dig.IT program—to ensure consistency, comparability, and reliability of results across sectors and regions. The diagnostic process would evaluate multiple dimensions, including the firm's existing digital infrastructure, the extent of technology integration in core operations, workforce digital skills, data management practices, and cybersecurity posture. In addition to quantitative scoring, the coordinator should gather qualitative insights through interviews with management and key staff to better understand operational bottlenecks, organizational culture, and leadership's vision for digital adoption. The outcome of this assessment is to produce a clear, evidence-based profile of the SME's strengths, gaps, and priority needs, serving as the foundation for targeted intervention.

Roadmap Development: Following the assessment, the coordinator will work closely with the SME's leadership team to co-create a Digital Transformation Roadmap that is both strategic and actionable. This roadmap should align proposed technology investments with the company's broader business objectives—whether improving operational efficiency, expanding market reach, enhancing customer experience, or developing new product lines. Where possible, it should also be synchronized with existing national or EU-backed programs such as the Smart Pathway under the FENG framework, ensuring that SMEs can leverage available funding modules and technical resources for maximum impact. The roadmap should define short-, medium-, and long-term milestones, specifying the technologies to be adopted, the sequence of implementation, associated costs, potential funding sources, and anticipated benefits. Additionally, it should include risk mitigation measures, workforce training plans, and KPIs to track progress. By providing SMEs with a tailored, realistic, and well-resourced plan, the coordinator ensures that digital investments are not isolated purchases but integral components of a coherent transformation strategy.

Solution Provider Matching: The coordinator helps the SME identify and connect with qualified technology solution providers. Leveraging a network or registry of vetted IT vendors and system integrators, the advisor recommends potential partners suited to the SME's needs- (This links to Recommendation 4.4 below—establishing a provider registry—which would equip coordinators with an up-to-date directory of credible suppliers).

Implementation Support and Training: The advisor offers light-touch guidance during the implementation of the digital solution. This can include troubleshooting minor issues, ensuring that the SME's staff receive proper training on new systems, and helping set up maintenance or data-management processes for the post-implementation phase. The goal is to ensure the SME not only installs new technology but also integrates it effectively into its operations and workforce practices.

To encourage SME uptake, the Coordinator program should be publicly funded or subsidized (for example, using technical assistance funds from FENG) so that services are either free or very low-cost for SMEs. The program's benefits justify this public investment: it provides personalized, on-site support that greatly increases the likelihood of successful digital adoption, especially for smaller firms outside major urban centers. It also creates a feedback loop—coordinators can report common obstacles or needs observed in the field, informing policymakers about where additional support or regulatory changes might be required. Overall, a Digital Transformation Coordinator program would significantly enhance the impact of existing grant schemes by ensuring SMEs have the knowledge and confidence to make the best use of digital investments, thereby advancing Poland's broader innovation agenda.

5.3. Implement a "Smart Service Voucher" and Matching Scheme

Building on the Korean model, Poland can introduce a Smart Service support voucher scheme to accelerate SME digitalization. The idea is to provide co-financing for SMEs to adopt approved digital solutions in a flexible, business-driven, and aligned manner with Poland's existing support programs, such as Dig-IT and the modular Smart Pathway under FENG. Using a voucher mechanism (a grant given directly to SMEs who then purchase services) would simplify administration and ensure compliance with EU procurement and competition rules.

Consortium-Based Applications: Similar to the Korean approach, each project proposal would be a joint application by an SME (the technology adopter) together with a certified technology provider (the solution supplier). Eligible tech providers could include IT firms, SaaS vendors, system integrators, or other digital service vendors. This consortium model ensures that SMEs have a committed tech partner and a clear implementation plan from the start. It mirrors elements of Poland's current Digital Strategy. IT and Smart Pathway programs, which also encourage collaboration between businesses and tech experts—

Pre-Approved Provider Pool: A maintained registry of certified solution providers will underpin the voucher system. Only providers listed in this pool can participate in projects (subject to reasonable exceptions for novel solutions). Korea's program requires that any supplier be registered in its Smart Service provider pool before an application. Poland can adopt a similar approach: set up criteria for vetting providers (technical capacity, product quality, cybersecurity standards, GDPR compliance, etc.) and allow vendors to enroll on a rolling basis. The provider registry (see Recommendation 5.4) should be open and continuously updated—for example, an online portal where new companies can apply and be evaluated within a short timeframe. This ensures a competitive, innovative market of solution providers for SMEs to choose from, and it builds trust that listed providers meet quality standards.

Voucher-Based Co-Funding: Under this scheme, SMEs would receive a significant public subsidy for approved digital projects—e.g., covering roughly 50% of project costs up to a predetermined cap. The subsidy operates like a voucher that the SME redeems when paying the chosen provider, and the government reimburses either the provider or the SME for the subsidized portion. This design enables SMEs to freely select the solution best suited to their needs (market-driven choice), while government support lowers the financial barrier to adoption. By channeling funds to SMEs via vouchers (rather than centralized procurement by government), the scheme remains consistent with EU procurement rules and mitigates state aid distortions—the demand is driven by SMEs, and providers compete to offer the best value. Moreover, elements of this scheme could mirror the "Technological Channel" approach under PFR's Digital Training Kit, which routes subsidy support through certified technology providers, ensuring that vetted and capable suppliers deliver the subsidized services.

Integration with Advisory Services: To maximize effectiveness, the voucher application process should be tied into the broader SME digital support ecosystem. Companies that have undergone a digital readiness assessment or received consulting (for example, through the Dig-IT program, an EDIH, or the proposed Coordinator program) could be given priority scoring or bonus points in the evaluation of their voucher funding applications. This encourages SMEs to make use of preliminary advisory services (so that they apply with well-prepared, needs-driven projects) and helps ensure that voucher-supported projects are "implementation-ready." It also aligns with national digitalization priorities by channeling support to SMEs that have demonstrated commitment to transformation. Additionally, linking with advisory services will create a pipeline—SMEs get advice, develop a plan, then obtain co-funding to execute it.

Administratively, the Smart Service Voucher scheme can be managed by a national agency (such as PARP or a dedicated unit within MRiT) in collaboration with industry partners. The scheme should align with FENG's funding allocations for digital transformation, potentially drawing on EU funds

available for SME tech uptake. Regular monitoring and audits would be put in place to ensure funds are used appropriately and projects meet their targets. Over time, this voucher program can significantly increase the scale and speed of SME digital adoption in Poland by combining financial incentives with accountability and choice.

5.4. Establish a Digital Solutions Provider Registry and Innovation Network

A critical component of SME digital transformation is the ecosystem of technology providers that deliver solutions (software, hardware, integration services, etc.). Poland should establish a formal national registry of digital solution providers, complemented by a network to facilitate innovation and knowledge exchange. This would enhance SMEs' access to trusted technology partners and foster a community of practice centered on digital innovation.

Certified Provider Directory: Create an open, online directory of pre-approved tech providers spanning various categories (cloud service providers, software developers, IoT and automation vendors, digital marketing platforms, etc.). Each listed provider would be vetted against clear criteria—for example, proven technical capabilities, security standards, data protection compliance, client references, and alignment with EU standards and certifications. The directory builds on the concept used in Korea (the Smart Service provider pool) but would be established nationally in Poland to fill the current gap.SMEs and public agencies alike can use this directory to find credible partners. The registry should remain dynamic: new companies can apply to join, and criteria can be updated to keep pace with technological and regulatory developments—

Public–Private Partnership in Outreach: To populate and maintain the provider network, cooperation with industry associations will be vital. Organizations such as chambers of commerce, IT industry associations, and sector-specific guilds should be involved in identifying and encouraging capable local tech firms to join the certified pool- These groups can also help disseminate information about available digitalization support to their SME members, acting as multipliers for program awareness- A joint public-private approach will ensure the registry includes a broad range of solutions (including from start-ups and regional providers) and stays relevant to what SMEs need. In line with practices observed in Poland's government support infrastructure (e.g., portals like Biznes.gov.pl that centralize access to business services and information), these industry associations could serve as intermediaries that both refer firms to the registry and funnel registry information through their member networks. This helps integrate the provider directory into existing national digital business outreach frameworks, strengthening the registry's legitimacy and reach.

Knowledge Sharing Platform: Beyond a static list of providers, Poland should cultivate an innovation network where SMEs, providers, and other stakeholders share experiences and best practices. This could take the form of an online platform or regular forum events. Korea's program has demonstrated the value of networking events in disseminating successful solutions and case studies among SMEs. Poland can create a digital platform (potentially integrated with existing EU initiatives or the EDIH platforms) where case studies are published and solution providers can showcase successful SME projects. Peer-to-peer learning will help diffuse innovation: an SME considering, say, a CRM system can read about how another SME in its sector successfully implemented one, and connect with the same provider through the network.

Leverage European Digital Innovation Hubs (EDIHs): Poland already hosts nine EDIHs co-funded by the EU (with a total budget of around EUR 23 million) to support SME digitalization. Their scope of support remains relatively narrow; they primarily serve industrial sectors, and they are still not widely recognized among entrepreneurs. Nonetheless, they offer "test before invest" facilities, training, and expert advice. The national provider network should coordinate closely with the EDIHs. For example, an SME could first experiment with a new technology at an EDIH testbed, and if the results are positive, identify a provider from the registry and use the voucher scheme to implement it in their business- EDIHs could also assist in maintaining the provider directory (by verifying competencies) or in training the digital coordinators and advisors who work with SMEs- Aligning the national network with EU-supported hubs avoids duplication of effort. It ensures that Polish SMEs benefit fully from European resources and expertise. It also helps maintain common standards on data security, interoperability, and other key issues, since EDIHs operate within EU frameworks-

By establishing a robust provider registry and innovation network, Poland will reduce information asymmetry in the SME tech market—enabling SMEs to find reliable solutions and providers to gain visibility and trust. This initiative, combined with the voucher scheme and coordinator support, creates an integrated ecosystem in which public funds, private solutions, and knowledge flows mutually reinforce one another.

5.5. Design a National Smart Factory Initiative

Manufacturing is a cornerstone of Poland's economy, and boosting productivity in this sector is crucial for competitiveness. While some Polish manufacturers (especially larger firms) have adopted Industry 4.0 practices, many SMEs lag in automation and data integration. Poland should therefore launch a dedicated National Smart Factory Initiative to drive digital transformation in manufacturing SMEs. This would align with EU industry digitization goals and can be modeled after Korea's national smart manufacturing programs, adapted to Poland's industrial landscape.

Strategic Elements of the Initiative:

National Smart Manufacturing Roadmap: The government should start by formulating a clear roadmap for SME digital manufacturing through 2030, with specific targets and milestones- For example, the roadmap could set a goal for the number or percentage of manufacturing SMEs achieving a certain level of digital maturity (such as "Industry 4.0 readiness") by 2025, 2027, and 2030- It should also define priority areas (e.g. adoption of advanced robotics, use of digital twins in production, AI for quality control) and assign responsibilities across ministries (e.g. MRiT, Ministry of Science and Higher Education, etc.) and industry partners. Establishing a dedicated national program—potentially underpinned by legislation, similar to Korea's Smart Manufacturing Innovation Promotion Act—would ensure continuity across government terms, foster inter-ministerial coordination, and hold stakeholders accountable to the roadmap's goals-

Tiered Support Based on Digital Maturity: Not all manufacturing SMEs are starting from the same level of technological advancement, so a one-size-fits-all support scheme would be inefficient. Instead, the initiative should adopt a *tiered support model* that tailors assistance to the SME's maturity stage:

Basic-level firms: Provide small grants or subsidized loans for entry-level automation and digital tools (for instance, simple sensors, basic process automation, or health and safety improvements through technology)- The focus here is to help the least-digitized factories take the first step.

Intermediate-level firms: Co-fund more integrated systems, such as ERP (Enterprise Resource Planning) or MES (Manufacturing Execution Systems) software, IoT sensor networks for production monitoring, and data analytics tools for process optimization. This level targets companies that have some digital experience but need to connect and enhance their existing systems.

Advanced-level firms: Support ambitious, cutting-edge projects—e.g., implementing model smart factories that use AI, machine learning, digital twin simulations, and full data integration across operations- These could be demonstration projects or "lighthouse" factories that showcase what is possible, potentially with larger consortia or partnerships with research institutes. Higher-tier support might involve larger grants or public-private co-investment in innovation centers.

This graduated approach ensures efficient use of funds, meeting each SME where it is on the digital journey and incentivizing progression to the next level.

SME Capacity Building—Consulting and Workforce Skills: Technology adoption must go hand in hand with building human capacity. The Smart Factory Initiative should therefore include publicly funded diagnostic consulting for manufacturing SMEs (potentially via the Coordinator program or specialized industrial tech consultants). Experts can visit factories, conduct on-site assessments, and help craft transformation plans that SMEs can then execute with available grants. Additionally, a national workforce development effort is needed to train workers and managers in digital manufacturing skills. This could leverage Poland's education and training institutions to offer short courses or certifications in areas such as industrial IT systems, data analytics for production, and robotics maintenance. Thousands of shop-floor workers, engineers, and SME managers should be upskilled to effectively implement and sustain new technologies. EU funding (e.g., European Social Fund Plus) and national funds can be tapped to support these training programs.

Foster a Domestic Smart Manufacturing Ecosystem: A vibrant local industry of technology providers and integrators is essential for long-term success. Poland's initiative should support the growth of domestic smart manufacturing solution providers—such as automation equipment suppliers, industrial software developers, IoT device producers, and system integrators- This can be achieved through targeted R&D grants, tax incentives, capacity-building programs, and recognition (certifications or labeling of proven solutions) for providers- Public-private co-innovation hubs or testbeds (perhaps linked with existing research institutes or technical universities) can facilitate pilot projects where local tech firms collaborate with manufacturing SMEs to develop new solutions- Furthermore, ensuring transparency about providers' performance (for instance, publishing case studies or user ratings for solutions implemented under the program) will build trust in local vendors and help SMEs make informed choices- By developing the domestic supply side, the smart factory transition not only upgrades manufacturers but also creates value within Poland's tech sector.

A National Smart Factory Initiative, structured as above, would position Poland's manufacturing SMEs to significantly upgrade their productivity and innovation capacity over the coming decade. It aligns with EU industrial policy (e.g., efforts under the Digital Decade to increase the adoption of advanced technologies among SMEs). It can be partially funded by EU structural funds allocated to

digitalization and innovation. Over time, this initiative is expected to contribute to higher competitiveness, increased resilience in supply chains, and the creation of high-skilled jobs, ensuring that Poland's industry remains strong in the face of global technological advancements.

References

European Chamber of Commerce in Korea. *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, 2022.

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

Financial Services Commission (FSC Korea). *FSC Regulatory Sandbox (dubbed).* YouTube video. February 19, 2025. https://www.youtube.com/watch?v=wjBp8MnJh20. [in Korean].

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

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 Industrial Technology Association. *DT Council.* n.d. https://www.koita.or.kr/conts/104006001001000.do. [in Korean].

Korea Software & Copyright Association. *SW·Copyright Trend Report (Issue 2021–16).* August 25, 2021. https://www.spc.or.kr/cs/news/images/21report16.pdf. [in Korean].

KOSMO. "What Is a Smart Factory?" Accessed February 20, 2025. https://smart-factory.kr/eng/smartFactory.do?menuId=03. [in Korean].

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&t=678s. [in Korean].

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. [in Korean].

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

Kwon, Inhyuk. "Korea's Institutional Framework on SME Digitalization." PowerPoint presentation, Slide 10. OECD Workshop, May 11, 2022.

Min, Roselyne. "'Each Dog Has a Unique Nose': Korea Tests Out 'Nose Print' ID for National Pet Registration." *Euronews,* January 11, 2022. https://www.euronews.com/next/2022/01/11/each-dog-has-a-unique-nose-south-korea-tests-out-nose-print-id-for-national-pet-registration.

Ministry of Science and ICT. *Pursuit of System Reform Restricting Large Enterprises from Participating in Public Software Projects after 11 Years.* Press Reference Material, January 31, 2024.

Ministry of Science and ICT. "Government Promotes Reform of Large Company Participation Restrictions in Public Software Projects for the First Time in 11 Years." Press Release, January 31, 2024. [in Korean].

Ministry of SMEs and Startups. *30,000 Smart Factories to Be Built by 2022 to Strengthen Korea's SME Manufacturing Base: Announcement of the 'Smart Manufacturing Innovation Strategy for SMEs (Joint Government Initiative).'* Press Release, December 13, 2018. Sejong: Ministry of SMEs and Startups. [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

National Animal Protection Information System. *Introduction to the Animal Registration System.* Ministry of Agriculture, Food and Rural Affairs, n.d. https://animal.go.kr/front/community/show.do?boardId=contents&seq=66&menuNo=2000000016. [in Korean].

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

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

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

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

World Bank Group. *Policies for Competitiveness: Position Paper on Regulatory Policy.* Washington, D.C.: World Bank Group, 2018. http://documents.worldbank.org/curated/en/617271543296023032.

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].

Relevant Ministries (Republic of Korea). *Strategy for Promoting New Digital Manufacturing Innovation.* September 18, 2023. [in Korean].

Skwarczynska, Barbara Maria, Donato De Rosa, Agnieszka Boratynska, Iwona Maria Borowik, Damian Iwanowski, Filip Piotr Kochan, Lukasz Marek Marc, Delia Rodrigo, and Emilia Skrok. *Poland Structural Policies for Competitiveness: Position Paper on Regulatory Policy.* Washington, D.C.: World Bank Group, 2023.

Software Policy & Research Institute. *An Analysis of Issues about the Effect of Restriction Policy against Conglomerates' Entry in Public Software Procurement Market.* By Ho-seok Yoo and Song-hui Kang. September 24, 2020. [in Korean].

World Bank. *Paths of Productivity Growth in Poland: A Firm-Level Perspective.* Washington, D.C.: World Bank, 2022.

02

Chapter

Strategy for Building an AI Innovation Ecosystem and Regulatory Innovation for SMEs' Digital Transformation in Poland

Hye-Shun (Melissa) Yoon (Hanyang University)
Katarzyna Colombel (Ministry of Economic Development and Technology)

Keywords:
Artificial Intelligence (AI), Small and Medium Enterprises (SMEs), Digital Transformation, Regulatory Innovation, Innovation Ecosystem, AI Adoption, Poland, Korea, Regulatory Sandbox, Voucher Programs, EU AI Act

Strategy for Building an AI Innovation Ecosystem and Regulatory Innovation for SMEs' Digital Transformation in Poland

Hye-Shun (Melissa) Yoon (Hanyang University)
Katarzyna Colombel (Ministry of Economic Development and Technology)

1. Introduction

1.1. Background

1.1.1. Poland's AI Transformation Challenge

Poland stands at a critical juncture in its digital transformation journey. The country's ambitious Digitalization Strategy 2035 provides a comprehensive roadmap, but significant implementation challenges remain. As outlined in Poland's national strategy, "the level of digitalization of enterprises is correlated with their size: the larger they are, the more they spend on average on research and development and the implementation of new technologies" (Ministry of Digital Affairs, 2023a). Despite recent progress, Poland continues to lag behind EU leaders in key areas, including the development of digital skills and the adoption of advanced technology.

The strategic importance of artificial intelligence (AI) adoption extends beyond mere economic considerations. As articulated in Poland's national strategy, "the implementation of the latest technologies and the use of systems based on human-centric, sustainable, trustworthy, safe, and inclusive AI are crucial for the development of Poland" (Ministry of Digital Affairs, 2023a). AI is positioned as a technology that can "significantly improve industrial production capacity, efficiency and quality of services provided, as well as support decision-making processes and resource management" (Ministry of Digital Affairs, 2023a).

For small and medium-sized enterprises (SMEs), which comprise 99.8% of Poland's enterprises and contribute approximately 43.6% of the country's GDP, AI presents both unprecedented opportunities and significant challenges. Poland's current position—24th among EU member states in the Digital Economy and Society Index (2022)—underscores the urgent need for accelerated AI transformation with particular emphasis on SME engagement (European Commission, 2022).

Current State of Digital Infrastructure and AI Adoption

Poland has made substantial improvements in digital infrastructure. Currently, 47% of Polish enterprises utilize medium- and advanced-level cloud technologies, and 19% employ data analytics. However, according to the European Commission's 2024 Digital Decade Report, AI adoption remains critically low, at just 3.7% of enterprises, which is below the EU average of 8% (European Commission, 2024a). This gap between cloud technology usage and AI adoption signals that while foundational digital capabilities exist, the transition to AI-enabled competitiveness remains elusive.

The AWS Barometer Report provides an additional perspective, reporting an overall adoption rate of 30% that includes experimental use, showing 36% year-over-year growth—the fastest in the EU. However, when measuring operational implementation, only 25% of Polish SMEs have actually deployed AI tools, primarily for predictive analysis (33%) and system automation (28%), yielding revenue growth (33%) and cost reductions (33%) (Amazon Web Services & Strand Partners, 2024b).

Sectoral and Regional Disparities

AI adoption exhibits pronounced sectoral variations. The defense and aerospace sectors lead with 71% adoption rates, followed by manufacturing at 47%, and financial services at 40%. In contrast, traditional service sectors lag significantly, with logistics at 25% and healthcare at 18% (Amazon Web Services & Strand Partners, 2024a). Geographic concentration in urban centers, such as Warsaw, Kraków, and Wrocław, creates additional territorial digital divides that require targeted regional interventions.

Impact of the EU AI Act

The EU AI Act, which entered into force on August 1, 2024, creates both challenges and opportunities for SME AI adoption. The Act presents significant compliance challenges for smaller enterprises, with 50% of enterprises expressing concerns about delays in innovation due to regulatory compliance (Digital Poland Foundation, 2024). The regulatory burden is particularly pronounced for high-risk AI systems, which must meet stringent requirements for data quality, documentation, human oversight, and conformity assessments. Additionally, 32% of surveyed defense companies cite a lack of legal clarity on AI as an obstacle, illustrating how regulatory uncertainty creates barriers, particularly in sensitive sectors.

However, the Act also provides structured support mechanisms specifically designed to assist SMEs. These include priority access to regulatory sandboxes under Article 55, which allows SMEs and startups to test AI innovations under more flexible regulatory conditions. The legislation incorporates cost reduction measures, offering discounted conformity assessment fees based on company size, development stage, and market demand. Furthermore, the phased implementation approach provides valuable preparation time, with full enforcement scheduled for August 2026.

Multi-Dimensional Barriers to Adoption

Polish SMEs face interconnected challenges across multiple dimensions:

- **Knowledge and strategic awareness deficits** regarding AI's business potential and implementation pathways
- **Human capital and resource limitations** with acute shortages in AI-ready talent, including "shortage of specialists on the market and lack of competences, especially in the field of software development skills, complex data and mathematical analysis" (Ministry of Digital Affairs, 2023b)
- **Technical infrastructure and integration complexities** compounded by "IT security problems" and "lack of time to implement digital solutions" (Ministry of Digital Affairs, 2023b)
- **Ecosystem and regulatory environment gaps** including fragmented support systems and weak research-industry linkages

The 2025 Digital Decade Report specifically highlights that only 44.3% of the Polish population possesses basic digital skills, compared to the EU average of 55.6%. It emphasizes that "the shortage of ICT specialists affects enterprise digitalization, advanced technology adoption, and cybersecurity efforts" (European Commission, 2025).

Poland has set an ambitious goal: to increase AI adoption from current levels to 50% by 2035, representing more than a thirteen-fold growth (Ministry of Digital Affairs, 2023a). This target requires comprehensive policy interventions that simultaneously address all identified barriers. The European Commission's 2025 report warns that "halfway through the Digital Decade, the time to act is now," emphasizing that achieving these targets could unlock economic gains of up to 1.8% of GDP (European Commission, 2025).

1.1.2. Korea as a Strategic Benchmark

Korea provides a highly relevant and practical benchmark for Poland's AI transformation strategy, given its similar trajectories of rapid industrialization, export-oriented growth, and the development of robust manufacturing sectors. Both countries currently prioritize digital transformation and SME competitiveness as core national strategies. Importantly, both operate within complex regulatory environments where supporting SME AI adoption must be balanced with strict compliance to data protection, AI governance, and cybersecurity standards.

What makes Korea particularly valuable as a benchmark is not high adoption rates but rather its systematic approach to addressing adoption barriers. Korea successfully transitioned from technology importer to innovation leader within two decades and developed integrated government-industry-academia collaboration models that Poland can adapt within its EU context (OECD, 2024). While Korea also faces measurement challenges with varying statistics depending on methodology, it has established more structured data collection through institutions such as Statistics Korea and the Korea SMEs and Startups Agency (KOSME), providing relatively consistent tracking compared to Poland's fragmented measurement ecosystem (Statistics Korea, 2024; KOSME, 2023).

Korea's Adoption Reality and Policy Response

Recent official statistics reveal that Korea faces similar adoption challenges to Poland: according to Statistics Korea (2024), only 9.2% of large enterprises and 2.9% of SMEs have achieved operational AI implementation. The Korea Federation of SMEs (KFSMB) (2025) reports a slight increase to 5.3% for SME adoption, though this remains far below the 80% of companies that recognize AI's necessity for competitiveness. This pattern mirrors Poland's experience, demonstrating how targeted government intervention can accelerate adoption.

Korea has established a diverse AI policy portfolio featuring:

- **Systematic AI and data voucher programs** providing financial support with technical assistance
- **Specialized SME support initiatives** tailored to different maturity levels and sectors
- **Multiple regulatory sandbox programs** across different sectors with streamlined approval processes

Korea's regulatory sandboxes have approved over 1,000 projects with an 85% approval rate, including 200+ AI-related projects. While the program reports 70% commercialization success rate, this figure varies significantly by sector, with fintech and digital health showing stronger outcomes than manufacturing AI applications. Despite these variations, the sandbox experience provides valuable lessons for regulatory innovation, particularly in balancing innovation promotion with risk management (Ministry of Science and ICT (MSIT), 2024a).

These policy instruments demonstrate how coordinated government efforts can effectively accelerate SME AI adoption within complex regulatory frameworks, providing a proven blueprint for addressing the persistent digital divide between large enterprises and SMEs.

1.1.3. Comparative Measurement Framework

The measurement complexity of AI adoption becomes evident when comparing Poland and Korea directly. Both countries exhibit significant variation in reported adoption rates, depending on the measurement methodology, which creates challenges for cross-national learning and policy adaptation.

<Table 2-1> Comparative AI Adoption Rates - Measurement Methodology Matters

Country	Large Enterprises	SMEs	Overall	Source & Methodology	Year
Korea	9.2%	2.9%	4.0%	Statistics Korea (actual operational use)	2024
	48.8%	28.7%	30.6%	Korea Chamber of Commerce and Industry (KCCI) (includes pilot projects)	2024
	65%	35%	-	Ministry of Trade, Industry and Energy (MOTIE) & E-Consumer Survey (AI utilization)	2025

Country	Large Enterprises	SMEs	Overall	Source & Methodology	Year
		5.3%	-	KFSMB (operational use)	2025
Poland	-	3.7%	3.7%	EU Digital Decade Report (full AI adoption)	2024
	-	5.9%	5.9%	GUS (any AI technology use)	2024
	-	25%	30%	AWS Barometer Report (AI integration in operations)	2024
EU Average	30%	7%	8%	EU Digital Decade Report	2024

Note: Variations reflect fundamental differences in measurement methodologies. "Operational use" measures full integration with business transformation, while "AI utilization" includes experimental applications and third-party tools.
Source: Statistics Korea (2024); KCCI (2024); MOTIE & E-Consumer via KPI News (2025); KFSMB (2025); European Commission (2024a); GUS (2024); Amazon Web Services & Strand Partners (2024a).

Korea's Measurement Approach

While Korea shows significant variation in AI adoption statistics, its government institutions and major industry associations provide relatively consistent categorization:

- Operational implementation requiring business transformation: 2.9-5.3%
- Pilot projects in testing phase: 28.7%
- Broad AI utilization including third-party tools: 35%

These measurements from established institutions provide insight into the various stages of AI adoption, despite the wide statistical range.

Poland's Measurement Landscape

Poland's AI adoption statistics derive from multiple sources with less institutional coordination:

- EU-wide surveys: 3.7%
- National statistical office: 5.9%
- Private sector studies: 25-30%

While both countries face measurement challenges, Korea's relatively more structured approach through government statistical agencies and industry associations provides clearer categorization of adoption stages. This measurement complexity underscores the importance of establishing consistent metrics for policy evaluation and cross-national learning.

1.2. Objectives and Scope

This research aims to develop comprehensive strategies to accelerate AI adoption among Polish SMEs through building an AI innovation ecosystem and developing innovation-friendly regulatory frameworks that balance innovation with necessary protections while maintaining EU compliance.

Specific objectives include:

1. Developing an AI innovation ecosystem strategy that provides necessary governance, support systems, and multi-stakeholder collaboration mechanisms
2. Designing an EU-aligned regulatory framework, including a regulatory sandbox system supporting diverse innovation scales
3. Establishing an integrated policy framework that includes specialized voucher programs and coordinated support mechanisms
4. Leveraging Korea's best practices through comparative analysis and adaptation to Poland's institutional context

The analysis covers both innovation ecosystem and regulatory dimensions while focusing on SMEs with fewer than 250 employees. Emphasis will be placed on ensuring these strategies are aligned with European Union standards while remaining responsive to Poland's unique economic and regulatory environment. The geographic scope encompasses Poland's primary innovation centers as well as rural regions, with the aim of enhancing accessibility to AI-driven growth opportunities for SMEs across the country. The regulatory analysis addresses EU AI Act compliance requirements and the adaptation of Korean innovations to European legal frameworks.

1.3. Methodology

This research employs a comparative case study approach combining qualitative policy analysis with quantitative benchmarking. Primary methods include:

- Comprehensive assessment of Poland's current AI ecosystem, regulatory framework, and SME adoption barriers through document analysis and expert consultations
- Systematic analysis of Korea's successful AI policies, support programs, and ecosystem development strategies
- Comparative gap analysis identifying best practices and adaptation potential
- Development of tailored policy recommendations based on theoretical frameworks and empirical evidence

Data sources encompass official government strategy documents, EU policy frameworks, OECD comparative statistics, industry reports analysis, and expert interviews with Korean and Polish policymakers and SME representatives.

1.4. Theoretical Framework

Designing effective AI adoption strategies for Polish SMEs requires theoretical foundations that explain technology diffusion processes and inform the design of policy interventions. This research integrates six complementary theoretical perspectives, progressing from individual adoption decisions to ecosystem-level coordination and system-wide transformation.

1.4.1. Core Analytical Frameworks

Innovation Diffusion Theory (Rogers, 2003) explains how innovations spread through social systems via five key characteristics: relative advantage, compatibility, complexity, trialability, and observability. The theory identifies adopter categories from innovators to laggards, providing insight into adoption timing and influence patterns. For the Polish SME AI policy, this framework explains persistent adoption hesitancy despite potential benefits, reflecting an insufficient demonstration of relative advantage and a high perceived level of complexity. Korea's voucher programs successfully address these barriers by reducing complexity through consortium partnerships and increasing observability through documented case studies.

The Triple Helix Model (Etzkowitz and Leydesdorff, 2000) describes the development of innovation ecosystems through dynamic interactions among government (policy framework and funding), industry (technology development and commercialization), and academia (research and talent development). Although some policy silos exist in all countries, Korea's AI success demonstrates effective ecosystem orchestration, avoiding the institutional fragmentation characteristic of Poland's multi-ministerial approach. This framework supports the creation of specialized coordination bodies that bridge government policy, industry needs, and academic research.

The Power and Prediction Framework (Agrawal et al., 2022) argues that AI's essential value lies in providing inexpensive, rapid, and accurate predictions that transform business decision-making structures. Most Polish SMEs currently operate at a "point solution" level (isolated AI applications) rather than a "system solution" level (comprehensive business redesign). This framework guides policies that help SMEs transition beyond incremental adoption to system-level transformation, emphasizing strategic consulting and organizational change management over mere access to technology.

1.4.2. Supporting Frameworks

The Technology Acceptance Model (TAM) extensions (Davis, 1989) address the psychological barriers faced by Polish SME leaders, emphasizing perceived usefulness and ease of use as critical factors in the adoption process. Digital Maturity Models enable segmented support programs, recognizing that Polish SMEs operate at vastly different readiness levels, from "Digital Beginners" requiring basic infrastructure to "Digital Champions" ready for advanced applications. The Technology-Organization-Environment Framework (Tornatzky and Fleischer, 1990) ensures multidimensional interventions addressing technological barriers (infrastructure support), organizational limitations (training and funding), and environmental challenges (regulatory clarity and ecosystem coordination).

Together, these frameworks provide analytical foundations for comparative analysis of Korea's ecosystem development and structured guidance for adapting successful innovations to Poland's specific institutional context and EU regulatory requirements.

2. Korea's Current Status and Cases: AI Innovation Ecosystem and Regulatory Innovation for SMEs' Digital Transformation

2.1. Korea's National AI Strategy and SME AI Strategy

2.1.1. Evolution of Korea's National AI Framework (2019-2025)

Korea has systematically developed one of the world's most comprehensive AI governance frameworks through iterative policy evolution spanning six years. This methodical approach demonstrates how countries can build sophisticated AI ecosystems through phased development rather than attempting comprehensive solutions immediately. The foundation was established with the National AI Strategy (2019), which positioned AI as a core driver of national competitiveness and established the basic institutional architecture. The strategy set forth ambitious targets: becoming a global top-4 AI power by 2030, with AI contributing 455 trillion KRW to GDP and creating 900,000 jobs (MSIT, 2019). Building on this foundation, the Trustworthy AI Strategy (2021) emphasized human-centered AI principles and ethical frameworks, while the Digital Strategy (2022) integrated AI within broader digital transformation objectives, recognizing the interconnected nature of digital technologies. The AI Innovation Strategy (2023) marked a significant advancement by establishing sector-specific implementation roadmaps and concrete performance indicators. The recent AI/Digital Growth Strategy (2024) demonstrates Korea's commitment to becoming a global leader in AI, setting even more ambitious targets for corporate adoption of AI. Most significantly, the Framework Act on Artificial Intelligence Development and Establishment of a Foundation for Trustworthiness (AI Framework Act), enacted on January 22, 2025, and effective from January 22, 2026, represents the first comprehensive AI legislation in the Asia-Pacific region and establishes fundamental legal foundations for AI development and utilization. This legislative progression reflects a sophisticated understanding of AI governance challenges, evolving from a broad strategic vision to specific regulatory frameworks that balance the promotion of innovation with risk mitigation—providing a valuable roadmap for Poland's AI strategy development.

2.1.2. Institutional Governance

Korea's national AI governance model is institutionalized under the AI Framework Act. Korea's AI governance development demonstrates a pragmatic institution-first approach where operational arrangements preceded legal codification. The National Committee on AI was operationally established by the Presidential Office in early 2024, formally launched in September 2024, and has been continuously operating since then. The Committee now operates under Article 7 of the AI Framework Act, with full implementation of the Act scheduled for January 2026. Similarly, the AI Policy Center was established within MSIT as an operational unit before receiving formal legal basis in Article 11. At the same time, the AI Safety Institute was created as a specialized unit in 2024 and

later received legal foundation in Article 12. This sequential development allowed Korea to test institutional arrangements, refine coordination mechanisms, and demonstrate effectiveness before creating permanent legal frameworks.

National AI Committee

The National AI Committee represents Korea's highest-level AI governance body with a distinctive public-private composition designed to ensure industry-driven policy development.

Committee composition and leadership are as follows:

- **Chair:** President of Korea (ensuring highest-level political commitment)
- **Membership Structure:** Majority of members from the private sector to enable industry-driven AI policies
- **Government Members:** Ministers from MSIT, MOTIE, the Ministry of SMEs and Startups (MSS), and other relevant agencies
- **Private Sector Experts:** AI industry leaders, researchers, legal and ethical safety specialists, ensuring practical policy development

Core responsibilities and functions are as follows:

- **Policy Coordination:** Deliberate and resolve major AI development policies across all government ministries
- **Strategic Planning:** Oversee the Basic AI Plan development every three years (coordinated with MSIT)
- **Regulatory Framework:** Provide recommendations on AI ethics, safety standards, and regulatory improvements
- **Investment and Infrastructure:** Coordinate policies on AI investment, infrastructure development, and resource allocation
- **Industry Promotion:** Guide comprehensive AI industry development strategies and international competitiveness enhancement
- **Cross-Sector Coordination:** Ensure coherent AI policies across education, labor, economy, and cultural sectors

The Committee's ambitious target-setting demonstrates effective integrated governance, aiming to achieve 70% AI adoption in corporate sectors and 40% in manufacturing by 2030, which requires coordinated implementation across multiple ministries and agencies (Korean Government, 2023; Korea Economic Institute of America, 2024).

Supporting Institutional Framework

- **AI Policy Center** (Article 11): Guides policy development implementation, supports AI-related professional skills development, analyzes societal impacts and trends, and provides technical policy support to the Committee
- **AI Safety Institute** (Article 12): Defines and analyzes AI safety risks, researches AI safety policies and evaluation standards, develops AI safety technologies and standardization frameworks, and promotes international cooperation on AI safety

2.1.3. SME-Specific AI Challenges and Strategic Response

Despite Korea's advanced AI framework, SMEs face adoption barriers remarkably similar to those identified in Poland. According to KOSME (2023), AI adoption rates reveal a persistent digital divide, with large companies achieving a 28.1% adoption rate, while SMEs lag significantly at 2.7%. This gap mirrors Poland's experience, where large enterprises lead in adoption, while smaller companies face barriers related to cost, expertise, and infrastructure. Korea's strategic response demonstrates how targeted government intervention can effectively bridge this gap. The government developed an integrated support ecosystem specifically addressing SME constraints through three complementary approaches: demand-driven voucher programs that reduce financial barriers, capability-building initiatives that address skills gaps, and regulatory innovation that reduces compliance burdens while maintaining necessary protections.

2.2. Legal and Regulatory Framework for AI

2.2.1. The AI Framework Act: Comprehensive Legal Foundation

The AI Framework Act represents a paradigm shift from traditional technology regulation toward outcome-based governance that explicitly supports the adoption of AI by SMEs. The Act's architecture demonstrates how comprehensive AI legislation can promote innovation while maintaining necessary safeguards.

- **A Tiered□Risk-Based Regulatory Structure:** The Act establishes a tiered approach, distinguishing between different categories of AI systems with varying regulatory requirements. High-impact AI systems in critical sectors (healthcare, energy, public services) face specific obligations, including transparency requirements, safety assessments, and human oversight provisions (Article 34). Providers or deployers of high-impact AI systems are encouraged to conduct human rights impact assessments, and such assessments are recommended for priority consideration in public procurement (Article 35). High-performance AI systems that exceed the computational thresholds set by Presidential Decree are subject to additional safety measures, risk management systems, and compliance reporting requirements (Article 32). Generative AI systems must implement mandatory user notification and content labeling requirements, ensuring users are informed when AI-generated content is being used (Article 31). Meanwhile, general AI applications commonly used by SMEs—such as business analytics, customer service chatbots, and process optimization tools—face minimal regulatory burden, enabling experimentation and adoption while maintaining basic safety standards.

- **SME Support Mandates:** The Act includes explicit support provisions for SMEs, recognizing that effective AI governance requires enabling widespread adoption rather than merely regulating advanced applications. Key provisions include:
  - Government assistance mandates for AI adoption support
  - Technological standardization requirements to reduce implementation costs
  - Access guarantees to AI data centers and training datasets
  - Simplified compliance procedures for low-risk AI applications
- **Innovation Enablement Framework:** Unlike restrictive regulatory approaches, the Act emphasizes fostering AI development through infrastructure support, standardization initiatives, and public-private collaboration mechanisms specifically designed to assist SMEs and startups in AI adoption and development.

2.2.2. Data Regulation Framework: Innovation-Friendly Foundation

Korea's data regulation reforms provide crucial foundations for AI development while maintaining robust privacy protections. The comprehensive amendments to three key data-related laws in 2020, collectively referred to as the "Three Data Laws," along with subsequent amendments through 2025, represent comprehensive data governance reform that enables AI innovation.

The Three Data Laws (2020) Initial Amendments:

- **Personal Information Protection Act (PIPA):** Introduced pseudonymized data processing (Article 28-2) and established the Personal Information Protection Commission as an independent regulatory authority (Article 7)
- **Credit Information Use and Protection Act:** Expanded available financial data scope and established data portability rights in the financial sector (Articles 33-2, 37-2)
- **Act on Promotion of Information and Communications Network Utilization and Information Protection:** Transferred personal information protection provisions to PIPA and streamlined regulatory oversight

Post-2020 PIPA Amendments: AI-Relevant Developments

Significant amendments in 2023-2025 directly impact AI utilization:

- **Automated Decision-Making (ADM) Provisions (Article 37-2):** Data subjects gained explicit rights to reject automated decisions, request explanations of AI decision criteria, and obtain human review of automated processes. These provisions require AI operators to implement transparency measures and obtain specific consent for automated processing (PIPC Guidelines on ADM, 2024).

- **MyData Expansion (Articles 17-2□39-2):** In 2025, amendments to the Personal Information Protection Act (Articles 17-2, 39-2) extended the MyData initiative from financial services to additional sectors, including healthcare, telecommunications, and energy, supported by a unified MyData platform (onmydata.go.kr). This expansion creates legitimate, user-consented pathways for SMEs to access a wider range of datasets for AI development, while maintaining strong privacy protections and compliance requirements (PIPC, 2025).
- **Cross-Organizational Data Collaboration:** Korea's framework enables secure, standardized data sharing between organizations through explicit provisions (Articles 17, 18 of the Personal Information Protection Act) and specialized protocols, supporting consortium-based AI projects and industry-specific data pools, particularly benefiting SMEs unable to establish such infrastructure independently.
- **AI Development Implications for SMEs:** MyData expansion offers SMEs new data access pathways for AI development based on user consent, while dedicated government guidelines on explainable AI and streamlined consent procedures (PIPC, 2024) reduce regulatory complexity, making compliance more accessible for SMEs.

This evolving regulatory framework demonstrates Korea's approach to balancing AI innovation enablement with robust privacy protection, providing a practical model for Poland's AI governance development within EU regulatory constraints.

2.2.3. Sectoral AI Guidelines: Industry-Specific Frameworks

Korea's approach to AI governance acknowledges that various sectors face distinct challenges, risks, and opportunities. Rather than applying uniform regulations across all industries, the government has developed comprehensive sector-specific guidelines that provide clear guidance while enabling innovation.

- **Healthcare AI Guidelines**: Address clinical validation requirements for AI medical devices, explainability standards for diagnostic systems, data quality and representation requirements, continuous monitoring protocols, and integration standards with existing healthcare information systems. These guidelines provide clarity for AI developers while ensuring patient safety and data protection.
- **Financial Services AI Guidelines**: Focus on algorithmic fairness in credit decisions, transparency requirements for automated financial services, risk management frameworks for AI-driven products, customer protection measures, and model governance requirements. The guidelines enable innovation while protecting financial stability and consumer interests.
- **Transportation and Education Guidelines**: Similar sector-specific frameworks address autonomous vehicle safety standards, liability frameworks, ethical AI use in educational assessment, and accessibility requirements for AI-enhanced learning tools.

This sectoral approach enables SMEs to navigate regulatory requirements within their specific industries while providing clear guidance for compliance and innovation pathways.

2.3. Governance Structure for AI Innovation

2.3.1. Multi-Stakeholder Coordination Model

Korea's governance structure illustrates the importance of coordination among government, industry, academia, and civil society in developing an effective AI ecosystem. The architecture comprises several complementary mechanisms that together create comprehensive support for AI innovation—many of which address the policy and capacity challenges Poland also faces.

- **Public-Private AI Partnerships:** Structured collaboration frameworks for joint projects, including industry-specific initiatives, technology development programs, and commercialization support. These partnerships leverage government resources and regulatory flexibility with private sector innovation and market knowledge. For example, AI Hub (aihub.or.kr), funded and managed by the National Information Society Agency, offers over 600 public AI datasets and cloud-based AI computing infrastructure. Startups and SMEs in sectors such as manufacturing, healthcare, and smart logistics utilize these data for product development and prototype testing—illustrating a model for closing the resource gap for smaller firms. The Seoul Metropolitan Government's partnership with IBM, which developed an AI-powered virtual assistant for city services during COVID-19, demonstrates how strategic public-private alliances can rapidly deploy AI for social needs.
- **Industry-Academia Collaboration:** Systematic connections between research institutions and commercialization needs, supported by government funding, regulatory flexibility for research projects, and structured technology transfer mechanisms. The collaboration model ensures that academic research addresses practical business needs, providing SMEs with access to cutting-edge research capabilities. Notably, AI Convergence Innovation Graduate Schools (run nationwide) are co-designed by universities and industry, ensuring curricula directly fit business demands. This approach could support Poland's aim to retain STEM graduates in its domestic AI sector. Partnerships like KAIST and Google, or Samsung's AI research investments at leading Korean universities, accelerate cutting-edge research and practical upskilling, facilitating joint R&D tailored to regional industries.
- **Regional Innovation Centers:** Local hubs supporting regional AI ecosystems, particularly important for non-capital region development and ensuring that AI innovation benefits extend beyond major metropolitan areas. These centers provide localized support, industry-specific expertise, and connections to both national programs and local business networks. The Gwangju National AI Industrial Complex is a flagship, housing an AI national data center, providing high-level training through its "AI academy," and linking local SMEs to both academic resources and national tech programs. Similar hubs in Busan and Daegu adapt the model to regional specializations (e.g., marine transport AI, manufacturing process AI)—a strategy Poland could consider in the context of its smart specialization policies and EU regional funding streams.

Each example is not just a point-in-time initiative but part of a long-term national effort to systematize collaboration and reduce regional and SME-specific innovation gaps. When adapting such models, Poland may want to analyze how Korean public funding, data infrastructure, and

targeted education programs are linked and coordinated to achieve effective scaling, localization, and sustainability.

2.3.2. Budget and Investment Coordination

Korea's integrated approach extends to financial coordination, ensuring that various support programs complement one another rather than compete. The MSS announced a KRW 15.2488 trillion (EUR 9.8 billion) budget for 2025, with specific priorities including:

- Fostering deep-tech startups in AI and fabless semiconductor sectors
- Supporting AI-enabled SME exports and global market entry
- Establishing global startup hubs to attract international talent and investment
- Creating AI-focused incubation and acceleration programs (MSS, 2024a)

This coordinated investment approach maximizes effectiveness for SME beneficiaries by ensuring clear program differentiation, complementary support mechanisms, and streamlined access procedures. Korea's governance framework provides the institutional foundation for the development of its AI ecosystem. Building on this foundation, the government has implemented comprehensive support programs that directly address SME adoption barriers through targeted interventions.

2.4. SME-Targeted Support Programs

Korea's comprehensive support system addresses the three primary barriers identified in Poland—prohibitive costs, data scarcity, and expertise deficits—through integrated voucher programs and capability-building initiatives. These programs demonstrate how systematic government intervention can accelerate the adoption of AI among SMEs while fostering sustainable ecosystem development.

2.4.1. Korea’s Integrated Voucher System Architecture

2.4.1.1 Strategic Design Principles

Korea's voucher system operates on four fundamental design principles that distinguish it from traditional subsidy programs and create sustainable ecosystem effects:

- **Demand-Driven Approach**: Unlike supply-side technology push programs, Korea's voucher system prioritizes actual business needs identified by SMEs themselves. This approach ensures that supported projects address real market challenges rather than predetermined technology solutions, leading to higher success rates and sustainable adoption.

- **Ecosystem Development Focus**: The programs support both demand (SME users) and supply (technology providers) sides simultaneously, creating sustainable business relationships and market development rather than one-time interventions. This dual-sided approach catalyzes market growth and reduces long-term dependence on government support.
- **Consortium-Based Implementation**: All major voucher programs require partnerships between SMEs and qualified technology providers, ensuring knowledge transfer, capability building, and reduced implementation risks. The consortium approach creates structured relationships that extend beyond project completion.
- **Graduated Support Structure**: Support levels and requirements vary based on project complexity, company size, and technology sophistication, enabling programs to serve SMEs at different digital maturity levels while maintaining cost-effectiveness.

2.4.1.2 Integrated System Overview

Korea's three primary voucher programs demonstrate a systematic approach to addressing different aspects of SME AI adoption barriers. The following comparison illustrates how each program targets specific challenges while maintaining complementary functionality within the integrated support ecosystem.

<Table 2-2> Korea's Integrated Voucher System Detailed Comparison

Program	Maximum Support	Implementation Period	Consortium Requirement	Target Barrier	Success Metrics
Data Voucher	EUR 40,000 (KRW 60M)	6-10 months	Data consumer + supplier	Data scarcity	7,376 applications (2023)
AI Voucher	EUR 133,000 (KRW 200M)	9-12 months	SME + AI solution provider	Cost & expertise	1,500+ companies supported
Smart Service	EUR 67,000 (KRW 100M)	6-9 months	Service business + ICT provider	Sector-specific adaptation	2,000+ service businesses

Source: MSIT (2024); MSS (2023); World Bank (2024).

This integrated voucher system represents a core element of Korea's success in SME AI adoption. Each program targets different barriers, operating complementarily, and enables SMEs to build AI capabilities progressively through structured support pathways.

2.4.2. Data Voucher Program: Comprehensive Implementation Model

2.4.2.1 Program Architecture and Strategic Context

The **Data Voucher Program** represents Korea's most significant innovation in addressing constraints in the SME data ecosystem. Managed by the Korea Data Agency (K-DATA) since 2019, the program demonstrates how systematic government intervention can transform data access barriers into opportunities for ecosystem development.

Strategic Timing and Context: Korea introduced the program during a period of significant public sector data transparency and emerging discussions about the utilization of private data. This timing enabled the program to leverage diverse, high-quality data from both public and private sources, establishing productive relationships between data suppliers and consumers that formed the foundation for ecosystem growth.

Three-Track Support Structure:

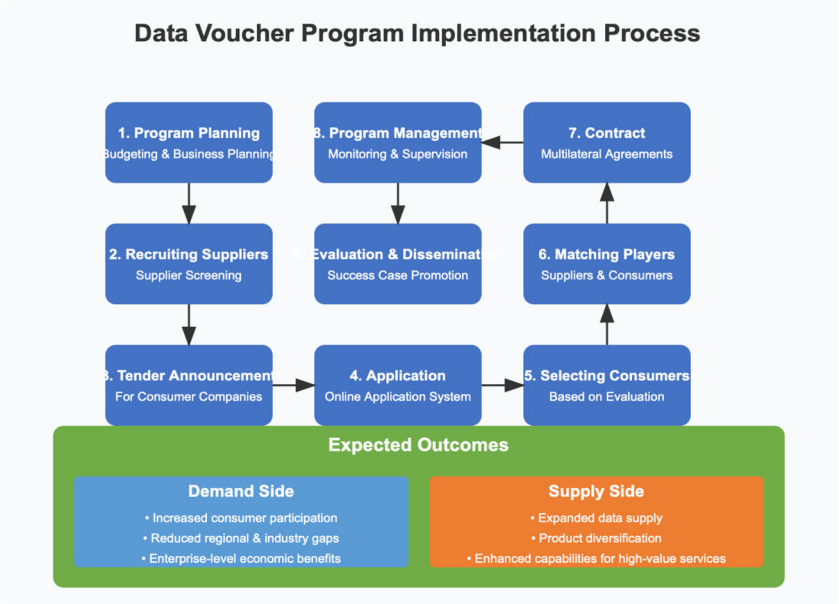
- **Purchasing Vouchers:** Support data acquisition costs, including APIs, enabling companies to access external datasets for marketing strategies, business intelligence, and product development
- **General Processing Vouchers:** Cover data processing service costs for analytics, visualization, and basic machine learning applications
- **AI Processing Vouchers:** Support advanced data processing using AI technologies, enabling sophisticated product development and business process optimization

2.4.2.2 Detailed Implementation Process

The program operates through a sophisticated nine-step process that ensures quality control, appropriate matching, and effective outcomes:

- **Phase 1: Program Planning and Supplier Development (Steps 1-2)** K-DATA begins each program cycle with comprehensive planning and budgeting, followed by rigorous supplier recruitment and screening. Supplier qualification involves assessing technical capabilities, verifying financial stability, and evaluating compliance, ensuring that participating data providers can deliver high-quality services.
- **Phase 2: Demand Generation and Application (Steps 3-4)** Public tender announcements through K-DATA's website generate SME applications through an integrated online system. The application process requires detailed business plans demonstrating specific data needs, expected outcomes, and implementation timelines.
- **Phase 3: Selection and Matching (Steps 5-6)** K-DATA prioritizes applications based on innovation potential, business viability, and alignment with national digital transformation goals. The subsequent matching process involves both online and offline interactions between suppliers and consumers, ensuring compatibility and a shared understanding of the project.
- **Phase 4: Implementation and Monitoring (Steps 7-9)** Rigorous contract management involves multilateral agreements between consumers, suppliers, and K-DATA, which define roles, responsibilities, and deliverables. Continuous program management involves regular progress monitoring, quality assurance, and technical support. Final evaluation and dissemination activities capture lessons learned and promote successful cases.

[Figure 2-1] Korea's Data Voucher Program Implementation Process



Note: Adapted and expanded by the author from World Bank Group Korea Office (2024).
Source: Author (Yoon, 2025).

2.4.2.3 Performance Results and Economic Impact

Korea's voucher programs demonstrate concrete business transformation through specific enterprise success stories. In manufacturing, a mid-sized automotive parts manufacturer utilized the AI Voucher Program to implement computer vision quality inspection systems, achieving a 40% reduction in defect rates, a 60% reduction in inspection time, and an 8-month return on investment. The success model was subsequently adopted by 12 companies in the same industry cluster, demonstrating the program's scaling effect.

Service sector transformation is exemplified by a regional retail chain that leveraged the Smart Service Support Program to deploy AI-powered customer service chatbots. The implementation resulted in a 70% reduction in customer response time and 25% improvement in customer satisfaction scores, enabling successful expansion to three additional locations within 18 months.

Agricultural innovation showcases the program's reach across traditional sectors, as a family-owned agricultural business integrated IoT-AI systems for crop growth prediction through the Data Voucher Program. The implementation delivered a 30% increase in crop yield and a 25% reduction in energy costs, with knowledge transfer extending to 8 neighboring farms through the consortium model.

The program's effectiveness is evidenced by remarkable growth metrics documented in the World Bank's comprehensive 2024 analysis:

Quantitative Performance Indicators:

- **Application Growth:** 164% increase from 2,795 (2019) to 7,376 (2023) applications.
- **Competition Intensity:** Competition ratio increased from 1.7:1 to 3.7:1, indicating strong demand.
- **Regional Inclusion:** Non-capital region participation increased from 27.8% to 40.6%.
- **Sectoral Diversification:** Non-ICT company participation rose from 38.0% to 74.6%.

Economic Impact Results:

- **Revenue Growth:** Participating company revenues increased 38-fold from KRW 330 billion (2019) to KRW 12,636 billion (2023).
- **Employment Creation:** 28,748 new jobs created since program inception.
- **Investment Attraction:** KRW 269 billion in domestic and foreign investment facilitated.
- **Intellectual Property:** 1,526 IP rights acquired, and 53 companies achieved public listing.

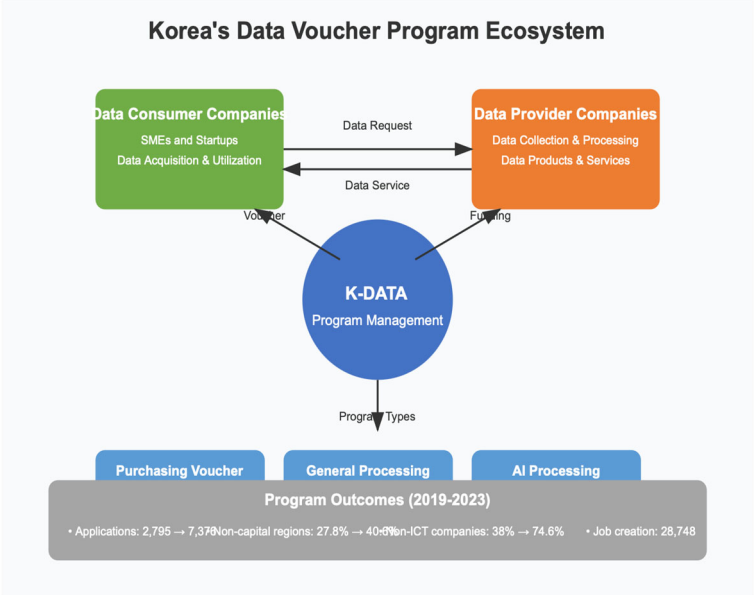
2.4.2.4 Virtuous Cycle Effects and Ecosystem Development

The program's most significant achievement involves creating self-sustaining data ecosystem dynamics. K-DATA documented 38 cases where data consumers successfully transitioned to supply companies, demonstrating the program's role in ecosystem expansion rather than mere one-time support.

Sector-Specific Transition Examples:

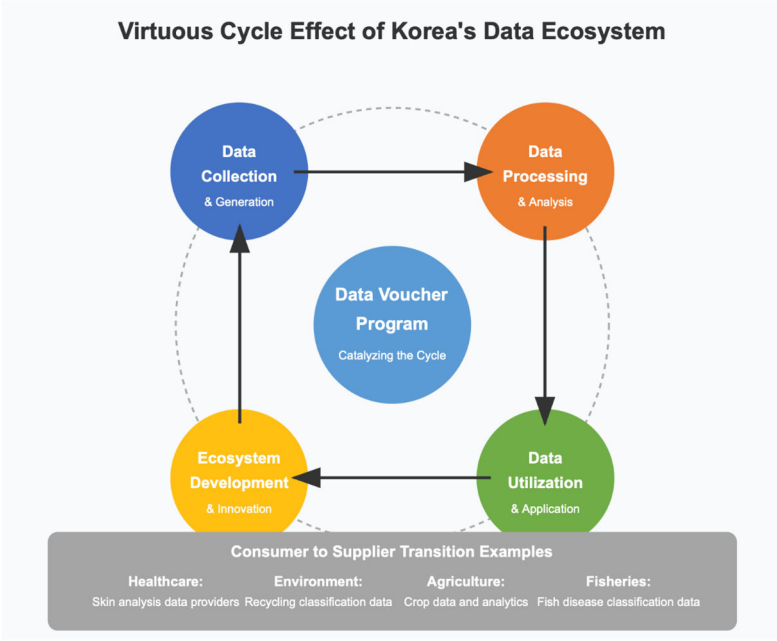
- **Healthcare:** Companies developing AI-powered skin analysis algorithms now provide dermatological analysis data to other firms.
- **Environment:** Businesses creating AI-based recycling systems offer environmental classification data.
- **Agriculture:** Enterprises developing smart farming solutions supply agricultural monitoring and disease prediction data.
- **Manufacturing:** Firms implementing AI supply chain management provide industry-specific logistics and production data.

[Figure 2-2] Korea's Data Voucher Program Ecosystem



Note: Adapted and expanded by the author from World Bank Group Korea Office (2024).
Source: Author (Yoon, 2025).

[Figure 2-3] Virtuous Cycle Effect of Korea's Data Voucher Program Ecosystem



Note: Adapted and expanded by the author from World Bank Group Korea Office (2024).
Source: Author (Yoon, 2025).

2.4.3. AI Voucher Program: Advanced Solution Implementation

2.4.3.1 Program Structure and Implementation Mechanisms

The **AI Voucher Program**, introduced in 2020, builds on the success of the Data Voucher Program while focusing specifically on the adoption of comprehensive AI solutions. The program

has supported over 1,500 companies implementing AI solutions across diverse industries, demonstrating scalable approaches to AI adoption support.

Program Architecture:

- **Supervision:** MSIT provides strategic oversight and policy coordination.
- **Operation:** The National IT Industry Promotion Agency (NIPA) manages the day-to-day program implementation.
- **Budget Scale:** KRW 38.5 billion (EUR 26.5 million) in 2024, supporting comprehensive AI implementations.
- **Support Level:** Up to KRW 300 million (EUR 206,000) per company for complex AI projects.

2.4.3.2 Consortium-Based Implementation Model

The program's consortium requirement creates structured partnerships between SMEs and certified AI solution providers, ensuring effective knowledge transfer and sustainable capability building:

Consortium Formation Process:

(1) **SME Application:** Companies submit detailed AI implementation plans specifying business challenges, expected outcomes, and resource requirements.

(2) **Provider Qualification:** AI solution providers demonstrate technical capabilities, relevant experience, and project management competencies.

(3) **Matching and Negotiation:** NIPA facilitates consortium formation through structured matching processes and joint planning sessions.

(4) **Joint Implementation:** Consortia execute projects with shared responsibilities, regular milestone reviews, and collaborative problem-solving.

Knowledge Transfer Requirements:

- **Technical Training:** Solution providers must deliver hands-on training to SME personnel.
- **Documentation Standards:** Comprehensive project documentation and methodology transfer.
- **Ongoing Support:** Post-implementation support periods to ensure sustainable AI utilization.
- **Capability Assessment:** Regular evaluation of SME internal AI capabilities development.

2.4.3.3 Sectoral Focus Areas and Application Domains

The program maintains a strategic focus on sectors with high AI adoption potential and significant SME presence.

Primary Focus Sectors:

- **General Industry:** Manufacturing optimization, quality control, and predictive maintenance.
- **Medical Sector:** Diagnostic support, patient monitoring, and healthcare workflow optimization.
- **AI Semiconductors:** Hardware-software integration and specialized AI chip applications.
- **Small Business Services:** Customer service automation, business analytics, and operational efficiency.
- **Global Expansion:** AI-enabled international market entry and export facilitation.

2.4.4. Smart Service Support Program: Service Sector Digital Transformation

2.4.4.1 Program Design and Voucher Structure

The **Smart Service Support Program**, administered by the MSS, specifically addresses service sector digital transformation through a comprehensive voucher-based approach. The program recognizes that service businesses require specialized support to enhance customer experience and integrate business processes.

Voucher-Based Support Structure:

- **Financial Support Range:** KRW 60-100 million (EUR 40,000-67,000) per project.
- **Project Duration:** 6-9 months implementation periods with extended support options.
- **Consortium Requirements:** Mandatory partnerships between service businesses and qualified ICT providers.
- **Sector Focus:** Retail, hospitality, professional services, and traditional service industries.

Program Implementation Features:

- **Solution-Oriented Approach:** Support for ICT implementations that directly enhance service delivery capabilities.
- **Business Process Integration:** Emphasis on comprehensive digital transformation rather than isolated technology adoption.
- **Scalable Implementations:** Solutions designed to grow with business expansion and changing needs.
- **Performance Measurement:** Systematic tracking of productivity improvements, customer satisfaction, and business model innovation.

2.4.4.2 Consortium Approach and Knowledge Transfer

The program's consortium model ensures sustainable capability building through structured partnerships.

Partnership Structure:

- **Service Business Responsibilities:** Business process analysis, user requirement specification, and staff training coordination.
- **ICT Provider Obligations:** Technical solution development, implementation support, and ongoing maintenance.
- **Joint Accountability:** Shared responsibility for project success, knowledge transfer effectiveness, and long-term sustainability.

Knowledge Transfer Mechanisms:

- **Collaborative Problem Definition:** Joint analysis of business challenges and solution requirements.
- **Staff Training Programs:** Comprehensive digital skills development for service business employees.
- **Documentation and Methodology Transfer:** Detailed process documentation and best practices sharing.
- **Post-Implementation Support:** Extended technical assistance and optimization guidance.

2.4.4.3 Performance Results and Business Impact

Since 2019, the program has supported over 2,000 service businesses, resulting in documented improvements across multiple performance dimensions.

Productivity Enhancement Results:

- **Operational Efficiency:** Average 25-40% improvement in service delivery time.
- **Cost Reduction:** 15-30% reduction in administrative and operational costs.
- **Revenue Growth:** 20-35% increase in revenue for participating businesses.

Customer Experience Improvements:

- **Service Quality:** Enhanced consistency and reliability of service delivery.
- **Customer Satisfaction:** Measurable improvements in customer feedback and retention.
- **Market Reach:** Expanded market access through digital channels and online presence.

2.4.5. AI Factory: From Smart Factory Limitations to Next-Generation Service Model (2024-2025)

Korea's AI Factory concept emerged as a strategic response to the fundamental limitations of Smart Factory initiatives. While Smart Factory programs successfully digitalized 30,000 manufacturing SMEs, they encountered a critical barrier: SMEs could automate processes but lacked the capabilities to develop and manage AI systems that enable true intelligent manufacturing (MSS, 2024b). Building on the success of voucher programs and recognizing persistent SME capability gaps, Korea introduced the AI Factory in 2024 as an evolved AI-as-a-Service business model (MSIT, 2024b). This represents a paradigm shift where AI models are produced, sold, and continuously managed according to customer demand, fundamentally restructuring the market from individual AI development to centralized AI service provision.

Key features include custom AI model production for SMEs without in-house capabilities, continuous management and updates, integration projects spanning large-scale manufacturing to medium-sized enterprises, and planned integration of humanoid robotics by 2025. The model addresses the reality that 97.1% of SMEs cannot afford in-house AI teams, transforming fixed AI development costs (200 million won) into variable service fees (20 million won per project) (KIET, 2024). This evolution from subsidy-based support to market-driven service ecosystems demonstrates Korea's strategic shift toward sustainable AI adoption models. While Korea is not necessarily ahead of Poland in AI Factory implementation—both countries are in early stages—Korea's concrete planning offers valuable insights for how Poland could leverage its PIAST infrastructure for similar service-based models that address both infrastructure and capability gaps simultaneously.

2.4.6. Education and Capability Building Programs

2.4.6.1 Comprehensive Human Capital Development Framework

Korea's approach to SME AI adoption includes substantial investment in capability-building programs that directly address the human capital constraints identified in Poland. The programs operate through multi-stakeholder partnerships involving government agencies, educational institutions, and private sector organizations.

Multi-Level Education Architecture

<Table 2-3> Korea's AI Education Support Programs - Detailed Structure

Program Level	Target Audience	Duration	Subsidy Level	Curriculum Focus	Delivery Method
Executive Leadership	SME CEOs/CTOs	2-3 weeks intensive	KRW 5M	AI strategy, ROI analysis	Case studies, peer learning
Technical Specialists	R&D Personnel	320+ hours	Variable	ML/AI implementation	Hands-on labs, projects
Operational Staff	General employees	Project-based	Variable	AI tool usage, data literacy	Online/offline hybrid
Cross-Functional Teams	Mixed levels	Flexible	Variable	Collaborative AI projects	Team-based learning

Source: Ministry of Employment and Labor (2024); MSS (2024c).

This multi-level education architecture provides customized capability development that accommodates diverse AI maturity levels among SMEs. The comprehensive approach, spanning from executive leadership to operational staff, is particularly effective in enhancing an organization's capacity for AI acceptance and implementation.

2.4.6.2 Industry-Academia Collaboration Programs

- **KAIST AI Bootcamp Model:** Advanced 320-hour programs targeting R&D personnel with KRW 5 million subsidies, delivered through partnerships between the Seoul Government and leading universities. The curriculum includes machine learning fundamentals, AI application development, and industry-specific implementation strategies.
- **Team Sparta Training Initiative:** Project-based learning programs focusing on generative AI, data analysis, and collaborative problem-solving through team hackathons and real-world business challenges. Programs adapt to emerging AI technologies and market demands.
- **CEO AI Leadership Development:** Intensive programs helping SME executives understand AI strategic implications, investment decisions, and organizational change management required for successful AI adoption.

2.4.6.3 Digital Maturity Assessment and Personalized Development

The education system includes comprehensive digital maturity assessment tools that provide personalized development pathways based on current organizational capabilities.

Assessment Dimensions:

- **Technical Infrastructure:** Current IT systems, data management capabilities, and technology readiness.
- **Human Resources:** Staff digital skills, leadership AI understanding, and learning capacity.

- **Business Processes:** Process digitization level, data utilization maturity, and change management capabilities.
- **Strategic Alignment:** AI vision clarity, investment readiness, and performance measurement systems.

Personalized Development Pathways:

- **Digital Beginners:** Basic digital literacy and foundational AI understanding.
- **Intermediate Users:** Specific AI tool training and implementation support.
- **Advanced Adopters:** Sophisticated AI strategy development and optimization techniques.
- **Digital Champions:** Peer mentoring and ecosystem leadership development.

2.4.7. Other Supporting Programs: Comprehensive Ecosystem Approach

2.4.7.1 Manufacturing AI-Specialized Smart Factory Program

Administered by the MSS, this specialized program addresses Industry 4.0 transformation challenges through phased support for manufacturing SMEs.

Program Structure:

- **Support Scale:** Maximum KRW 200 million (EUR 133,000) for AI autonomous factory development.
- **Technology Focus:** AI agents, on-device AI, process optimization, and predictive maintenance.
- **Implementation Period:** Up to 9 months with extended monitoring and support.
- **Flexibility Features:** Simultaneous participation with other manufacturing innovation programs.

Phased Development Approach: The program recognizes that most SMEs require a gradual transition from traditional manufacturing to AI-powered systems. The model supports progression from basic digitization → smart factory implementation → AI-integrated autonomous operations, providing realistic development pathways for SMEs with varying technological readiness levels.

2.4.7.2 Government-Commissioned AI Analysis Services

The Korea Intelligence Information Society Agency (KIISSA) operates a unique model that provides direct government support for AI adoption.

Service Delivery Model:

- **Support Method:** Free consulting and customized development support.
- **Annual Capacity:** Support for 40 SMEs and small businesses across multiple sectors.
- **Service Content:** AI-based problem analysis, solution design, and industry-specific demonstrations.
- **Sector Coverage:** Disaster safety, environment, distribution, and emerging technology applications.

Representative Implementation Cases:

- **Edge Computing Safety Systems:** Intersection safety sensor development for traffic management.
- **Agricultural AI Applications:** Livestock facility fire risk prediction and automated monitoring.
- **Infrastructure Maintenance:** Concrete crack detection and predictive maintenance systems.

This approach significantly lowers entry barriers for initial AI adoption stages, particularly effective for SMEs with limited AI understanding or resources. While support programs address financial and capability barriers, regulatory innovation is equally crucial for enabling AI experimentation and adoption. Korea's regulatory sandbox system complements its support programs by providing safe spaces for AI innovation.

2.5. Regulatory Innovation: Regulatory Sandbox System

Effective AI governance necessitates a balanced approach that enables innovation while maintaining suitable safeguards. Korea's regulatory sandbox system offers a comprehensive model for achieving this balance through structured experimentation and evidence-based development of regulatory frameworks.

2.5.1. Comprehensive Multi-Ministry Framework

Korea's regulatory sandbox system, operational since 2019, enables systematic experimentation with AI innovations through structured regulatory flexibility. The system addresses the challenge of fostering innovation in rapidly evolving AI domains where existing regulations may not adequately accommodate new technologies or business models. Rather than comprehensive deregulation, it provides controlled environments for testing innovative applications under modified regulatory conditions. The system operates through seven ministry-level deliberation committees covering ICT Convergence, Industrial Convergence, Financial Innovation, Regulation-Free Zones, Smart Cities, R&D Special Zones, and Mobility Innovation. Each committee comprises industry experts, legal specialists, and government officials, ensuring that sector-specific expertise informs regulatory decisions while maintaining cross-government coordination. This evidence-based approach enables concurrent technology development and regulatory learning, informing permanent regulatory

frameworks through practical implementation experience rather than theoretical assessments (See Chapter 1 for further details on the Korean regulatory sandbox system).

2.5.1.1 Three Representative AI Innovation Cases

Korea's sandbox system enables different types of companies to experiment with AI innovations at appropriate scales and risk levels, accommodating diverse SME needs across different regional clusters and innovation readiness levels.

1) National-Level Innovation: Healthcare AI Diagnostic Systems

National-level sandboxes address high-risk, high-impact AI applications requiring sophisticated regulatory coordination across multiple agencies. The healthcare AI sector provides the most comprehensive examples of national-level sandbox effectiveness.

Regulatory Innovation Examples:

- **AI Medical Device Testing:** Temporary exemptions from full medical device certification for AI diagnostic tools in controlled clinical environments.
- **Remote Patient Monitoring:** Regulatory flexibility for AI-enabled telemedicine and continuous patient monitoring systems.
- **Predictive Health Analytics:** Data sharing and privacy exemptions for AI systems analyzing population health patterns.

Implementation Safeguards:

- **Mandatory Clinical Oversight:** Required medical professional supervision during sandbox periods.
- **Patient Safety Protocols:** Comprehensive safety monitoring and adverse event reporting.
- **Data Protection Measures:** Enhanced privacy protections and consent procedures.
- **Performance Evaluation:** Regular assessment of AI system accuracy and clinical outcomes.

2) Sectoral Innovation: Manufacturing AI Quality Control Systems

The Industrial Convergence sandbox, managed by the Ministry of Trade, Industry, and Energy (MOTIE), facilitates sector-specific AI innovations that require industry expertise and specialized safety standards.

Manufacturing AI Applications:

- **Quality Inspection Systems:** AI-powered visual inspection and defect detection in production lines.
- **Predictive Maintenance:** Machine learning algorithms for equipment failure prediction and optimization.
- **Process Optimization:** AI systems for production efficiency improvement and resource optimization.
- **Supply Chain Management:** AI-enabled logistics and inventory management systems.

SME-Specific Benefits: Manufacturing SMEs use sectoral sandboxes to test AI applications that would otherwise face significant regulatory barriers, enabling practical experimentation with industry-specific solutions while maintaining safety standards.

3) Regional Innovation: Autonomous Delivery Robot Case Study

The most illustrative regional-level innovation case demonstrates how local sandboxes enable practical testing while building public trust and regulatory experience.

Woowa Brothers Autonomous Delivery Robot Project (2021-2023)

- **Regulatory Challenge:** The Korean Road Traffic Law prohibits the operation of unmanned delivery robots on public roads, creating legal barriers to the development of autonomous delivery services.
- **Sandbox Solution:** The Mobility Innovation sandbox provided structured regulatory relief:
- **Limited Area Operation:** Designated demonstration zones in controlled urban environments.
- **Safety Verification Standards:** Comprehensive safety protocols and performance requirements.
- **Insurance Framework Adjustments:** Modified liability and insurance requirements for autonomous operations.
- **Public Consultation Process:** Community engagement and feedback collection procedures.

Implementation Outcomes:

- **Commercial Success:** Service launch in 4 Seoul districts with regulatory approval.
- **Efficiency Gains:** 40% improvement in delivery efficiency compared to traditional methods.
- **Innovation Development:** 12 related patents filed during the sandbox period.
- **International Expansion:** Successful technology transfer to the US and Japanese markets.

Institutional Impact: The sandbox experience informed comprehensive regulatory reform, leading to autonomous delivery law amendments and the establishment of permanent safety standards for unmanned delivery services.

This case demonstrates how regional sandboxes enable SMEs to test AI innovations in familiar local environments while building regulatory experience that informs national policy development.

2.5.2. Innovation-Safety Balance and Comprehensive Safeguards

Korea's sandbox system incorporates sophisticated safeguards that protect public safety while fostering innovation, demonstrating how regulatory experimentation can maintain public trust.

Mandatory Risk Management Requirements:

- **Comprehensive Insurance:** All demonstration projects require appropriate insurance coverage.
- **Revocation Clauses:** Clear termination procedures if safety risks emerge during testing.
- **Continuous Monitoring**: Real-time safety and performance monitoring throughout demonstration periods.
- **Public Consultation:** Community engagement processes for applications affecting public services.

Evidence-Based Regulation Development: Sandbox results systematically inform permanent regulatory frameworks, ensuring that new regulations reflect practical implementation experience rather than theoretical concerns.

2.6. Success Factor Analysis and Strategic Lessons

2.6.1. Demand-Driven Ecosystem Development

Korea's success fundamentally stems from prioritizing actual business needs over technology-push approaches, as emphasized in the World Bank's comprehensive analysis. This demand-driven strategy ensures that government support programs address real SME challenges rather than promoting predetermined technology solutions.

Key Implementation Mechanisms:

- **SME-Led Problem Definition:** Programs begin with SME identification of specific business challenges rather than government-determined technology priorities.
- **Solution Flexibility:** Support systems accommodate diverse technology approaches and implementation strategies based on individual business needs.

- **Market Validation:** Program success is measured by commercial viability and business impact rather than technology adoption rates alone.
- **Continuous Feedback Integration:** Regular program refinement based on SME feedback and market response.

2.6.2. Balanced Supply-Demand Ecosystem Support

Korea's integrated approach simultaneously develops both supply (technology providers) and demand (SME users) sides of AI markets, creating sustainable business relationships rather than temporary interventions.

Ecosystem Development Results:

- **Market Creation:** Voucher programs catalyze market development for AI and data services specifically tailored to SME needs.
- **Sustainable Business Models:** Consumer-to-supplier transitions in the data ecosystem demonstrate program success in creating self-sustaining market dynamics.
- **Reduced Government Dependency:** Successful programs gradually reduce reliance on government support as markets mature and business relationships solidify.

2.6.3. Tiered Innovation Support Architecture

The three-tier structure (national, sectoral, regional) accommodates diverse company types and innovation scales, providing appropriate support mechanisms for the different needs and capabilities of SMEs.

Strategic Advantages:

- **Risk-Appropriate Support:** Different innovation levels match different risk tolerances and regulatory requirements.
- **Scalable Implementation:** Companies can progress through support tiers as their AI capabilities develop.
- **Regional Accessibility:** Local and regional programs ensure that non-metropolitan SMEs have appropriate access to innovation support.

2.6.4. Continuous Program Adaptation and Learning

Korea's systematic approach to program refinement underscores the importance of adaptive governance in technology policy, characterized by regular evaluation and modification based on implementation experience.

Adaptation Mechanisms:

- **Annual Program Reviews:** Comprehensive evaluation of program effectiveness, participant feedback, and market impact.
- **Policy Iteration:** Regular updates to program design, eligibility criteria, and support mechanisms.
- **Best Practice Dissemination:** Systematic sharing of successful implementation models and lessons learned.
- **International Benchmarking:** Ongoing comparison with global best practices and adaptation of successful international approaches.

2.6.5. Integrated Public-Private Partnership Model

The consortium-based approach in voucher programs and multi-ministerial coordination in regulatory sandboxes demonstrate effective public-private partnerships that leverage sectoral strengths while maintaining appropriate oversight.

Partnership Effectiveness Factors:

- **Clear Role Definition:** Specific responsibilities and accountability for government agencies, private companies, and SME participants.
- **Shared Risk Management:** Balanced risk allocation that encourages private sector participation while protecting public interests.
- **Knowledge Transfer Requirements:** Systematic capability building that extends beyond individual project completion.
- **Performance-Based Evaluation:** Success metrics that align public policy objectives with private sector business goals.

2.7. Implementation Challenges and Areas for Improvement

While Korea's AI support programs demonstrate significant achievements as outlined above, recognizing implementation challenges provides valuable insights for continuous improvement and international adaptation.

2.7.1. Sustainability Considerations

The AI Voucher Program's project-based support model has raised questions about long-term sustainability. Analysis shows that approximately 30% of voucher recipients maintain active AI utilization 18 months post-support, suggesting opportunities for enhanced follow-up mechanisms (Kim and Lee, 2024). Recent stakeholder feedback indicates that SMEs would benefit from extended support periods, with industry associations identifying current programs as "single-shot support with limitations" and recommending transition to multi-year frameworks (ZDNET Korea, 2025).

2.7.2. Budget Optimization Opportunities

Evolving fiscal priorities have led to budget adjustments across various programs, with some experiencing 15-20% modifications in 2025 allocations (Ministry of Economy and Finance, 2024). Additionally, recent audit reviews identified opportunities for operational enhancement, including strengthened outcome monitoring and improved supplier qualification processes (Board of Audit and Inspection, 2025).

2.7.3. Regulatory Sandbox Evolution

The regulatory sandbox system shows varying effectiveness across sectors—while fintech demonstrates 80% commercialization rates, manufacturing AI achieves 40-50%, indicating sector-specific adaptation needs (Korea Development Institute, 2024). More critically, the EU AI Act's regulatory sandbox requirements under Article 55 demand more comprehensive and effective guarantees than Korea's current model provides, suggesting that Korea itself needs to evolve its sandbox approach to meet international standards. The transition from temporary exemptions to permanent regulatory reform remains an ongoing development area, with stakeholders seeking clearer pathways for sustained innovation. Poland may potentially benefit from designing EU-compliant sandboxes from the outset rather than adapting Korea's pre-EU AI Act model.

2.7.4. Accessibility Enhancement Potential

Current programs demonstrate higher participation among companies with established digital infrastructure, highlighting opportunities to serve micro-enterprises better (those with fewer than 10 employees), which represent 97% of all businesses. Simplifying application procedures and adjusting co-financing requirements could expand program reach to resource-constrained enterprises.

2.7.5. Insights for International Adaptation

These implementation experiences offer practical insights for countries considering similar approaches:

- Multi-year support frameworks enhance sustainability beyond initial implementation.
- Dedicated funding mechanisms provide greater program stability.
- Sector-specific sandbox approaches recognize varying innovation contexts.
- Graduated support tiers improve accessibility for enterprises at different digital maturity levels.

Understanding both strengths and areas for improvement enables more informed adaptation of successful models while incorporating lessons learned from ongoing refinements.

2.8. Conclusion: Korea’s Integrated AI Ecosystem Model

Korea's experience demonstrates that accelerating SME AI adoption requires comprehensive, coordinated approaches that address multiple barriers simultaneously rather than isolated interventions. The Korean model's effectiveness stems from systematic integration of legal frameworks, institutional coordination, financial support, and regulatory innovation that together create enabling environments for AI adoption.

- **Strategic Integration Achievements:** Korea's success results from coordinated development of legal foundations (AI Framework Act), institutional coordination (National AI Committee system), comprehensive support programs (integrated voucher system), and regulatory innovation (three-tier sandbox system) that collectively address the complex challenges of SME AI adoption.
- **Sustainable Ecosystem Development:** The program's evolution from government-supported adoption to self-sustaining market dynamics demonstrates how well-designed public intervention can catalyze permanent market development rather than creating ongoing dependency.
- **Scalable Implementation Model:** Korea's phased approach to program development, systematic evaluation and adaptation, and tiered support structure provide practical models that can be adapted to different national contexts and institutional capabilities.

For Poland, Korea's experience provides concrete evidence that coordinated government intervention can effectively accelerate SME AI adoption while maintaining necessary protections and creating sustainable ecosystem growth. The specific program designs, implementation mechanisms, and governance structures offer practical blueprints for addressing Poland's identified challenges in SME AI adoption and institutional coordination.

The subsequent comparative analysis will examine how these Korean approaches can be adapted to Poland's specific institutional context, regulatory environment, and economic conditions to achieve similar results in ecosystem development.

3. Poland's Current Status and Cases: AI Innovation Ecosystem and Regulatory Innovation for SMEs' Digital Transformation

3.1. Current Status of AI Innovation Ecosystem

3.1.1. Overview of Poland's AI Industry and Infrastructure

Poland's approach to AI and digital transformation is undergoing significant evolution, anchored by the landmark Digital Strategy for Poland until 2035, ongoing revisions to its national AI policy, and implementation of the European AI Act. These initiatives reflect the country's ambition to position itself as a regional leader in digital innovation while addressing socio-economic challenges through technology.

Poland's digital economy is experiencing rapid growth. In 2023, the Polish ICT sector was valued at approximately USD 26 billion, representing a 5.1% increase from 2022, primarily driven by growth in software and cloud services. Government recovery and resilience plans have dedicated substantial funding (over EUR 7 billion by 2030) to broadband, digital skills, e-government, and cybersecurity. Major domestic tech firms (e.g., Asseco, CD Projekt, Brainly) and innovative start-ups (such as Eleven Labs, Samurai Labs, DeepSense.ai, and Infermedica) are developing cutting-edge AI solutions.

As the development of AI requires a robust and efficient infrastructure to support all stages of the AI lifecycle, in order to cater to a wide range of stakeholders (industry, academia, government, and civil institutions), Poland is implementing new solutions while also leveraging its existing infrastructure. It has developed a broad "horizontal" AI ecosystem. The foundation of this structure consists of supercomputers (including AI Factories and Gigafactories), data centers, high-performance computing (HPC) infrastructure, and high-bandwidth connections.

AI Factories will combine computing power, data, and highly skilled professionals to foster innovation, collaboration, and experimentation in the field of artificial intelligence. These specialized AI supercomputers will enable the training of general-purpose AI (GPAI) models that require substantial computational power. The AI Factories will integrate supercomputing centers with scientific, research, and industrial entities, including SMEs and start-ups.

The most recent and significant infrastructure investments, such as the PIAST AI Factory in Poznań—a joint EU–Poland EUR 400 million initiative currently under development at the Poznań Supercomputing and Networking Center (PSNC). The AI Factory in Poznań will focus on priority sectors, including health and life sciences, cybersecurity (including quantum), space/robotics, energy and climate, and the public sector.

As Poland participates in the EuroHPC PL initiative to upgrade national high-performance computing for research and industry, other regional centers are also being strengthened. In Kraków, the Cyfronet AGH supercomputing center is expanding (a PLN 70 million investment was approved for its Helios system). The AGH University's Cyfronet launched the "Helios" supercomputer in 2024—currently the fastest system in Poland (35 petaflops peak performance, with GPU-based AI partitions). Moreover, Poland co-funds the LUMI AI project. This EUR 600 million EuroHPC supercomputer is expected to be operational by 2026, delivering over 20 exaflops for AI model training (Poland's share is EUR 10 million).

In northern Poland, the Pomeranian Digital Innovation Hub (PDIH, in Gdańsk) has been designated by the European Commission as the regional digital transformation center, specializing in Industry 4.0, robotics, AI, VR/AR, and cybersecurity for maritime and other industries. These projects, together with parallel investments in 5G networks and cloud infrastructure, are laying the groundwork for advanced AI research and innovation.

Poland is also planning to expand initiatives such as PLGrid and the National Data Repository (KMD). Of particular importance will be ensuring access to the national cloud infrastructure offered by KDM centers. This will enable the secure and regulation-compliant processing of sensitive data and will reinforce Poland's technological sovereignty.

These investments in computing infrastructure and data centers (e.g., Google, Amazon, Microsoft, and Palo Alto have all opened Polish cloud facilities) underscore Poland's commitment to a robust AI and digital backbone.

3.1.2. Current State of AI Adoption in SMEs

AI adoption in Polish firms remains modest but is on the rise. An EU Commission report (2023) found that only about 3.7% of Polish companies have fully adopted AI, well below the EU average of 8%. A more recent GUS report similarly found that by 2024, only approximately 5.9% of Polish companies reported using any AI technologies, with 94% not utilizing AI at all.

By contrast, an independent Amazon Web Services (AWS) commissioned study reports a 36% increase in business AI adoption year-on-year (the fastest in the EU), with roughly 30% of companies now integrating AI into their operations. The study finds that 83% of AI-using firms report positive business value from AI, and 79% report cost savings. Maintaining this momentum could add an estimated EUR 134 billion to Poland's economy by 2030. Sectorally, the defense and aerospace industry leads with 71% of companies employing AI (e.g., in quality control, content generation).

Despite these headline gains, Poland's SMEs remain relatively under-digitized overall. A 2024 EU report notes that over 75% of Polish companies fall into the "very low" or "low" digital intensity categories. Recent research categorizes SMEs into six segments by digital maturity—from "Uninterested" through "Ready to Act" to "Digital Champions"—and highlights that firms labelled "Ambitious without Knowledge", "Needing Support" or "Ready to Act" have the highest latent potential for AI adoption.

Market feedback confirms these trends. EY's latest survey (2024/25) shows that the share of firms completing successful AI deployments rose from 20% to 25%, and those prepared for further AI projects rose from 78% to 89% year-on-year. More than half of the surveyed companies plan to significantly increase their AI spending over the next 18 months, and a clear majority of organizations that have implemented AI report achieving the expected benefits. These indicators suggest growing strategic commitment, even as overall digitalization levels lag, underscoring an ongoing transition from experimentation to real-world deployment.

3.1.3. Key Barriers and Implementation Challenges

Polish SMEs face multiple, interlinked challenges in adopting AI. Studies (including the "Advancing Digital Transformation" project) identify categories of barriers as follows:

- **Financial/Resource Constraints:** Many SMEs cite high AI implementation costs relative to budgets and a lack of tailored financing. Limited internal funds (often tied up in day-to-day operations) and low awareness of available grants or loans hinder investment.
- **Technical and Integration Challenges:** Companies frequently lack in-house expertise to select and integrate suitable AI technologies. Legacy IT infrastructure gaps make deployment difficult.
- **Organizational and Cultural Factors:** AI initiatives often lack strategic prioritisation. Decision-making remains highly owner-driven with little expert input, and digital projects may be sidelined in favor of routine operations. Additionally, many firms exhibit resistance to change (fear of the unknown, uncertainty about benefits, preference for familiar workflows), viewing digital transformation more as a cost than an investment.
- **Regulatory Uncertainty:** A significant share of firms (especially in the defense sector) regard unclear AI regulations as a barrier – for example, 32% of surveyed defence companies cited lack of legal clarity on AI as an obstacle.
- **Skills and Talent Shortage:** There is a pronounced gap in AI-relevant skills. Companies report difficulty recruiting qualified AI/data professionals. To counteract shortages, 85% of firms say they are willing to offer higher salaries (on average, 28% higher) to attract candidates in AI, cybersecurity, and data analytics.

Together, these factors constrain SMEs' ability to innovate with AI. Overcoming them will require coordinated support (financial, advisory, and regulatory) as well as workforce development to build digital skills.

3.1.4. Analysis of Industrial Clusters and Regional Innovation Capacity

AI innovation in Poland is geographically concentrated in several hubs. The Poznań region is emerging as a leading AI cluster: the PIAST AI Factory (PSNC) is being developed in collaboration with local universities (Poznań University of Technology, Adam Mickiewicz University, Nicolaus Copernicus University) and industrial partners. In Kraków, the Cyfronet AGH center is key—its

enhanced Helios supercomputer (with recent PLN 70 million funding) will integrate with European AI networks. In the Tri-city area (Gdańsk), the Pomeranian Digital Innovation Hub (PDIH)—coordinated by the Pomeranian Special Economic Zone and Gdańsk Science Park—serves as a one-stop center for Industry 4.0 and AI adoption, including maritime applications.

Despite these centers of excellence, talent, and AI activities remain unevenly distributed. A 2021 Digital Poland Foundation report ranked Poland first in Central/Eastern Europe (7th in the EU) by number of AI experts, but this expertise is clustered in large cities. Major urban hubs (Warsaw, Kraków, Poznań, Gdańsk) drive most innovation, while smaller cities and rural regions lag. These regional disparities highlight the need for targeted programs to diffuse AI capacity beyond the leading clusters.

3.2. Legal and Regulatory Framework for AI

3.2.1. Government Policy Framework for AI Innovation Ecosystem

Poland's comprehensive policy framework encompasses multiple strategic documents currently being developed and coordinated across government ministries. The institutional framework is being established in tandem with policy development, ensuring alignment between the strategic vision and operational capacity.

National Documents (Poland):

(1) Act on Artificial Intelligence Systems (*Ustawa o systemach Sztucznej Inteligencji*) – draft

(2) Policy for the Development of Artificial Intelligence in Poland until 2030 (*Polityka rozwoju sztucznej inteligencji w Polsce do 2030 roku*) – draft

(3) State Digitalization Strategy until 2035 (*Strategia Cyfryzacji Państwa do 2035 roku*) – draft

(4) Policy Program "Path to the Digital Decade" until 2030 (*Program polityki „Droga ku cyfrowej dekadzie" do 2030 r.*)

(5) Enterprise Digital Transformation Program (*Program Transformacji Cyfrowej Przedsiębiorstw*) – draft

(6) Productivity Strategy 2030 (*Strategia Produktywności 2030*—Ministry of Development and Technology, MRiT)

(7) Poland's Economic Promotion Policy (*Polityka Promocji Gospodarczej Polski*—MRiT)

(8) Ministerial Strategy for Artificial Intelligence until 2039 (*Resortowa Strategia Sztucznej Inteligencji do roku 2039*—Ministry of National Defence, MON)

(9) E-Health Development Program in Poland for 2022–2027 (*Program rozwoju e-zdrowia w Polsce na lata 2022–2027*—Ministry of Health, MZ)

(10) e-Health Centre Strategy for 2023–2027 (*Strategia Centrum e-Zdrowia na lata 2023–2027*)

(11) Draft Medium-Term National Development Strategy until 2035 (*Projekt średniookresowej strategii rozwoju kraju do 2035*—Ministry of Funds and Regional Policy, MFiPR)

(12) NCBR "Infostrateg" Program Assumptions (*Założenia programu Narodowego Centrum Badań i Rozwoju „Infostrateg"*)

(13) Report: "Where is Poland's AI Niche and How to Use It" (*Raport Polskiego Instytutu Ekonomicznego*)

(14) European Funds for a Modern Economy (*Fundusze Europejskie dla Nowoczesnej Gospodarki - FENG*)—program

(15) Substantive Recommendations for the AI Policy 2025–2030 from GRAI Expert Group (*Rekomendacje merytoryczne do dokumentu Polityka Rozwoju Sztucznej Inteligencji w Polsce 2025–2030 – grupa GRAI*)

European Documents:

(1) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 establishing harmonized rules on artificial intelligence—AI Act

(2) European Commission Guidelines on Prohibited Artificial Intelligence Practices—Official title may vary; refers to the Commission's interpretative guidelines on prohibited AI practices under the AI Act, published in February 2025

(3) DRAFT Artificial Intelligence Liability Directive

(4) DRAFT AI Innovation Package—A set of measures and initiatives supporting AI innovation, including the launch of AI Factories and the Coordinated Plan on AI

(5) DRAFT AI Pact - A voluntary initiative by the European Commission to facilitate the early implementation of the AI Act and cooperation with stakeholders

(6) DRAFT Coordinated Plan on Artificial Intelligence—A strategic document outlining joint actions by EU Member States and the Commission for the development and adoption of AI in the EU

(7) AI Continent Action Plan (2025), European Commission initiative to boost AI innovation through:

- AI Factories and Gigafactories
- Data Labs and Data Union Strategy
- Apply AI initiative and EDIHs
- AI Skills Academy and talent attraction
- AI Act Service Desk for regulatory support

(8) Digital Decade Policy Program 2030 (Europe's overarching digital strategy until 2030)

(9) OECD AI Principles (2019) Guidelines promoting AI that respects human rights and democratic values

3.2.2. Public-Private Governance Structure

Main Public and Public-Private Institutions of the Polish AI Ecosystem:

- **Minister Responsible for Digital Affairs (Minister of Digital Affairs):** The Minister of Digital Affairs, together with the Ministry, plays a pivotal role in shaping and coordinating the Polish AI ecosystem. This institution ensures the continuous and active engagement of public sector entities in the development of the AI landscape. In collaboration with the Minister of National Defense, it is also responsible for establishing the IDEAS Institute, the country's principal AI research center.
- **Commission for the Development and Security of Artificial Intelligence (KRiBSI):** KRiBSI will serve as the supervisory authority for the AI market, overseeing the implementation and use of artificial intelligence in Poland and ensuring the alignment of national activities with European standards. The Commission is to be established under the forthcoming act on artificial intelligence systems.
- **IDEAS Research Institute:** The IDEAS Institute is tasked with conducting advanced research in artificial intelligence and its applications across various sectors of the economy and public administration. It will also focus on developing innovative tools for the defense sector and serve as the principal institution for research collaboration, talent acquisition, and knowledge exchange in the field of AI.
- **Artificial Intelligence Funds Council:** This Council will play a central role in formulating strategies to support the development and implementation of AI in Poland. Its responsibilities include designing programs to concentrate funding on specific projects, fostering cooperation among key institutions financing AI initiatives, and issuing opinions on AI policy directions, funding, and research priorities. It is also tasked with implementing a funding program that will allocate fifty million euros annually between 2026 and 2030 to support research and development in the area of trustworthy AI. Funding is contingent on the completion of ethical impact assessments.
- **AI HUB Initiative:** Under development as part of ecosystem coordination efforts
- **Other Key Ecosystem Entities:** Essential institutions also include entities that collaborate in fulfilling the aforementioned tasks, such as NASK, OPI, the Łukasiewicz Research Network, and the broader public administration. These organizations contribute to the effective implementation of AI policy, research, and innovation in Poland.

3.2.3. Support Programs and Implementation Mechanisms

Poland is planning to develop comprehensive support programs that draw on international best practices, including Korea's proven voucher system model.

3.2.4. Performance Evaluation System

A performance evaluation system will be established alongside the development of institutional frameworks to monitor program effectiveness and measure progress toward AI adoption targets.

3.3. Regulatory Innovation for AI Adoption

3.3.1. EU AI Act and Its Implementation Requirements

The EU Artificial Intelligence Act (adopted 2024) establishes the first comprehensive legal framework for AI, using a risk-based approach. Under the Act, AI systems are categorized into three tiers (low, medium, and high risk) based on their impact on safety and fundamental rights. High-risk systems (e.g., AI in healthcare, education, employment, justice) are subject to strict requirements (data quality, documentation, human oversight).

As an EU member, Poland must implement these requirements. Key tasks include designating a national competent authority for AI oversight, establishing at least one AI regulatory sandbox by August 2, 2026, enforcing conformity assessments for high-risk applications, and setting penalties for non-compliance. Transparency obligations will also apply to systems like consumer chatbots and biometric identification. The Polish Ministry of Digital Affairs is already preparing to transpose the EU rules. It is drafting national regulations and creating complementary guidelines to fit Poland's context.

Poland's legislative response to the EU AI Act (Regulation 2024/1689) centers on establishing a robust institutional and regulatory framework to align with the EU's risk-based approach to artificial intelligence. The draft Act on Artificial Intelligence Systems (version from February 10, 2025) introduces mechanisms for market surveillance, compliance enforcement, and innovation support while addressing high-risk AI applications. Key institutions include the Commission for the Development and Security of Artificial Intelligence (KRiBSI) as the national supervisory authority, the Ministry of Digital Affairs for strategic coordination, and the IDEAS Research Institute for advanced AI development. This framework analyzes Poland's proposed solutions, emphasizing governance structures, compliance mechanisms, and safeguards for fundamental rights.

The draft legislation fully incorporates the four-tier risk hierarchy of the EU AI Act. It prohibits the use of AI systems deemed unacceptable, including those that manipulate individuals through subliminal techniques or implement social scoring. High-risk AI systems—those deployed in sectors such as recruitment, law enforcement, or healthcare—are subject to rigorous conformity assessments, technical documentation requirements, and mandatory human oversight. The new law also introduces specific transparency obligations, requiring that users be clearly informed when interacting with AI-generated content, including deepfakes and chatbots.

Accredited third-party bodies oversee the conformity assessment regime. Developers of high-risk systems must undergo audits. The Artificial Intelligence Funds Council is responsible for administering public financing to support AI development, with a particular emphasis on projects that demonstrate full compliance with European standards. Non-compliance with the Act may result in fines of up to EUR 10 million or 2% of the developer's global turnover.

KRiBSI will be established as Poland's primary supervisory authority for the AI market. Its role encompasses oversight of compliance with both the EU AI Act and corresponding national regulations, including risk assessment for high-risk systems such as biometric identification technologies and applications relevant to critical infrastructure. KRiBSI is also tasked with ensuring cross-sectoral coordination among relevant public authorities, including the Financial Supervision

Authority (KNF), the Office of Competition and Consumer Protection (UOKiK), and the Personal Data Protection Office (UODO). In addition to supervisory and coordinating duties, KRiBSI is empowered to enforce compliance, with legal authority to impose administrative fines and to issue binding decisions requiring the withdrawal of non-compliant systems from the market. It is also authorized to impose administrative fines based on the severity of violations.

The Ministry of Digital Affairs plays a key role in shaping and implementing Poland's national AI strategy. It is responsible for ensuring alignment with overarching EU priorities, including the goals of the Digital Decade 2030. The Ministry is also charged with overseeing the establishment and operation of the IDEAS Research Institute, which will develop advanced AI solutions for use in defense, public administration, and the healthcare sector. Furthermore, the Ministry is responsible for promoting innovation through regulatory sandboxes, which allow for controlled testing environments, particularly beneficial to startups and SMEs.

Poland will participate in the European Artificial Intelligence Board, ensuring alignment with EU-wide standards and contributing to best practices through KRiBSI's annual implementation reports. The Board will serve as a platform for coordination and joint action among national supervisory authorities.

3.3.2. National Regulatory Framework Development

As mentioned before, Poland is developing its own Act on Artificial Intelligence Systems to implement the EU AI Act locally. A second draft (published February 2025) incorporates feedback from public consultations and aligns with Regulation (EU) 2024/1689. This draft law envisages the creation of a Commission for Artificial Intelligence Systems (a new regulatory authority). It establishes a National Program for the Development of AI to support innovation projects. Crucially, it formally provides for AI regulatory sandboxes.

The revised draft shows significant improvement over the first version. For example, the AI Chamber (a business advisory group) observes that the approach is now more balanced and innovation-friendly. However, it has also flagged remaining issues, such as the governance structure of the new AI Commission and the appointment criteria for its members. The government is engaging with industry, academia, and civil society to refine the bill so that it both fulfills EU obligations and nurtures Poland's AI ecosystem.

3.3.3. Regulatory Sandbox Initiatives

Regulatory sandboxes are a flagship element of Poland's approach. The draft AI Act requires each member state to establish an AI sandbox by August 2026. Under the new Act on Artificial Intelligence Systems, the Polish regulator decided to place the regulatory sandboxes for AI under the oversight of KRiBSI. They are being designed to support experimentation, particularly by SMEs and entities whose projects contribute to national priorities such as digital public services or climate resilience. Sandbox projects may operate for a period of up to eighteen months, with the possibility of extension in more complex cases. Participants are required to submit technical reports at the conclusion of the testing period to inform regulatory improvements and future policymaking.

Sandboxes must be accessible and streamlined. The AI Chamber emphasizes that bureaucratic complexity could undermine the sandbox's value. Poland intends to learn from established sandboxes (e.g., in the EU and Korea) to design clear application and approval processes. If implemented well, sandboxes should accelerate responsible AI innovation by balancing experimentation with oversight.

3.3.4. Data Regulation and Privacy Protection

Data governance is central to Poland's AI vision. The national strategy explicitly calls for building a "trustworthy data ecosystem", ensuring quality data and secure sharing practices.

Poland is aligning its data regime with EU laws. It fully implements the General Data Protection Regulation (GDPR) and is preparing for new EU rules (the Data Act, Data Governance Act) that will regulate access to and sharing of data. The government supports mutual recognition of interoperability standards and compliance procedures for "trustworthy AI," with special attention to safeguarding business trade secrets. In practice, this means encouraging certified data-sharing platforms while enforcing strong confidentiality protections.

Regarding AI Act implementation, the draft law reinforces alignment with the GDPR. KRiBSI, in cooperation with the Personal Data Protection Office (UODO), will monitor and enforce data protection standards applicable to AI systems. Obligations include the principle of data minimization, which limits data collection to purposes explicitly permitted under the EU AI Act, as stated in Article 23. In addition, developers must implement cybersecurity measures to prevent adversarial attacks and ensure system resilience, as required under Article 22. The law also introduces a mandatory 24-hour incident reporting requirement for breaches that affect health, safety, or fundamental rights, in accordance with Article 78.

An additional ethical dimension is provided by the Social Council for Artificial Intelligence. This body, which serves in an advisory capacity to KRiBSI, is responsible for issuing recommendations on the responsible development and deployment of AI, particularly in sensitive areas such as education and healthcare, pursuant to Article 25.

Cybersecurity is another priority. The PIAST AI Factory, for example, explicitly includes cybersecurity research as a core theme alongside AI applications.

3.4. Conclusion: Poland’s Emerging AI Ecosystem

Poland's AI ecosystem is characterized by significant potential coupled with substantial implementation challenges. The country has established ambitious policy frameworks and is developing comprehensive institutional structures to support AI innovation, particularly among SMEs. However, the translation from strategic vision to operational reality remains a work in progress.

- **Emerging Strengths:** Poland's substantial infrastructure investments, including the PIAST AI Factory and regional innovation hubs, create a strong foundation for AI development. The

comprehensive policy framework, incorporating both EU requirements and national priorities, provides clear strategic direction. The planned institutional structure, including KRiBSI and the IDEAS Research Institute, offers potential for coordinated governance and innovation support.

- **Persistent Challenges:** Despite these foundations, significant barriers remain. AI adoption among SMEs remains critically low at 4%, with pronounced regional and sectoral disparities. The fragmented implementation of support programs and the nascent state of many institutional arrangements limit immediate impact. Skills shortages and financing constraints continue to constrain SME participation in AI innovation.
- **Implementation Imperative:** The gap between Poland's ambitious AI strategy and current implementation reality underscores the urgent need for systematic, coordinated action. While the policy frameworks provide direction, their effectiveness will depend on successful translation into operational programs that directly address SME barriers and create sustainable ecosystem development.

The subsequent comparative analysis will examine how Korea's proven implementation approaches can inform Poland's transition from strategic planning to effective execution, providing concrete pathways for accelerating SME AI adoption within the EU regulatory framework.

4. Comparative Analysis and Policy Implications

4.1. AI Innovation Ecosystem Comparative Analysis

4.1.1. Measurement Framework and Evidence-Based Policy Foundation

A fundamental challenge in comparing the AI ecosystem development of Korea and Poland lies in the complexity of measurement across different survey methodologies. Poland's AI adoption measurement reveals substantial variance across multiple sources: EU Commission statistics indicate 3.7% of enterprises have achieved "full AI adoption," while GUS reports 5.9% using "AI technology," regional surveys suggest 36% utilize AI technologies, and the AWS Barometer Report reports 30% integrating AI into operations with 36% year-over-year growth. This measurement complexity creates definition ambiguity between "experimental use" and "strategic integration," with most Polish SMEs remaining at the "point solution" level rather than a comprehensive business transformation.

The lack of a unified measurement methodology creates critical barriers to effective policy implementation. Without consistent baseline data, policymakers cannot design targeted interventions or allocate resources effectively to the right SME segments. Different measurement approaches identify different priority segments—the EU methodology focuses on comprehensive adopters requiring advanced support. At the same time, broader surveys suggest a need for basic awareness programs, leading to scattered resources without a strategic focus. Program evaluation becomes impossible when different measurement systems show conflicting results for the same policy interventions, undermining the entire policy implementation cycle from design through evaluation and continuous improvement.

Korea's more mature ecosystem demonstrates clearer progression pathways, with systematic measurement enabling targeted policy interventions. Korea established unified measurement frameworks through the KOSME, ensuring consistent tracking of adoption rates, business impact, and program effectiveness. This measurement consistency enabled Korea to identify precise intervention points, track program effectiveness, and adapt policies rapidly based on real-time feedback, demonstrating that measurement consistency is not merely an administrative requirement but a fundamental success factor for effective AI ecosystem development.

4.1.2. Infrastructure Investment vs SME Utilization Gap

Poland has invested substantially in world-class AI infrastructure, including the EUR 400 million PIAST AI Factory, the 35 petaflops Helios supercomputer, and regional centers such as the Pomeranian Digital Innovation Hub in Gdańsk, creating technical foundations comparable to Korea's infrastructure development strategy. However, only 4% of Polish SMEs have adopted AI, compared

to Korea's overall adoption rate of 22% (with large enterprises at 28.1% and SMEs at 2.7%), revealing a critical disconnect in infrastructure utilization that represents EUR 134 billion in unrealized economic potential.

The critical difference lies in infrastructure-to-SME connectivity mechanisms. Korea designed infrastructure investments with explicit SME access protocols and systematic support mechanisms. At the same time, Poland's development has focused primarily on research and large-scale applications, creating an accessibility gap that requires systematic bridging through targeted policy interventions. This pattern demonstrates that infrastructure alone is insufficient without accompanying support mechanisms that connect technical capacity to practical business applications.

4.1.3. Governance Architecture and Institutional Coordination

Korea's National AI Committee model integrates public and private sector leadership under Presidential oversight, with a majority private sector membership intended to enable industry-driven policy development. However, the actual effectiveness of this model depends heavily on implementation factors—how committee members are selected, the extent of real decision-making authority granted, and whether government agencies genuinely respect committee recommendations. Even in Korea, the model's success varies depending on political priorities and inter-ministerial dynamics that are difficult to replicate or predict.

Poland's emerging institutional framework faces coordination challenges across KRiBSI (regulatory authority), IDEAS Research Institute (research coordination), Artificial Intelligence Funds Council (funding coordination), and various ministries. Rather than attempting to replicate Korea's specific governance structure—which emerged from Korea's unique history of government-led development and corporatist collaboration between bureaucracy, business, and academia—Poland should develop governance mechanisms aligned with its own institutional traditions and EU membership context.

The critical insight is that effective governance depends less on formal structures than on underlying institutional culture and trust relationships. Korea's experience of bureaucracy-dominant corporatism may not translate to Poland's different historical experience with public-private cooperation. Poland should therefore focus on principles rather than forms:

- Ensuring meaningful private sector input (through whatever mechanism fits Polish traditions).
- Creating effective coordination (whether centralized or distributed).
- Building adaptive capacity (recognizing that even successful models require constant adjustment).

Poland's governance design should remain open and flexible, allowing for evolution based on what works in its specific context, rather than adhering to predetermined models from other countries.

4.1.4. Support Program Architecture and Implementation Systems

Korea's transformation demonstrates five critical success factors providing proven blueprints for Poland's adaptation. Evidence-based policy making, facilitated through regular surveys and impact assessments, enables continuous program refinement based on empirical results rather than theoretical assumptions. Integrated governance through coordinated, multi-ministerial operations eliminates policy silos and creates a coherent support ecosystem. Ecosystem approach development focuses on simultaneously cultivating supply and demand, creating sustainable business relationships. Korea's Data Voucher Program documented 38 cases where data consumers successfully transitioned to supply companies, demonstrating ecosystem expansion rather than dependency creation.

Korea's integrated voucher system represents a paradigmatic shift from traditional subsidy approaches to market-driven ecosystem development. The system's effectiveness stems from demand-driven approaches that prioritize actual business needs, ecosystem development that supports both supply and demand sides simultaneously, consortium-based implementation requiring partnerships between SMEs and qualified technology providers, and a graduated support structure that varies assistance levels based on project complexity and company maturity.

Korea's three primary voucher programs demonstrate systematic approaches to addressing different SME AI adoption barriers: the Data Voucher Program, which supports up to EUR 40,000 for data acquisition; the AI Voucher Program, providing up to EUR 133,000 for comprehensive AI solutions; and the Smart Service Support Program, offering up to EUR 67,000 for service sector digital transformation. The Data Voucher Program achieved a 164% increase in applications between 2019 and 2024 through seven major design modifications informed by systematic participant feedback.

Poland possesses substantial policy frameworks and infrastructure investments, but faces a critical implementation gap in operational SME support programs. The gap manifests in program accessibility, where complex procedures prevent SME participation, coordination effectiveness, where multiple agencies operate without systematic integration, and outcome measurement, where success metrics focus on infrastructure deployment rather than SME adoption and business impact.

4.1.5. AI Factory Models: Service vs Infrastructure Approaches

Korea and Poland's AI Factory concepts, despite sharing the same terminology, represent fundamentally different approaches emerging from distinct challenges. Korea's AI Factory evolved from the limitations of Smart Factory—after digitalizing 30,000 manufacturers, Korea recognized that process automation alone cannot achieve intelligent manufacturing without continuous AI model development and management (MSS, 2024b). Poland's PIAST initiative, conversely, represents proactive infrastructure investment aimed at preventing future computational bottlenecks.

Korea's AI Factory operates as an AI-as-a-Service business model, where large-scale facilities produce, customize, and continuously manage AI models based on SME demand. Early implementations have shown a 33% cost reduction and a 33% revenue growth among participating companies (MSIT, 2024b). This model fundamentally restructures the market—instead of each SME

attempting individual AI development, centralized AI factories supply diverse customized models, transforming how SMEs access AI capabilities. In contrast, Poland's PIAST AI Factory, with a PLN 400 million investment scheduled for Q3 2026 operation, emphasizes the provision of physical infrastructure through GPU clusters and supercomputing resources (PSNC, 2024).

<Table 2-4> AI Factory Models Comparison

Aspect	Korea AI Factory	Poland PIAST AI Factory
Primary Focus	Service/Business Model	Physical Infrastructure
Core Function	AI Model Production & Management	Computing Resources Provision
Target Users	SMEs requiring AI services	Research institutions & Companies developing AI
Operation Model	Private-led with government support	Government/EU-led
Investment Priority	Business model development	Hardware infrastructure
Accessibility	Pay-per-use AI services	Resource allocation for R&D

Source: MSIT (2024b); PSNC (2024); European Commission (2024b).

This conceptual divergence reflects the different market failures that each country prioritizes. Korea addresses the capability gap, where 97.1% of SMEs lack AI expertise (KOSME, 2023), while Poland tackles the infrastructure gap that prevents computational access. Neither approach claims superiority; both countries are in early implementation stages, exploring different paths to the same goal.

The strategic value for Poland lies not in Korea's current position but in its concrete planning for market restructuring. Korea's phased approach—2024 large-scale manufacturing integration, 2025 medium enterprise expansion, and humanoid robotics integration—offers practical examples of how Poland could leverage its PIAST infrastructure for similar service models. This hybrid approach could maximize Poland's infrastructure investment while creating sustainable business models that reduce long-term dependence on government support, potentially achieving what neither country currently offers: comprehensive addressing of both infrastructure and capability barriers.

4.2. Regulatory Framework Comparative Analysis

4.2.1. Legal Framework Comparison: Philosophy and Structure

The comparative analysis reveals that both Korea and Poland operate under similar regulatory philosophies, prioritizing AI safety and risk management, but demonstrate different implementation approaches. Korea's AI Framework Act (enacted January 2025) takes a different approach from the EU AI Act, integrating regulatory oversight with industrial development strategies for an innovation-friendly approach that balances trust and innovation. The law features "high-impact AI" focused regulation, generative AI transparency obligations, National AI Committee establishment, AI data center support for SME accessibility, and relatively low fine levels (maximum of KRW 30 million, approximately equivalent to EUR 21,000).

Both countries operate complex multi-layered regulatory frameworks. Poland implements the EU AI Act, combined with enhanced GDPR requirements, the NIS2 Directive's cybersecurity obligations (although Poland missed the October 2024 implementation deadline), and Polish-specific regulations covering employee data processing and national security considerations, with potential fines of up to EUR 35 million. Korea operates under a comprehensive framework that includes the Personal Information Protection Act, sectoral regulations, and cybersecurity requirements, while maintaining a coordinated approach through integrated governance mechanisms.

The critical difference lies in the implementation approach and the integration of SME support. While both frameworks emphasize risk-based regulation, Korea's approach integrates industrial development support directly within the regulatory framework, providing systematic government assistance for SME compliance through Pre-Assessment Systems, simplified procedures, and coordinated guidance. Poland's regulatory framework, while comprehensive in protection standards, lacks comparable integrated SME-specific support mechanisms, creating a disproportionate compliance burden on smaller enterprises despite similar underlying regulatory philosophies.

4.2.1.1 Compliance Burden Quantification: The 2.5x Reality

Polish SMEs face regulatory compliance costs that are 2.5 times higher than those of their Korean counterparts, consuming 15 to 25% of their annual revenue. Manufacturing SMEs in Poland incur annual costs ranging from EUR 150,000 to EUR 400,000, compared to those in Korea, which range from EUR 60,000 to EUR 150,000. Meanwhile, service SMEs face annual costs of EUR 110,000 to EUR 230,000, versus EUR 50,000 to EUR 130,000 in Korea.

<Table 2-5> Manufacturing SMEs - Annual Regulatory Burden

Regulatory Area	Poland	Korea	Impact Ratio
AI Act Compliance	EUR 50K-150K	N/A	Poland's exclusive burden
Data Protection	EUR 30K-80K	EUR 20K-50K	1.5x higher
Cybersecurity	EUR 50K-120K	EUR 30K-70K	1.7x higher (NIS2)
Product Liability	EUR 20K-50K	EUR 10K-30K	2x higher (EU stricter)
Total Cost	EUR 150K-400K	EUR 60K-150K	Poland 2.5x higher

Note: Author's analysis based on regulatory requirements and market research (2024-2025), with computational analysis performed using Claude AI.
Source: Yoon (2025).

<Table 2-6> Service SMEs - Annual Regulatory Burden

Regulatory Area	Poland	Korea	Impact Ratio
GDPR/Data Protection	EUR 80K-150K	EUR 30K-80K	2x higher (GDPR complexity)
AI Transparency	EUR 20K-50K	EUR 10K-30K	2x higher (labeling duties)
Consumer Protection	EUR 10K-30K	EUR 10K-20K	Similar level
Total Cost	EUR 110K-230K	EUR 50K-130K	Poland 2x higher

Note: Author's analysis based on regulatory requirements and market research (2024-2025), with computational analysis performed using Claude AI.
Source: Yoon (2025).

Detailed Cost Component Analysis Framework:

With the assistance of AI software Claude, this analysis examined seven primary cost categories affecting SME AI adoption, utilizing a comprehensive methodology that considered multiple cost components and various implementation scenarios.

Analysis Scope and Assumptions

Geographic Scope:

- **Poland:** EU AI Act + GDPR + NIS2 Directive + Polish-specific regulations
- **Korea:** AI Framework Act + Korean data protection laws + sectoral guidelines

SME Categories Analyzed:

- **Manufacturing SMEs:** 10-250 employees, EUR 2-50 million annual revenue
- **Service SMEs:** 10-250 employees, EUR 1-20 million annual revenue

AI Implementation Complexity:

- Medium-complexity AI systems are typical for SMEs

Applications include predictive analytics, automated customer service, quality control systems, inventory optimization, and basic process automation.

Cost Component Analysis Framework

The analysis examined seven primary cost categories affecting SME AI adoption.

(1) Legal Consultation Fees

- **Poland*:*** EUR 200-400 per hour for AI Act specialists, GDPR consultants
- **Korea*:*** EUR 150-250 per hour for AI Framework Act guidance
- **Annual requirement*:*** 100-300 consultation hours, depending on complexity

(2) Compliance Documentation Development

- **Poland*:*** EUR 15,000-50,000 for technical documentation packages meeting EU standards
- **Korea*:*** EUR 8,000-25,000 for simplified compliance documentation
- **Includes*:*** Risk assessments, technical specifications, compliance procedures

(3) Third-Party Audit and Conformity Assessment

- **Poland*:*** EUR 20,000-80,000 for conformity assessments required under the EU AI Act
- **Korea*:*** EUR 10,000-35,000 for simplified verification procedures
- **Frequency*:*** Annual for high-risk systems, biennial for standard systems

(4) Staff Training and Capacity Building

- **Poland*:*** EUR 5,000-15,000 for comprehensive GDPR, AI Act, and NIS2 training
- **Korea*:*** EUR 3,000-8,000 for AI Framework Act and data protection training
- **Coverage*:*** Management, technical staff, compliance officers

(5) Ongoing Monitoring and Compliance Systems

- **Poland*:*** EUR 10,000-30,000 annually for compliance management systems
- **Korea*:*** EUR 5,000-15,000 annually for monitoring and reporting systems
- **Functions*:*** Automated compliance tracking, incident reporting, audit trails

(6) Penalty Insurance and Risk Mitigation

- **Poland*:*** EUR 5,000-20,000 annually for cyber liability and compliance insurance
- **Korea*:*** EUR 2,000-8,000 annually for equivalent coverage
- **Coverage*:*** Regulatory fines, data breach costs, business interruption

(7) Translation and Localization Costs

- **Poland*:*** EUR 2,000-8,000 annually for Polish language requirements
- **Korea*:*** EUR 1,000-3,000 annually for Korean documentation
- **Requirements*:*** Privacy policies, user agreements, compliance documentation

Analysis Methodology and Limitations:

Cost estimates represent approximate ranges based on available market research, assuming external professional service engagement rather than in-house capability development. Actual compliance costs may vary significantly based on company-specific factors and market conditions, as the regulatory landscape continues to evolve and potentially impacts future cost structures.

Key Policy Implications:

The significant regulatory burden differential creates substantial barriers to AI adoption, with the EU's multi-layered regulatory framework (AI Act + GDPR + NIS2 + national requirements) creating

exponential complexity requiring specialized expertise that smaller companies cannot afford independently. This competitive disadvantage necessitates policy interventions to transform regulatory compliance from a barrier to innovation into a competitive advantage. Higher compliance costs reduce Polish SME competitiveness relative to countries with different regulatory frameworks, potentially impacting long-term economic development and innovation capacity.

4.2.2. Innovation Support Mechanisms: Sandboxes and Data Frameworks

4.2.2.1 Korea's Multi-Ministerial Sandbox Success

Korea's regulatory sandbox system demonstrates how structured regulatory experimentation can enable innovation while maintaining appropriate safeguards. The system's effectiveness stems from its comprehensive, multi-ministerial framework, which covers seven specialized domains, each addressing sector-specific challenges with the appropriate expertise. Korea operates sandbox programs across six ministries, including ICT Convergence, Industrial Convergence, Financial Innovation, Regulation-Free Zones, Smart Cities, R&D Special Zones, and Mobility Innovation, with over 1,000 projects approved since 2019, achieving an 85% approval rate and over 200 AI-related projects achieving more than 70% commercialization success (MSIT, 2024).

Critical success factors Korea demonstrates include risk-appropriate regulatory relief providing different levels of regulatory flexibility based on innovation scale and risk profile, evidence-based regulation development where sandbox results systematically inform permanent regulatory frameworks, and comprehensive safeguards maintaining public trust through mandatory insurance coverage, clear termination procedures, continuous monitoring, and public consultation processes. This approach demonstrates that regulatory flexibility need not compromise safety or consumer protection.

Poland faces the EU AI Act mandate to establish AI regulatory sandboxes by August 2026, creating both opportunity and compliance necessity. Poland's draft Act on Artificial Intelligence Systems places sandbox oversight under KRiBSI, providing centralized coordination potential while requiring careful design to ensure SME accessibility. Based on Korea's success factors, Poland's sandbox system should incorporate a three-tier structure adaptation with national-level KRiBSI operation for high-risk AI systems and EU AI Act compliance, sectoral-level ministry-specific operations for industry applications, and regional-level local operations through PIAST, Cyfronet AGH, and PDIH for SME innovation.

SME-specific advantages should include regional-first approaches, enabling SMEs to begin testing in familiar local environments with established trust networks. Graduated progression should allow successful regional pilots to advance to sectoral or national levels. Additionally, reduced entry barriers should be achieved through simplified applications, faster approval, and minimal paperwork for low-risk innovations. This design addresses the preference of Polish SMEs for trusted, familiar environments where they can experiment without exposing trade secrets, while maintaining compliance with EU regulatory requirements.

4.2.2.2 Korea's Data Innovation Framework and SME Support

Korea's data regulation reforms demonstrate how systematic legal adaptation can enable AI innovation while maintaining robust privacy protections. The "Three Data Laws" amendments (2020) and subsequent modifications established innovation-friendly foundations that do not compromise individual rights. Key innovation enablers include pseudonymized data processing, which enables AI development using anonymized datasets; MyData expansion, creating legitimate user-consented pathways for SMEs to access diverse datasets; cross-organizational data collaboration, supporting consortium-based AI projects; and streamlined consent procedures, which reduce regulatory complexity while maintaining privacy protection (PIPC, 2025).

Beyond legal reform, the Korean Personal Information Protection Commission (PIPC) implemented concrete AI-specific initiatives supporting SMEs' AI adoption:

- **Preemptive Compliance Review (Pre-Assessment System):** This early-stage evaluation service allows AI innovators, particularly startups, to confirm compliance with privacy laws before deployment, mitigating legal risk and uncertainty. The system is under pilot testing in 2024 with a planned full launch in 2025. This Pre-Assessment System represents a paradigm shift from reactive compliance to proactive support, directly addressing SMEs' primary concern about regulatory uncertainty.
- **Legal Exceptions for AI Data Use:** Special provisions permit the lawful use of unstructured original data types (e.g., images, audio) in AI learning, particularly for socially important sectors such as healthcare and defense.
- **AI Development and Service Guidelines:** Published in July 2024, these guidelines offer practical, non-binding recommendations on managing publicly accessible personal data within AI training sets, emphasizing technical and managerial safeguards like data minimization, filtering, privacy impact assessments, and privacy red teaming. This guidance reduces legal ambiguity and fosters responsible AI innovation.
- **Ecosystem and Capacity Building:** Complementary government programs provide explainable AI guidelines, simplify compliance procedures, and enhance data ecosystem infrastructure, specifically targeting resource-constrained SMEs to lower barriers to advanced AI adoption.

4.2.2.3 Poland's Strategic Adaptation Pathway

Poland operates under enhanced GDPR requirements that create particular challenges for AI development, especially for SMEs lacking specialized legal expertise. Poland has additional regulations beyond GDPR, including employee data processing requirements, marketing activity principles, mandatory Polish language translation of privacy documents, an obligation to notify the Polish supervisory authority when appointing a DPO, and specific retention periods. The combination of GDPR complexity with EU AI Act transparency requirements creates a compliance burden concentration that disproportionately impacts smaller enterprises. Strategic adaptation requires Poland to develop SME-specific guidance frameworks that translate complex EU requirements into actionable compliance pathways, following Korea's example of government-provided compliance support for enterprises that cannot afford specialized legal consultation. Poland could implement similar initiatives to Korea's Pre-Assessment System and practical AI guidelines, adapted to EU regulatory requirements, to reduce the compliance burden.

4.3. Strategic Gap Analysis and Adaptation Framework

4.3.1. Poland’s AI Paradox Analysis

Poland's AI development presents a fundamental paradox that requires immediate policy attention. The country has invested heavily in world-class AI infrastructure, including the EUR 400 million PIAST AI Factory, the 35 petaflops Helios supercomputer, and regional centers, while experiencing minimal SME utilization, with only 4% adoption compared to Korea's 22%. This can be articulated as, "Poland is building the highway (AI infrastructure), but SMEs need to be ready to drive on it." This paradox reflects a critical policy challenge that represents both significant opportunity cost and strategic vulnerability, with EUR 134 billion in unrealized economic potential, requiring systematic bridging through targeted policy interventions.

Polish SMEs face a four-layer barrier structure that hinders effective AI adoption, despite having available infrastructure. Technical barriers include the complexity of integrating legacy systems, insufficient datafication levels, and limited access to high-quality datasets suitable for AI applications. Organizational barriers encompass a shortage of AI expertise, management's limited understanding of AI's potential, and resistance to change within traditional business models.

Environmental barriers involve regulatory uncertainty regarding EU AI Act compliance, cybersecurity concerns related to data protection and system vulnerabilities, and intense competitive pressure that limits experimentation resources. Socio-cultural barriers present the most significant challenge, with 80.7% of SMEs believing AI is "not necessary" and 14.9% reporting they "do not know how AI can help" their businesses (Ministry of Digital Affairs, 2023b). These attitudes reflect fundamental knowledge gaps and risk-averse cultural orientations that require systematic educational and demonstration interventions.

This multi-layered structure demonstrates that single-policy solutions cannot address the complexity of SME AI adoption barriers. Instead, integrated approaches that simultaneously address technical, organizational, environmental, and socio-cultural challenges are essential for creating sustainable momentum in adoption and overcoming the disconnect in infrastructure utilization.

4.3.2. Korea-Poland Partnership Framework and Implementation Strategy

The strategic framework envisions Korea-Poland Partnership 2.0 as an evolution beyond knowledge sharing toward implementation collaboration. Korea brings proven experience in transforming from an AI laggard to an OECD leader within five years, while Poland offers EU market access and potential leadership in Central Europe. This partnership framework encompasses the transfer of sandbox operation know-how, cooperation on voucher program design, the sharing of performance measurement methodologies, and bilateral mechanisms for accelerating innovation.

Poland's strategic transformation requires shifting from its current role as an "AI infrastructure builder" to becoming an "AI-powered SME ecosystem" that leverages substantial infrastructure investments for widespread business innovation. This transformation builds on Poland's substantial assets, including a EUR 400 million PIAST investment, 450 million EU market access, a leading

position in Central European AI expertise, and a comprehensive national AI policy framework. It addresses the four-layer barrier structure through systematic support mechanisms that connect world-class infrastructure to practical business applications.

4.4. Key Findings and Policy Implications

4.4.1. Critical Success Factors for Poland's Adaptation

4.4.1.1 Demand-Driven Ecosystem Development

Korea's fundamental success stems from prioritizing actual business needs over technology-push approaches, achieving 85% approval rates and more than 70% commercialization success, because programs address real SME challenges rather than predetermined government technology priorities. Poland's support programs should begin with a comprehensive assessment of SME needs and market validation, rather than relying on infrastructure-first approaches. While infrastructure investments such as the PIAST AI Factory provide valuable foundations, their impact depends on systematic SME access and utilization programs that connect technical capabilities to business applications.

4.4.1.2 Balanced Supply-Demand Ecosystem Support

Korea's integrated approach simultaneously develops both supply (technology providers) and demand (SME users) sides of AI markets, creating sustainable business relationships rather than temporary interventions. The Data Voucher Program's achievement of 38 consumer-to-supplier transitions demonstrates ecosystem expansion rather than dependency creation. Poland should design programs that simultaneously strengthen both AI solution providers and SME adopters, creating market sustainability beyond government intervention periods and fostering long-term ecosystem development.

4.4.1.3 Graduated Support Architecture and Regulatory Innovation as Competitive Advantage

Korea's multi-scale approach accommodates diverse company types and innovation scales, providing appropriate support mechanisms for different SME capabilities and risk tolerances. Poland's diverse SME maturity segments require differentiated approaches rather than uniform programs, with regional sandboxes providing accessible entry points for less advanced SMEs while national programs serve innovation leaders.

Korea transforms regulatory compliance from a barrier to innovation into a competitive advantage through systematic sandbox operations and evidence-based regulation development. Poland should position its EU AI Act implementation as a competitive advantage rather than a compliance burden, using sophisticated regulatory frameworks to attract international AI investment and establish regulatory leadership in Europe.

4.4.1.4 Continuous Program Adaptation

Korea's systematic evaluation and modification mechanisms enable rapid response to market changes and implementation challenges through adaptive governance that ensures programs remain relevant and effective over time. Poland should establish comprehensive monitoring and evaluation systems from program inception, enabling rapid adaptation based on implementation experience and market feedback while maintaining alignment with EU regulatory requirements.

4.4.2. Strategic Considerations for Policy Development

4.4.2.1 Infrastructure-to-Implementation Connection

Poland's substantial infrastructure investments require systematic SME access mechanisms to achieve policy objectives and realize economic potential. Korea's experience demonstrates that the impact of infrastructure depends on programmatic support that enables SME utilization, with successful integration requiring coordination between technical capability development and business application support.

4.4.2.2 EU Integration Advantage and Market Duality Recognition

Poland should leverage its EU market access advantages while adapting Korean operational excellence, positioning itself as the bridge between Asian AI innovation and European market opportunities. This approach requires balancing EU regulatory compliance with innovation-friendly policies that enable systematic SME experimentation and development.

Poland's SME maturity segmentation requires differentiated program design, accommodating varying capabilities and readiness levels rather than uniform approaches. The 42% priority support targets (Ambitious without Knowledge, Needing Support, Ready to Act) represent immediate intervention opportunities while systematic approaches can gradually influence remaining segments through demonstration effects and peer learning mechanisms.

4.4.2.3 Phased Implementation Strategy and Strategic Timing

Given Poland's multiple simultaneous implementation requirements, systematic phasing with clear priorities and measurable milestones enables sustainable progress while maintaining quality and coordination. The EU AI Act sandbox requirements create a critical implementation window, with an August 2026 deadline, presenting both a compliance necessity and a strategic opportunity for establishing Poland as an EU leader in SME AI support.

Early implementation of Korean-inspired approaches can establish Poland as a European leader in SME AI support, attracting international investment and partnerships while creating competitive advantages in the evolving European AI landscape. This timing advantage requires coordinated action across institutional development, program implementation, and the establishment of a regulatory framework to maximize strategic positioning opportunities.

The subsequent policy recommendations will outline specific mechanisms for leveraging these strategic considerations while addressing identified implementation challenges through systematic adaptation of Korea's success factors to Polish institutional and regulatory contexts.

5. Policy Recommendations for the Polish Government

Based on a comprehensive comparative analysis and strategic gap assessment, this chapter presents a systematic framework for transforming Poland from an "AI infrastructure builder" to an "AI-powered SME ecosystem" through the adaptation of Korea's proven success models within the EU regulatory context.

5.1. Strategic Vision and Framework

5.1.1. AI Highway-Driven SMEs: Poland’s Transformation Vision

Poland stands at a critical juncture where substantial infrastructure investments must be connected to widespread business innovation through systematic SME engagement. The strategic vision centers on "AI Highway-Driven SMEs"—a framework that leverages Poland's EUR 400 million PIAST AI Factory, EUR 50 million annual AI HUB budget, and 35 petaflops Helios supercomputer to create systematic pathways for SME AI adoption and innovation.

This vision transforms Poland's current paradigm from infrastructure-focused development to an ecosystem-centered growth approach, positioning SMEs as primary beneficiaries and drivers of AI innovation. The transformation recognizes that Poland possesses exceptional foundational assets, including access to the EU market of 450 million people, the number one position in Central European AI expertise, and comprehensive policy frameworks across 12 national AI strategies. However, these assets require systematic activation through targeted interventions that address the four-layer barrier structure, while creating sustainable momentum for adoption.

Poland faces significant structural barriers that must be addressed systematically. The fragmentation particularly affects AI adoption initiatives, where responsibilities are scattered across multiple ministries and agencies without clear coordination. MRiT handles economic policy aspects, the Ministry of Digital Affairs manages AI strategy development, NASK focuses on cybersecurity dimensions, NCBR oversees R&D funding, and various other agencies address different components without integrated oversight. This creates a situation where an SME seeking comprehensive AI implementation support must navigate multiple agencies with different application processes, eligibility criteria, and timelines.

The vision statement emphasizes transformation from "AI infrastructure builder" to "AI-powered SME ecosystem" by 2030, positioning Poland as the Central European AI Hub Supporting SME Innovation. This transformation requires coordinated development across governance enhancement, demand creation, regulatory innovation, specialized support programs, regional implementation, and university-industry partnerships that collectively address identified gaps while leveraging existing strengths.

5.1.2. Six-Pillar Policy Innovation Framework

The comprehensive policy framework establishes six core policy priorities as structural pillars that systematically address Poland's AI paradox while building on Korea's proven success factors. Each priority pillar addresses critical aspects of the infrastructure utilization gap while creating synergistic policy interactions that amplify the overall ecosystem's development effectiveness.

- **Pillar 1: AI-Focused Governance Enhancement** leverages existing infrastructure and budgets for expanded SME support while establishing evidence-based policy feedback mechanisms essential for adaptive governance.
- **Pillar 2: Demand-Creation Vouchers** implements Korean-style stimulation policies adapted to EU regulatory requirements, directly addressing financial and capability barriers that prevent SME adoption.
- **Pillar 3: Three-Tier Regulatory Sandbox** provides national-sectoral-regional innovation support structures that accommodate diverse SME needs while transforming regulatory compliance from a barrier to a competitive advantage.
- **Pillar 4: SME-Specialized Programs** offers tailored support based on company type and maturity level, recognizing that Poland's diverse business landscape requires differentiated approaches, particularly for microenterprises representing 97% of all Polish enterprises.
- **Pillar 5: Regional Implementation** establishes five-city demonstration centers building on existing infrastructure strengths with specialized AI focus: Warsaw (fintech), Kraków (healthcare), Gdańsk (maritime), Wrocław (industrial), and Poznań (agricultural).
- **Pillar 6: University-Industry Partnerships** connects academic excellence with practical business innovation needs, addressing the insufficient collaboration between academia and SMEs through systematic extension programs and innovation centers.

5.2. Pillar 1: AI-Focused Governance Enhancement

5.2.1. AI HUB Poland 2.0: Strengthened Governance Architecture

Poland should strengthen AI HUB Poland by leveraging the existing EUR 50 million annual budget for expanded SME support while creating integrated one-stop services that connect PIAST-Helios-PDIH networks into a coherent support ecosystem. The enhanced governance structure should establish an AI Adoption Observatory for continuous policy feedback, implementing Korea's evidence-based policy-making approach through regular surveys, impact assessments, and systematic program refinement mechanisms.

The governance enhancement strategy requires addressing the current fragmentation where responsibilities are scattered across multiple ministries and agencies without clear coordination. While Korea addressed similar challenges through its National AI Committee, Poland should develop coordination mechanisms that fit its institutional context rather than directly replicating foreign models. Korea's approach emerged from specific conditions—government-led development traditions and established corporatist collaboration—that differ from Poland's EU membership context and institutional culture.

The enhanced structure should pursue coordination and private sector engagement through flexible pathways:

- Strengthen AI HUB Poland with an expanded inter-ministerial coordination mandate.
- Create advisory councils with progressive private sector involvement.
- Establish sector-specific working groups, building on existing industry associations.
- Leverage EU Digital Innovation Hub networks for cross-border collaboration.

Operational improvements should focus on eliminating policy silos through systematic coordination, establishing clear performance metrics, and creating feedback mechanisms that enable rapid adaptation based on Polish implementation experience.

The governance enhancement should recognize that effective public-private cooperation will evolve through practice, beginning with advisory mechanisms and expanding based on demonstrated effectiveness. Poland's unique institutional context requires discovering appropriate coordination forms through experimentation rather than imposing predetermined structures from external models.

5.2.2. Evidence-Based Policy Framework

Poland must establish a unified measurement methodology as an immediate priority before implementing major support programs, addressing the current measurement inconsistency where AI adoption statistics vary from 3.7% (EU Commission) to 30% (Amazon Web Services & Strand Partners, 2024a). As shown in <Table 2-1>, even Korea faces measurement variations (2.9% to 35%), but its relatively more structured approach through government institutions and industry associations provides useful lessons. This measurement foundation should include standardized definition frameworks distinguishing between experimental use, operational adoption, and strategic integration, regular systematic surveys using consistent methodologies across all regions and sectors, and real-time monitoring capabilities enabling rapid policy adaptation based on implementation feedback.

The evidence-based framework should adapt Korea's quarterly program review model with a comprehensive evaluation of program effectiveness, participant feedback, and market impact, enabling rapid policy iteration and improvement. Performance measurement should track adoption progression, business impact, ecosystem development, regional distribution, and sectoral penetration through comprehensive measurement frameworks that support adaptive governance mechanisms.

5.3. Pillar 2: Demand Creation

5.3.1. Comprehensive Data and AI Voucher Programs

Poland should implement comprehensive voucher programs based on Korea's proven model. These programs simultaneously address critical data scarcity barriers and AI capacity gaps while developing domestic data and AI service markets through demand stimulation. Many Polish SMEs possess operational data but lack capabilities for effective utilization. In contrast, others could significantly improve operations by accessing external datasets for market analysis, operational optimization, or customer insights. This approach directly addresses current funding constraints where Polish SMEs rely heavily on EU funds, requiring substantial co-financing of 50% or more, which can be prohibitive for AI projects with uncertain returns. Korea's Data Voucher Program, which supported over 2,000 projects in 2023, demonstrates an alternative approach where vouchers cover up to 80% of AI implementation costs, paid directly to certified solution providers, thereby eliminating upfront financial barriers for SMEs.

The Data Voucher Program should provide SMEs with vouchers up to EUR 40,000 for purchasing datasets or data processing services from approved providers, addressing critical data scarcity barriers while simultaneously developing domestic data service markets through demand stimulation. The program should support three tracks: purchasing vouchers for data acquisition, including APIs and external datasets, general processing vouchers covering data analytics and visualization services, and AI processing vouchers supporting advanced data processing using machine learning technologies. Poland's program should align with the EU's data strategy and leverage European data spaces to maximize dataset diversity and quality.

Building on data voucher foundations, the AI Voucher Program Architecture should provide up to EUR 133,000 for the comprehensive implementation of AI solutions through consortium partnerships between SMEs and certified AI solution providers. The program addresses Poland's ambitious target of increasing AI adoption from 4% to 50% by 2035, requiring systematic intervention that makes AI implementation financially accessible and technically feasible for resource-constrained enterprises. The AI Voucher Program should be implemented through structured phases. The process begins with the SME identifying specific AI use cases, such as predictive maintenance, customer service automation, or quality control enhancement. SMEs partner with certified AI solution providers who possess technical capabilities, relevant experience, and project management competencies verified through qualification processes. Joint implementation involves shared responsibilities, regular milestone reviews, and collaborative problem-solving that builds internal capabilities rather than creating external dependencies. Knowledge transfer requirements should include hands-on training for SME personnel, comprehensive project documentation and methodology transfer, ongoing support periods to ensure sustainable utilization, and regular capability assessments that track internal AI competency development. The program should prioritize solutions that align with EU guidelines on trustworthy AI, while also addressing social and environmental benefits, such as energy efficiency, healthcare improvement, and sustainability enhancement.

The voucher programs should create virtuous cycle effects where participating SMEs develop internal capabilities and eventually transition from consumers to suppliers, as demonstrated by

Korea's 38 documented consumer-to-supplier transitions that expanded the overall ecosystem rather than creating dependency relationships (World Bank Group Korea Office, 2024).

5.3.2. AI Education and Capacity Building Infrastructure

Sustainable demand creation requires comprehensive education addressing human capital constraints, where only 44.3% of Poles have basic digital skills compared to the EU average of 55.6%, while the shortage of AI specialists is even more acute. SMEs report particular difficulty attracting both general tech talent and AI expertise, with many lacking resources to compete with large enterprises for scarce skills.

Multi-Stakeholder Partnership Model

Sustainable demand creation requires comprehensive education and capacity building through public-private partnerships that address knowledge gaps and cultural barriers preventing the adoption of AI. The education framework should implement a multi-level architecture targeting different organizational roles and competency requirements, recognizing that successful AI adoption requires coordination across executive leadership, technical specialists, and operational staff (Ministry of Employment and Labor, Korea, 2024).

CEO Training Programs should provide intensive education for SME executives covering AI strategic implications, investment decision frameworks, and organizational change management required for successful adoption. Technical Specialist Development should offer advanced training for R&D personnel through partnerships with universities and AI institutes, providing hands-on experience with machine learning implementation and industry-specific applications. Operational Staff Training should focus on AI tool usage, data literacy, and collaborative work practices that enable effective human-AI integration.

The multi-stakeholder approach should combine government funding with academic expertise and private sector training capabilities, thereby creating sustainable knowledge transfer mechanisms that extend beyond the duration of government programs. Partnerships with universities provide talent pipeline development while industry involvement ensures training content addresses practical business requirements and current technology capabilities.

Digital Maturity Assessment and Personalized Development

The education system should include comprehensive digital maturity assessment tools that provide personalized development pathways based on current organizational capabilities, following Korea's successful approach to segmenting readiness levels among SMEs. Assessment dimensions should cover technical infrastructure readiness, human resource capabilities, business process digitization levels, and strategic alignment with AI opportunities (KOSME, 2023).

Personalized development pathways should accommodate different maturity levels, including Digital Beginners who require basic digital literacy and foundational AI understanding, Intermediate

Users who need specific AI tool training and implementation support, Advanced Adopters seeking sophisticated strategy development and optimization techniques, and Digital Champions prepared for peer mentoring and ecosystem leadership roles. This graduated approach ensures that education investments align with actual needs, while creating progression pathways that encourage continued development.

Leadership and Digital Literacy Development

This framework should establish comprehensive programs targeting microenterprise owners and managers. This should include 'AI Leadership Bootcamps'—short, intensive 2-3 day programs for micro-business owners to understand AI basics and strategic implications—peer-to-peer learning networks where early adopters share experiences and mentor other microenterprise owners, and digital maturity assessments creating personalized development pathways. The program should emphasize practical business applications rather than technical complexity, focusing on decision-making capabilities and strategic thinking about AI integration while building confidence in AI adoption among Poland's extensive microenterprise sector.

5.4. Pillar 3: Multi-Scale Regulatory Innovation

5.4.1. Three-Tier Regulatory Sandbox System

National Level: KRiBSI Operation for High-Risk Systems

Poland's regulatory sandbox system should establish three integrated tiers that accommodate diverse innovation scales while meeting EU AI Act requirements by the August 2026 deadline. Tier 1 operates at the national level under KRiBSI oversight, focusing on EU AI Act requirements, high-risk system evaluation, and projects exceeding EUR 1 million investment thresholds that require comprehensive regulatory coordination across multiple agencies (EU AI Act, 2024).

National-level sandboxes should address technologies of national significance and regulatory complexity, including large-scale digital infrastructure projects, national strategic technology development, and contributions to EU standard-setting. The KRiBSI operation should emphasize systematic evaluation procedures, comprehensive safety assessments, and evidence-based regulation development that informs permanent policy frameworks based on practical implementation experience rather than theoretical concerns.

Implementation safeguards should include mandatory comprehensive insurance coverage, clear project termination procedures in place if safety risks emerge, continuous monitoring throughout demonstration periods, and public consultation processes for applications that affect broader public interests. These safeguards demonstrate that regulatory flexibility maintains rather than compromises public protection while enabling systematic innovation development.

Sectoral Level: Ministry of Cooperation for Industry Applications

Tier 2 operates at the sectoral level through ministry-specific cooperation, providing industry expertise and specialized knowledge for sector-specific AI applications. Manufacturing 4.0 sandboxes should operate through the Ministry of Industry's cooperation, covering both AI applications and general automation systems that require manufacturing expertise and adhere to safety standards. Healthcare Digital Innovation sandboxes should involve cooperation with the Ministry of Health for AI diagnostics, telemedicine applications, and health data management systems.

Fintech and Digital Financial Services sandboxes should coordinate with KNF (Polish Financial Supervision Authority) for payment systems, algorithmic trading, and financial risk management applications. AgTech and Smart Agriculture sandboxes should operate through the Ministry of Agriculture cooperation for IoT sensor networks, AI crop monitoring, and precision agriculture systems. Smart Education Technologies sandboxes should involve cooperation with the Ministry of Education for adaptive learning systems, educational analytics, and digital classroom innovations.

Sectoral sandboxes enable specialized evaluation criteria, industry-specific safety standards, and regulatory expertise that general frameworks cannot provide. This approach recognizes that effective AI governance requires domain knowledge and sector-specific risk assessment capabilities rather than uniform regulatory approaches across diverse application areas.

Regional Level: Five-City Innovation Centers

Tier 3 establishes regional sandboxes through five major Polish cities, each leveraging local industry strengths and existing infrastructure while providing accessible entry points for SMEs to experiment with AI innovations in familiar environments. Warsaw Digital Innovation Hub should serve as a comprehensive platform for all emerging technologies, providing broad-spectrum support and coordination with national-level initiatives.

Kraków Tech Valley should focus on R&D and AI development, leveraging the city's concentration of universities and technology expertise for advanced research applications and academic-industry partnerships. Gdańsk Maritime Innovation Hub should specialize in maritime digitalization and AI applications, building on the city's port infrastructure and marine industry expertise. The Wrocław Industry 4.0 Center should focus on smart manufacturing and industrial automation, while the Poznań PIAST Center should leverage its AI infrastructure and digital services capabilities.

Regional sandboxes address SME preferences for trusted, familiar environments where they can experiment without exposing trade secrets to large enterprise competitors. This local approach enables peer learning networks, industry cluster development, and regional specialization that builds on existing economic strengths while creating pathways for progression to sectoral and national innovation levels.

5.4.2. AI Compliance Learning Sandbox (AI Regulatory Compliance Support Program)

Regulatory Compliance as Competitive Advantage

Poland should establish an AI Compliance Learning Sandbox specifically designed to transform regulatory complexity from an innovation barrier to a competitive advantage through systematic education and support programs. This specialized sandbox addresses the reality that Polish SMEs face regulatory compliance costs that are 2.5 times higher than those of their Korean counterparts (see [Table 2-5] and [Table 2-6]), requiring targeted interventions that build compliance capabilities rather than simply reducing requirements.

The AI Compliance Learning Sandbox should implement a four-level stepwise learning process that builds comprehensive compliance capabilities. Level 1 covers GDPR basics over two weeks, providing a foundational understanding of data protection requirements and privacy-by-design principles essential for AI development. Level 2 focuses on understanding the AI Act and its requirements over four weeks, covering risk assessment procedures, conformity assessment processes, and transparency obligations.

Level 3 addresses sector-specific AI regulations over four weeks, providing specialized knowledge for manufacturing, healthcare, finance, or other industry-specific compliance requirements. Level 4 involves practical application and testing over six weeks, including mock regulatory environment testing, potential legal risk assessment, compliance cost prediction, and development of best practices based on real-world scenarios.

Risk Simulation and Practical Implementation

The learning sandbox should incorporate risk simulation components that enable SMEs to understand compliance requirements through practical experience rather than theoretical study. Mock regulatory environment testing allows companies to simulate compliance procedures and understand documentation requirements without real regulatory consequences. A potential legal risk assessment helps SMEs identify specific vulnerability areas and develop mitigation strategies tailored to their business models and technology applications.

Compliance cost prediction tools should help SMEs understand financial implications and budget appropriately for regulatory requirements, while best practices development creates industry-specific guidance based on successful compliance experiences. The program should emphasize multi-stakeholder cooperation involving legal experts, technology consultants, and regulatory authorities to provide comprehensive support that addresses both technical and legal compliance dimensions.

Success metrics should aim for a 50% reduction in regulatory compliance burden through improved efficiency, enhanced risk management, and the development of systematic compliance capabilities. This approach transforms the EU's complex regulatory environment from a competitive disadvantage to a competitive advantage by preparing Polish SMEs to lead in sophisticated regulatory compliance, which is becoming increasingly important in global AI markets.

5.4.3. SME Fast Track Program

The sandbox system should include a dedicated SME Fast Track Program targeting companies with 50 or fewer employees and revenue under EUR 10 million, providing specialized support that addresses resource constraints and simplified procedures appropriate for smaller organizations. Rapid review processes should reduce processing time from standard six months to three months through streamlined evaluation procedures and dedicated review staff.

High support rates should provide 80% demonstration cost support compared to general 50% support levels, recognizing that smaller companies face disproportionate financial barriers to regulatory experimentation. Dedicated mentors should offer a 1:1 consultant assignment providing personalized guidance throughout the sandbox process. At the same time, legal support should include free digital and AI legal consultation that smaller companies cannot typically afford.

EU linkage support should facilitate market entry in other member states by ensuring that sandbox results provide evidence and documentation that supports broader European market access. This approach recognizes that successful sandbox participation should create business opportunities beyond domestic market testing, leveraging Poland's EU membership to gain a competitive advantage in broader European markets.

5.5. Pillar 4: SME-Specialized Support Programs

5.5.1. Typology-Based Customized Support Framework

Poland should implement a comprehensive typology-based support system that recognizes the diverse needs and capabilities of different SME categories. Rather than applying one-size-fits-all approaches, this framework categorizes SMEs based on their AI relationship and sectoral characteristics, enabling targeted interventions that maximize the effectiveness of support and the efficiency of resource allocation.

The primary categorization should distinguish between AI Solution Adopting Enterprises (companies seeking to implement existing AI technologies to improve operations) and AI Solution Developing Enterprises (companies creating AI products or services). Within each category, further segmentation by sector—manufacturing versus services—ensures that support addresses specific industry requirements, regulatory environments, and implementation challenges.

This typological approach enables resource optimization by matching support intensity and type to actual needs, prevents over-supporting advanced companies while under-supporting beginners, and creates clear progression pathways that encourage continued development. Korea's experience demonstrates that such differentiated support systems achieve higher adoption rates and more sustainable outcomes compared to generic programs.

5.5.2. Type A: AI Solution Adopting Enterprises

Manufacturing SMEs: Industry 4.0 Leadership Development

Poland's manufacturing sector demonstrates significant potential for AI adoption, with current adoption rates of 47% among larger manufacturers, indicating sector readiness and competitive pressures that create momentum for adoption. Type A-1 support for manufacturing SMEs should establish Industry 4.0 sandbox environments that provide hands-on experimentation with smart factory technologies, including AI-powered quality control, predictive maintenance systems, and production optimization algorithms.

Smart factory demonstration environments should enable manufacturers to test AI applications in controlled settings before committing to full implementation, reducing risk and building confidence through practical experience. AI adoption investment tax credits of 20% should provide financial incentives that offset implementation costs while encouraging systematic rather than ad hoc adoption approaches. The support should emphasize consortium partnerships with technology providers that ensure knowledge transfer and capability building, rather than simply providing services.

Manufacturing-specific support should address common challenges, including the integration of legacy systems, workforce training for AI-enhanced operations, and standardizing quality control to maintain product consistency while improving efficiency. The program should leverage Poland's strong manufacturing base and EU market access to position Polish SMEs as leaders in AI-enabled manufacturing within European supply chains.

Service SMEs: Privacy-by-Design Excellence

Type A-2 support for service SMEs should address the sector's 25% current adoption rate by providing Privacy-by-Design Support Packages that help service companies navigate GDPR complexity while implementing AI solutions. GDPR-compliant AI architecture design should provide technical frameworks and implementation guidance that ensure privacy protection while enabling AI functionality for customer service, business analytics, and operational optimization.

Verified chatbot and consultation solutions should offer pre-approved AI applications that meet EU regulatory requirements while providing immediate business value through customer service automation, appointment scheduling, and basic inquiry handling. The support should emphasize transparency requirements and user consent mechanisms that build customer trust rather than creating compliance burdens.

Service sector programs should recognize diverse business models and customer interaction patterns, providing flexible implementation approaches that accommodate different operational requirements. Support should include customer communication training that helps SMEs effectively explain AI applications to customers, build acceptance for AI-enhanced services, and maintain personal relationships while upholding service quality expectations.

5.5.3. Type B: AI Solution Developing Enterprises

AI Startups: Accelerator and Investment Support

Type B-1 support for AI startups with 50 or fewer employees and five years or less of operation should establish Polish AI Startup Accelerator programs that provide intensive development support, mentorship, and facilitation of market access. Initial investment support of up to EUR 500,000 should enable promising startups to develop and test AI solutions while building sustainable business models that contribute to the development of Poland's AI ecosystem.

MVP (Minimum Viable Product) Sandbox programs should provide six-month demonstration opportunities that enable startups to test AI solutions with real customers under regulatory protection, building evidence for investor attraction and market validation. The accelerator should emphasize connections with larger enterprises that can serve as early customers and implementation partners, thereby creating pathways for startup growth while addressing the needs of SMEs for AI adoption.

International linkage support should help Polish AI startups access broader European markets and establish global partnerships, leveraging Poland's EU membership and Central European positioning to gain a competitive advantage. Mentorship programs should connect startups with experienced entrepreneurs, technical experts, and business development professionals who guide them throughout the development process.

AI Specialized SMEs: Excellence Center Development

Type B-2 support for AI-specialized SMEs with 51-250 employees should establish an AI Excellence Center to recognize these companies as potential ecosystem leaders and export champions. R&D tax credits up to 200% should incentivize continued innovation and technology development, while global partnership linkage should facilitate international collaboration and market expansion opportunities.

Excellence centers should focus on developing specialized AI capabilities that serve the broader needs of the SME ecosystem, creating domestic solution providers that understand local business requirements and regulatory environments. Support should emphasize intellectual property development, technology standardization, and the sharing of best practices that elevate overall ecosystem capabilities, rather than merely supporting individual companies.

The specialized SME support should recognize these companies' potential role as AI solution providers for smaller enterprises, creating supply-side ecosystem development that complements demand-side voucher programs. Partnership facilitation should connect specialized SMEs with universities, research institutes, and international technology companies to accelerate innovation development and market reach.

5.5.4. SME Regulatory and Market Access Support Programs

Integration with Regulatory Innovation Framework

The SME-specialized support system should integrate with the regulatory innovation programs detailed in Section 5.4 to provide comprehensive regulatory and market access support. This integration ensures that SMEs receive both operational support through typology-based programs and regulatory assistance through specialized compliance and fast-track mechanisms.

SME AI Regulatory Compliance Support Program

Building on the AI Compliance Learning Sandbox framework (Section 5.4.2), this program transforms regulatory complexity from an innovation barrier to a competitive advantage for SMEs. The four-level stepwise learning process—covering GDPR basics, AI Act requirements, sector-specific regulations, and practical implementation—should be enhanced with SME-specific elements, including simplified documentation requirements, peer learning networks among similar-sized companies, and cost-sharing mechanisms that make compliance education accessible to resource-constrained enterprises.

Success metrics should target a 50% reduction in regulatory compliance burden through improved efficiency and systematic capability development, positioning Polish SMEs as leaders in sophisticated regulatory compliance within European markets.

SME Market Entry Fast Track Program

Complementing the regulatory sandbox Fast Track Program (Section 5.4.3), this initiative extends streamlined procedures to standard product and service market entry processes beyond experimental regulatory environments. The program maintains the same targeting criteria (≤50 employees, ≤EUR 10 million in revenue) and support structure (80% cost coverage, dedicated mentorship, and EU market facilitation), while focusing on conventional market access rather than regulatory experimentation.

This dual approach ensures that SMEs benefit from both innovative regulatory testing environments and practical market entry support, creating comprehensive pathways from innovation development through regulatory compliance to market commercialization.

EU Market Leadership Preparation

Compliance support should position Polish SMEs as leaders in sophisticated regulatory compliance, which is becoming increasingly important in global AI markets, thereby creating competitive advantages rather than merely meeting minimum requirements. Advanced compliance capabilities should enable Polish companies to serve as trusted partners for international businesses seeking to enter the EU market, leveraging their regulatory expertise to drive business development opportunities.

The support should prepare SMEs for evolving regulatory requirements and emerging compliance challenges, building adaptive capabilities that respond to changing regulations rather than simply meeting current requirements. International partnership facilitation should connect Polish SMEs with global companies seeking regulatory guidance and compliance expertise, creating new business opportunities based on regulatory competence.

Training should include emerging technologies and regulatory trends that enable SMEs to anticipate rather than react to regulatory changes, positioning them as innovation leaders rather than compliance followers. The program should create peer learning networks that share compliance experiences and best practices, building collective ecosystem capabilities that benefit all participants while reducing individual compliance burdens through shared knowledge and resources.

5.5.5. Microenterprise-Focused Programs

Microenterprises, representing 97% of all Polish enterprises, face the most severe challenges in digital and AI adoption. These firms with fewer than 10 employees are often family businesses or sole proprietorships with limited bandwidth to engage with government programs. Language barriers, bureaucratic complexity, and co-funding requirements deter them from accessing support.

Microenterprise Digital Transformation Hub

The framework should establish dedicated coordination units that provide a single point of contact for all microenterprise digital and AI support programs. It should also include local expertise centers offering hands-on technical assistance, program coordination to ensure seamless integration between micro-grants, loans, tax incentives, and training programs, as well as regional network facilitation to connect microenterprises for knowledge sharing and collaborative procurement.

Structured Digital-to-AI Progression Pathway

Implementation should follow a clear three-stage development: Stage 1 (Digital Foundation) focusing on basic digitalization, including e-commerce platforms and cloud-based accounting systems, Stage 2 (Data Readiness) introducing data collection and analytics capabilities through integrated business management tools, and Stage 3 (AI Integration) introducing AI-powered tools only after completing previous stages. Each stage should have specific completion criteria and dedicated support mechanisms that ensure sustainable progression rather than premature advancement to complex technologies.

Microenterprise support should prioritize low-friction access by simplifying application processes. These turnkey solutions require minimal technical expertise and integration with existing business services that microenterprises already utilize, such as banking and accounting platforms. This approach recognizes that traditional policy tools are often too complex for the smallest enterprises and requires innovative delivery mechanisms that meet them where they are rather than requiring them to navigate complex government programs.

5.6. Pillar 5: Regional Implementation Strategy

5.6.1. Five-City Regional Implementation Strategy

Leveraging Existing Infrastructure and Regional Strengths

Poland's regional AI implementation should build on existing infrastructure investments and regional industry specializations to create coordinated ecosystem development that maximizes synergies while avoiding duplication. Each regional center should develop specialized capabilities that serve both local needs and national ecosystem development, creating complementary rather than competitive relationships among regional hubs.

The Poznań PIAST Center should serve as an AI infrastructure and digital services hub leveraging the EUR 400 million PIAST AI Factory investment to provide access to supercomputing data processing capabilities, and technical infrastructure support for SMEs throughout Poland. The center should emphasize connecting advanced infrastructure to practical business applications while developing expertise in translating infrastructure to business applications that can be replicated in other regions.

Kraków Tech Valley should focus on R&D and AI development, building on the city's university concentration, international technology companies, and research expertise. The enhanced Cyfronet AGH supercomputing center, with its 35 petaflops Helios system, should serve as a foundation for advanced AI research and development that addresses practical SME challenges while maintaining academic excellence and leadership in innovation.

Gdańsk Maritime Innovation Hub should specialize in maritime industry AI applications, leveraging the Pomeranian Digital Innovation Hub and the region's port infrastructure to develop AI solutions for maritime logistics, shipping optimization, and port management systems. This specialization should position Poland as a leader in maritime AI applications within the European context, while serving the domestic needs of the port and shipping industries.

Warsaw Innovation Hub should operate as a comprehensive platform for all emerging technologies, providing broad-spectrum support and coordination with national-level initiatives. The capital's concentration of government agencies, international businesses, and financial institutions should enable the development of a comprehensive ecosystem that serves as a model for other regions, while addressing diverse industry needs.

The Wrocław Industry 4.0 Center should focus on smart manufacturing and industrial automation leveraging the region's manufacturing base and engineering expertise to develop AI applications for production optimization, quality control, and supply chain management that serve manufacturing SMEs throughout Poland and Central Europe.

5.6.2. Inter-Regional Coordination and Knowledge Sharing

Regional implementation necessitates systematic coordination mechanisms that facilitate knowledge sharing, resource optimization, and complementary development, rather than fostering isolated regional competition. Inter-regional coordination should establish regular information exchange, joint project development, and shared resource utilization that maximizes collective impact while building on individual regional strengths.

Coordination mechanisms should include quarterly inter-regional conferences that share best practices and identify opportunities for collaboration. These joint research projects leverage complementary capabilities across regions and shared training programs that reduce costs while improving quality through specialization and economies of scale. Resource sharing should enable smaller regions to access specialized capabilities while providing larger centers with diverse application opportunities.

The coordination framework should establish clear roles and responsibilities that minimize overlap while ensuring comprehensive coverage of SME needs and technology applications. Performance measurement should track both individual regional success and collective ecosystem development, incentivizing collaboration rather than competition among regional centers.

5.6.3. Digital Innovation Hubs and Living Labs Expansion

Poland should expand and empower the network of European Digital Innovation Hubs, ensuring capacity to serve more SMEs and cover all regions. These hubs should acquire the latest technologies, including small-scale Industry 4.0 demo lines, AI computing resources with GPU clusters for machine learning, specialized AI testing labs, and cybersecurity labs that SMEs can use.

Living Labs should be created at the regional level, tied to local industry strengths: a fintech AI lab in Warsaw, 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.

5.7. Pillar 6: University-Industry AI Partnerships

5.7.1. Academic-Industry Collaboration Framework

Systematic university-industry partnerships should leverage Poland's academic excellence to address the practical innovation needs of SMEs, while bridging the current gap. Unlike countries with established university extension programs or innovation centers supporting SME digital projects, Poland's such linkages remain nascent or limited to EU-funded pilot projects.

NCBR (National Centre for Research and Development) specialized programs should facilitate AI-dedicated industry-academia cooperation through structured project frameworks, funding mechanisms, and partnership facilitation. Practical research initiatives should match AI graduate

thesis topics with SME challenges, creating mutually beneficial relationships where students gain practical experience. At the same time, SMEs gain access to cutting-edge research and technical expertise that they cannot afford to acquire independently.

AI for SMEs Collaboration Programs should establish specialized partnerships where university AI research centers work directly with SMEs to develop practical AI applications. This should include AI graduate thesis projects addressing real SME challenges and joint AI pilot projects funded by government grants, thereby building trust and fostering systematic knowledge flow between academia and the SME sector, which currently remains underdeveloped.

Government-funded university-SME teams should provide sustained collaboration opportunities that extend beyond individual projects to create ongoing partnership relationships and knowledge transfer mechanisms. Joint development projects should emphasize commercially viable solutions that address real business problems while advancing academic knowledge and research capabilities, with intellectual property sharing agreements and technology transfer mechanisms that benefit both partners.

5.7.2. Talent Pipeline Development and Retention

University partnerships should address Poland's AI talent shortage by creating career pathways that retain graduates within domestic companies, rather than losing them to international technology companies. While Poland produces significant numbers of ICT graduates in absolute terms, many are absorbed by large firms or emigrate to higher-paying markets, creating a talent drain that undermines the development of the SME ecosystem.

Industry placement programs should provide students with practical AI experience in Polish SMEs, while also giving companies access to talented interns and potential employees who understand both the technical capabilities and business applications of AI. This "Digital Transformation Internship/Secondment" scheme should place ICT students or researchers in SMEs to work on specific digital projects, with government funding for stipends to make participation attractive.

Professional development programs should support continuing education for working professionals who need to update their AI skills, while also providing universities with opportunities for industry engagement and additional revenue streams. Technical universities should offer certificate courses in data analytics, cybersecurity, and comprehensive AI literacy programs for SMEs, including "AI for Business Leaders" executive education and practical AI implementation workshops for technical staff with flexible timings or online modes.

Executive education programs should target SME leaders who require strategic understanding of AI without needing technical depth, thereby creating market demand for university expertise while enhancing SME adoption readiness. The talent development approach should emphasize practical applications and business understanding over purely academic AI knowledge, ensuring graduates can contribute immediately to SME AI adoption efforts while maintaining their technical competence.

5.7.3. Innovation Ecosystem Integration Formula

The university-industry partnership framework should implement the strategic equation: "Existing Infrastructure + Academic Excellence + SME Innovation = Polish AI Ecosystem 2.0." This integration recognizes that sustainable ecosystem development requires coordination among technical infrastructure, research capabilities, and business innovation rather than isolated development in each area.

Academic excellence should be channeled toward practical problem-solving that addresses SME challenges while maintaining research quality and innovation standards. Infrastructure utilization should be optimized through the expertise of universities and student research projects that maximize resource utilization while creating business value. SME innovation should be supported through an academic partnership that provides technical expertise, research capabilities, and access to talent that smaller companies cannot develop independently.

The integration approach should create feedback loops where business success supports continued academic research, research advances enable better business solutions, and infrastructure development serves both academic and business needs. Long-term sustainability requires mutually beneficial relationships that create value for all participants while contributing to broader economic development and competitiveness goals.

5.8. Implementation Timeline and Success Metrics

5.8.1. Three-Phase Strategic Roadmap (2025-2030)

Phase 1: Foundation Building (2025-2026)

Phase 1 focuses on establishing fundamental infrastructure and program foundations required for systematic ecosystem development. AI HUB Poland 2.0 development should strengthen existing governance structures while establishing SME support systems that connect infrastructure investments to practical business applications. The enhanced hub should coordinate across PIAST, Helios, and PDIH networks while establishing evidence-based policy feedback mechanisms essential for adaptive program management.

1,000 SME voucher pilot programs should test both data and AI voucher models on a sufficient scale to generate meaningful lessons learned, while demonstrating the government's commitment to systematic SME support. Pilot programs should emphasize diverse SME types, regional distribution, and sector variety to understand adaptation requirements and effectiveness across different business contexts. Systematic evaluation and documentation should create reusable program models and implementation guidance.

AI awareness campaigns should address socio-cultural barriers identified in the analysis, particularly the 80.7% of SMEs who believe AI is "not necessary" and 14.9% who "do not know how AI can help" (Ministry of Digital Affairs, 2023b). Educational initiatives should emphasize practical business benefits, risk mitigation, and peer success stories that demonstrate achievable rather than theoretical AI applications.

A three-tier sandbox framework design should establish operational procedures, evaluation criteria, and coordination mechanisms across national, sectoral, and regional levels, while ensuring compliance with the EU AI Act and accessibility for SMEs. Framework development should incorporate lessons learned from Korea's multi-ministerial system while adapting to Polish institutional capabilities and European regulatory requirements.

- **Target: 6% AI Adoption** represents conservative but achievable progress that builds momentum for subsequent phases, while demonstrating systematic rather than random improvement in adoption. This target recognizes the time required for program establishment and initial market penetration while providing clear success metrics for evaluation and program refinement.

Phase 2: Ecosystem Scale-Up (2027-2028)

Phase 2 emphasizes systematic scaling and ecosystem integration, building on established foundations while expanding reach and sophistication. A full 3-tier sandbox operation should demonstrate regulatory innovation leadership while providing comprehensive support for diverse innovation scales and risk levels. Sandbox success should attract international attention and investment while serving domestic SME innovation needs.

The nationwide expansion of the PIAST network should ensure that advanced AI infrastructure serves SMEs throughout Poland, rather than benefiting only major metropolitan areas. Network expansion should include mobile capabilities, remote access systems, and regional support staff that bring supercomputing capabilities to smaller cities and rural areas where SMEs may lack direct access to advanced technical infrastructure.

Sector-specific AI solutions should emerge from successful sandbox projects and voucher programs, creating reusable applications and best practices that accelerate adoption while reducing costs for subsequent implementers. Sector specialization should build on Poland's industrial strengths while creating exportable expertise and solutions that serve broader European markets.

Regional hub networks should achieve full operational coordination with specialized capabilities that serve national ecosystem needs while addressing local business requirements. Inter-regional collaboration should demonstrate effective resource sharing and knowledge transfer while creating competitive advantages through specialization and coordination rather than duplication and competition.

- **Target:** 8% AI Adoption represents continued systematic progress that approaches EU average levels while building a foundation for accelerated growth in the final phase. This target recognizes the time required for ecosystem effects to mature while maintaining ambitious but realistic expectations for systematic adoption improvement.

Phase 3: Leadership and Innovation (2029-2030)

Phase 3 positions Poland as an EU leader in SME AI support while creating sustainable ecosystem momentum that continues beyond government program periods. The development of

EU AI best practices should establish Poland as a model for other member states, while creating expertise and a reputation that attracts international partnerships and investment opportunities.

Central European AI hub positioning should leverage Poland's success in supporting SMEs to attract regional businesses and international companies seeking access to a sophisticated AI ecosystem. Hub positioning should emphasize regulatory expertise, SME integration capabilities, and market access advantages that create competitive positioning within the broader European AI landscape.

Cross-border AI collaboration should extend successful domestic models to international partnerships while serving as a bridge between European and global AI markets. International collaboration should encompass both inward investment attraction and outward expertise export, creating revenue opportunities while building Poland's reputation as a leader in AI innovation.

Knowledge sharing and model replication should systematize successful approaches for domestic scaling and international transfer, creating intellectual property and consulting opportunities while contributing to the broader development of the European AI ecosystem. Documentation and methodology transfer should create revenue opportunities while establishing Poland's thought leadership in SME AI adoption strategies.

- **Target:** 16% AI Adoption represents achievement of critical mass that enables self-sustaining ecosystem growth while positioning Poland for accelerated progress toward the 2035 50% target. Based on innovation diffusion theory, 16% represents the critical tipping point where early majority adoption begins and exponential growth follows (Rogers, 2003). This target ensures achievement of critical mass, enabling self-sustaining ecosystem growth while positioning Poland for accelerated progress toward the 2035 50% target. At 16% adoption, Poland moves beyond early adopters to broader SME engagement, creating the momentum needed for exponential growth characteristic of technology diffusion patterns. This conservative target builds solid foundations while creating momentum for continued growth that extends beyond the immediate program period.

5.8.2. Success Metrics and Performance Evaluation

Quantitative Performance Indicators

Success measurement should track both immediate program outputs and longer-term ecosystem development outcomes that demonstrate sustainable progress rather than temporary improvements. The AI adoption rate, progressing from a 4% baseline to 6%, 8%, and ultimately 16% by 2030, provides clear targets while acknowledging that ecosystem development requires time for full impact realization.

A 50% reduction in SME regulatory compliance costs should demonstrate a successful transformation of the regulatory burden from a barrier to a competitive advantage, while maintaining compliance quality and risk management effectiveness. Cost reduction measurement should include both direct financial savings and efficiency improvements that reduce time and resource requirements for regulatory compliance activities.

Economic impact realization should track progress toward the EUR 134 billion potential economic benefit through systematic measurement of participating SME revenue growth, employment creation, productivity improvements, and export development. Economic measurement should distinguish between direct program effects and broader ecosystem impacts that demonstrate sustainable value creation rather than temporary subsidy effects.

Regional distribution metrics should ensure that benefits reach SMEs throughout Poland, rather than concentrating in major metropolitan areas, with specific targets for participation in non-capital regions that demonstrate inclusive ecosystem development. Sectoral diversification should track adoption progress across different industries while identifying successful models that can be replicated in other sectors.

Qualitative Assessment Framework

Ecosystem health indicators should assess collaboration quality, knowledge transfer effectiveness, and sustainable relationship development among ecosystem participants, including SMEs, technology providers, universities, and government agencies. Relationship quality measurement should include partnership durability, repeat collaboration patterns, and peer recommendation networks that demonstrate genuine ecosystem development rather than transactional program participation.

Innovation quality assessment should evaluate the sophistication and business impact of AI implementations, rather than merely counting adoption instances. This is because sustainable ecosystem development requires meaningful business transformation, rather than superficial technology adoption. Innovation measurement should encompass problem-solving effectiveness, competitive advantage creation, and scalability potential, demonstrating genuine value creation.

Regulatory effectiveness should assess the quality of compliance, risk management improvement, and enhancement of international competitiveness that result from sophisticated regulatory capabilities, rather than minimal compliance approaches. Regulatory assessment should include audit results, penalty avoidance, and international partnership opportunities that demonstrate competitive advantage rather than mere compliance achievement.

Adaptive Evaluation and Program Refinement

Quarterly program reviews should enable rapid adaptation based on implementation experience, while maintaining strategic direction and achieving long-term objectives. Review processes should include participant feedback, market analysis, and comparative assessment that identify program improvements and adaptation requirements for changing market conditions and regulatory environments.

International benchmarking should track Poland's progress relative to other EU member states and global AI leaders while identifying emerging best practices and adaptation opportunities. Benchmarking should encompass both quantitative metrics and a qualitative assessment of ecosystem development approaches that maintain Poland's competitive position in the evolving global AI landscape.

Program modification protocols should enable systematic adaptation while maintaining program integrity and stakeholder confidence, recognizing that effective ecosystem development requires a balance between stability and responsiveness. Modification processes should include stakeholder consultation, impact assessment, and implementation planning that ensures changes improve rather than disrupt ecosystem development progress.

5.8.3. Korea-Poland Partnership 2.0: Sustained Collaboration Framework

Beyond Knowledge Transfer to Implementation Partnership

Korea-Poland Partnership 2.0 represents an evolution from the current knowledge-sharing phase (Korea-Poland Partnership 1.0) to a sustained implementation collaboration that leverages complementary strengths for mutual benefit. Korea brings proven experience transforming from an AI laggard to an OECD leader within five years, while Poland offers EU market access and Central European leadership potential that creates mutually beneficial partnership opportunities.

Sandbox operation know-how transfer should provide ongoing technical assistance and best practice sharing that accelerates Poland's regulatory innovation development while creating opportunities for Korean companies to understand European regulatory environments. Collaboration should include staff exchange programs, joint training initiatives, and shared evaluation methodologies that build institutional capabilities rather than simple knowledge transfer.

Voucher program design cooperation should adapt Korea's proven models to EU regulatory requirements while sharing implementation experiences that benefit both countries' ecosystem development efforts. Collaboration should include joint evaluation studies, comparative analysis, and shared performance measurement that creates intellectual property and thought leadership opportunities for both partners.

Performance measurement methodology sharing should establish comparable metrics and evaluation frameworks that enable ongoing collaboration and mutual learning while contributing to a broader international understanding of effective SME AI support strategies. Methodology development should create consulting and advisory opportunities while building both countries' reputations as leaders in AI ecosystem development.

Bilateral Innovation Acceleration Mechanisms

Partnership framework should create systematic mechanisms for ongoing collaboration that extend beyond government programs to include private sector partnerships, academic exchanges, and business development opportunities. Bilateral innovation should include joint research projects, technology development initiatives, and market entry facilitation that create commercial opportunities while advancing ecosystem development objectives.

Regular partnership reviews should assess the effectiveness of collaboration while identifying new opportunities for mutual benefit and shared value creation. Review processes should include both government and private sector participants to ensure that partnership benefits extend throughout both ecosystems rather than remaining at the government level only.

Long-term partnership sustainability should be ensured through institutional mechanisms, ongoing value creation, and mutual benefit distribution that creates incentives for continued collaboration beyond initial program periods. Sustainability mechanisms should include commercial partnerships, joint ventures, and shared intellectual property development that creates lasting relationships and continued cooperation incentives.

The partnership framework should serve as a model for other international AI cooperation initiatives while positioning both Korea and Poland as leaders in systematic ecosystem development and international collaboration that advances global AI adoption and governance best practices.

6. Conclusion

This comprehensive policy framework provides Poland with systematic pathways to transform from "AI infrastructure builder" to "AI-powered SME ecosystem" through proven adaptation of Korea's success models within the EU regulatory context. The six-pillar approach addresses identified gaps while leveraging Poland's substantial advantages, creating a sustainable ecosystem for development that positions Poland as a leader in Central European AI, supporting SME innovation.

The analysis reveals that Poland faces a fundamental paradox, where substantial infrastructure investments coexist with minimal SME utilization, representing an unrealized economic potential of EUR 134 billion. This can be articulated as "Poland is building the highway (AI infrastructure), but SMEs need to be ready to drive on it." The transformation requires addressing multi-dimensional barriers, including measurement inconsistency, governance fragmentation, regulatory burden 2.5 times higher than Korean counterparts, and socio-cultural resistance, where 80.7% of SMEs believe AI is "not necessary."

Implementation success requires coordinated action across governance enhancement addressing current ministry fragmentation, demand creation through voucher programs covering up to 80% of costs, regulatory innovation transforming compliance from barrier to competitive advantage, specialized support programs recognizing that microenterprises represent 97% of Polish enterprises, regional development leveraging specialized strengths, and university partnerships addressing talent shortages where only 44.3% of Poles have basic digital skills compared to EU average of 55.6%.

The three-phase timeline presents realistic yet ambitious targets, building momentum toward the critical 16% adoption threshold, where innovation diffusion theory suggests exponential growth is expected to begin. This approach ensures sustainable progress toward Poland's 2035 objectives while creating competitive advantages in the evolving European AI landscape.

The Korea-Poland Partnership 2.0 provides ongoing collaboration opportunities that benefit both countries, contributing to a broader international understanding of effective AI ecosystem development strategies. The partnership framework creates mechanisms for sustained cooperation and mutual learning, extending beyond initial program implementation to create lasting value and continued innovation leadership.

Poland has the infrastructure, Korea has the experience, and SMEs have the potential. Now, systematic policy implementation must bridge the gap to realize the EUR 134 billion economic potential while establishing Poland as the Central European AI Hub Supporting SME Innovation. The window of opportunity is critical, as EU AI Act requirements create both a compliance necessity and a strategic positioning advantage for countries that can transform regulatory complexity into competitive strength.

The success of this transformation will determine whether Poland becomes a leader in European AI ecosystem development or remains constrained by the infrastructure-utilization paradox that currently limits its enormous potential. The framework presented here provides the roadmap; implementation requires political commitment, institutional coordination, and sustained investment in systematic SME support that connects world-class infrastructure to practical business innovation throughout Poland's diverse enterprise landscape.

References

Agrawal, A., Joshua Gans, and Avi Goldfarb. *Power and Prediction: The Disruptive Economics of Artificial Intelligence.* Harvard Business Review Press, 2022.

Amazon Web Services and Strand Partners. *Polish AI Barometer Report.* Luxembourg: Amazon Web Services, 2024a.

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

Board of Audit and Inspection. *AI Voucher Program Audit Report.* Seoul: BAI, 2025.

Bridge Economy. "AI 바우처 지원 사업 부실 운영·관리 적발 [AI Voucher Support Program Inadequate Operation and Management Detected]." Seoul: Bridge Economy, August 11, 2025.

Davis, Fred D. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology." *MIS Quarterly* 13, no. 3 (1989): 319–340.

Digital Poland Foundation. *Polish AI Ecosystem Report 2024.* Warsaw: Digital Poland Foundation, 2024.

Etzkowitz, Henry, and Loet Leydesdorff. "The Dynamics of Innovation: From National Systems and 'Mode 2' to a Triple Helix of University–Industry–Government Relations." *Research Policy* 29, no. 2 (2000): 109–123.

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

European Commission. *Digital Economy and Society Index (DESI) 2024: Poland.* Brussels: European Commission, 2024.

European Commission. *Digital Decade Report 2024: Country Report Poland.* Brussels: European Commission, 2024a.

European Commission. *PIAST AI Factory Investment Decision.* Brussels: European Commission, 2024b.

European Commission. *Digital Decade Report 2025: Mid-Term Assessment.* Brussels: European Commission, 2025.

Główny Urząd Statystyczny (Central Statistical Office of Poland). *Information Society in Poland: Statistical Survey Results 2023–2024.* Warsaw: GUS, 2024.

Kim, J., and S. Lee. "Sustainability Analysis of AI Voucher Programs in Korean SMEs." *Journal of Technology Innovation* 32, no. 4 (2024): 45–67.

Korea Chamber of Commerce and Industry (KCCI). *Survey on AI Technology Utilization in Korean Enterprises.* Seoul: KCCI, 2024.

Korea Data Agency (K-DATA). *Data Voucher Program Annual Report 2023.* Seoul: K-DATA, 2024.

Korea Development Institute (KDI). *Regulatory Sandbox Effectiveness Evaluation Report.* Seoul: KDI, 2024.

Korea Economic Institute of America (KEI). *Korea's AI Strategy and Implementation.* Washington, D.C.: KEI, 2024.

Korea Federation of SMEs (KFSMB). *SME AI Adoption Status Report 2025.* Seoul: KFSMB, 2025.

Korea Institute for Industrial Economics and Trade (KIET). *Policy Tasks for Expanding Corporate AI Adoption and Utilization.* Sejong: KIET, 2021.

Korea Institute for Industrial Economics and Trade (KIET). *AI Factory Implementation Strategy and Economic Impact Analysis.* Sejong: KIET, 2024.

Korea Legislation Research Institute (KLRI). *A Study on the Plan for Enacting an Integrated Law for the Regulatory Sandbox System.* Seoul: KLRI, 2023.

Korea SMEs and Startups Agency (KOSME). *SME Digital Transformation Status Report.* Seoul: KOSME, 2023.

Korean Government. *National AI Committee Establishment and Operation Plan.* Seoul: Office of the President, 2023.

KPI News. "대기업 65% AI 활용 중…중소기업은 35% 그쳐 [65% of Large Enterprises Using AI, SMEs Only 35%]." Seoul: KPI News, February 14, 2025.

Kwon, Jun-hwa. 중소기업의 *AI* 도입 및 활용에 관한 사례분석과 시사점 *[Case Analysis and Implications of AI Adoption and Utilization in SMEs].* Daejeon: Korea SMEs and Venture Business Research Institute, 2024.

Ministry of Digital Affairs, Poland. *Digitalization Strategy 2035.* Warsaw: Ministry of Digital Affairs, 2023a.

Ministry of Digital Affairs, Poland. *Reports on Digital Transformation and AI Adoption in Poland.* Warsaw: Ministry of Digital Affairs, 2023b.

Ministry of Economy and Finance (MOEF). *2025 Budget Allocation and Fiscal Priorities.* Seoul: MOEF, 2024.

Ministry of Employment and Labor (MOEL). *AI Workforce Development Program Guidelines.* Seoul: MOEL, 2024.

Ministry of Science and ICT (MSIT). *National AI Strategy.* Seoul: MSIT, 2019.

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

Ministry of Science and ICT (MSIT). *Regulatory Sandbox Annual Report 2024.* Seoul: MSIT, 2024a.

Ministry of Science and ICT (MSIT). *AI Factory Initiative Implementation Plan.* Seoul: MSIT, 2024b.

Ministry of SMEs and Startups (MSS). *2025 Budget and Fund Management Plan.* Seoul: MSS, 2024a.

Ministry of SMEs and Startups (MSS). *Smart Factory to AI Factory Transition Strategy.* Seoul: MSS, 2024b.

Ministry of SMEs and Startups (MSS). *SME Education and Training Support Programs.* Seoul: MSS, 2024c.

Ministry of Trade, Industry and Energy (MOTIE) and E-Consumer. *AI Adoption Survey of Korean Enterprises (via KPI News, February 14, 2025).* Seoul: MOTIE, 2025.

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

Personal Information Protection Commission (PIPC). *Guidelines on the Processing of Publicly Available Personal Information for AI Development and Service.* Seoul: PIPC, 2024.

Personal Information Protection Commission (PIPC). *Annual Reports, Press Releases, and Announcements regarding "Three Data Laws" Amendments, the Pre-Assessment System, and AI Data Regulatory Reforms.* Seoul: PIPC, 2024/2025.

Personal Information Protection Commission (PIPC). *MyData Implementation Guidelines.* Seoul: PIPC, 2025.

Poznań Supercomputing and Networking Center (PSNC). *PIAST AI Factory Technical Specifications and Implementation Plan.* Poznań: PSNC, 2024.

Rogers, Everett M. *Diffusion of Innovations.* 5th ed. Free Press, 2003.

Statistics Korea. *ICT Utilization Survey of Businesses 2024.* Daejeon: Statistics Korea, 2024.

Tornatzky, Louis G., and Mitchell Fleischer. *The Processes of Technological Innovation.* Lexington Books, 1990.

World Bank Group Korea Office. *Data Vouchers: Korea Case Study for Revitalizing the Data Ecosystem.* Innovation and Technology Note Series, 12. Washington, D.C.: World Bank, 2024.

ZDNET Korea. "AI 발전, '수요' 없인 불가…더존비즈온 '중소·중견기업 DX 시급' [AI Development Impossible without Demand: Douzone Bizon Urges SME DX at National Assembly AI G3 Forum]." Seoul: ZDNET Korea, August 1, 2025.

03

Chapter

Cybersecurity Innovation Ecosystem and Regulatory Reform for Polish SMEs

Hyung-Jong Kim (Seoul Women's University)

Keywords:
Cybersecurity, Small and Medium Enterprise (SME), Government Policy, Technology Protection

Cybersecurity Innovation Ecosystem and Regulatory Reform for Polish SMEs

Hyung-Jong Kim (Seoul Women's University)

1. Introduction

In this report, we present research findings from site visits to Poland and interviews with Polish experts from both public and private sectors regarding cybersecurity practices among SMEs. It is widely acknowledged that cybersecurity regulations and their implementation constitute fundamental components of digital transformation; this principle should apply equally to SMEs, regardless of the operational challenges they face.

Korea and Poland have similar backgrounds concerning cybersecurity issues, particularly in their relationships with neighboring countries. To protect their national information assets, both countries have made extensive efforts by enacting laws and introducing regulations. Almost all essential institutional frameworks for cybersecurity and privacy, such as ISMS, CSAP, CCRA, and ISO/IEC 27001, have been well established. Regarding cybersecurity technologies and tools, both countries are well-equipped with advanced capabilities in both the public and private sectors. Poland, in particular, has a distinguished legacy in the field of security, dating back to its role in the cryptanalysis of the Enigma machine during World War II. This tradition continues today through brilliant cybersecurity experts who have discovered critical vulnerabilities in widely used platforms such as Java, Gmail, and major cloud services.

In Korea, cybersecurity is primarily governed by the Act on Promotion of Information and Communications Network Utilization and Information Protection and the Personal Information Protection Act. Similarly, Poland regulates cybersecurity through the Act on National Cybersecurity System (implementing the EU NIS Directive) and protects personal data via the Personal Data Protection Act (*Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679*). Specialized agencies such as KISA (Korea Internet & Security Agency) and NASK (Scientific and Academic Computer Network) facilitate the implementation of these frameworks.

Both Poland and Korea face a common challenge where Small and Medium-sized Enterprises (SMEs), which form the backbone of their robust economies, have become a vulnerable link in cybersecurity. In Poland, where SMEs represent approximately 99.8% of all enterprises, they are often overlooked in national cybersecurity strategies despite being core to the economy. As the transition to a digital economy accelerates, SMEs operating through online platforms have become increasingly

attractive targets for cyberattacks. However, despite being central to the national economy, SMEs encounter persistent barriers, including a lack of cybersecurity awareness, limited financial resources, and difficulties in securing skilled personnel. Polish SMEs exhibit a unique characteristic where a low rate of cyber incident experience (with 84% reporting no incidents) paradoxically leads to high security confidence (with 84% perceiving their measures as sufficient). This perception, however, results in weak cybersecurity governance. A point worth considering is that 84% of firms lack dedicated personnel, and less than half have formal security policies in place. While basic “Cyber Hygiene,” such as password management (86%) and software updates (83%), is relatively well-observed, these measures are limited to low-cost activities, and comprehensive security practices, like systematic risk assessments, remain inadequate. Similarly, Korean SMEs face serious cybersecurity challenges. They have become a primary target, accounting for 84.4% of all cyber incidents, which has led to a high level of risk awareness (79%). However, despite this recognition of the importance of security, the core problem is that 64.5% of firms have no information security budget or are unaware of its scale, resulting in virtually no security investment without government support. To address these issues, the Korean government is lowering the investment barrier for companies through financial programs, such as providing up to KRW 5.4 million in support for the adoption of security solutions. As a result, efforts to strengthen institutional responses are underway, with the adoption rate of security policies among companies approaching 60%. The table below summarizes the key differences in the cybersecurity posture of SMEs in both countries, based on the available data.

<Table 3-1> Comparison of Cybersecurity Posture of SMEs in Poland and Korea

Category	Indicator	Poland	Korea
Situation Diagnosis	Risk Perception	• 84% perceive themselves as "safe"	• 79% recognize the "importance of security"
Response Approach	Dedicated Personnel	• 84% of firms lack dedicated staff	• Data unavailable for firms with <10 employees
	Investment & Policy	• Investment: With digital transformation spending at only 1,000-2,000 PLN/year, cybersecurity investment is expected to be very minimal • Focus: Basic, low-cost activities (>80%) • System: <50% have security policies	• Problem: 64.5% lack a formal budget • Solution: Gov't support (up to KRW 5.4 million) • Result: Policy adoption approaching 60%

Source: KPMG Poland (2024), MSIT & KISI (2024), Kang (2023), Author (2025).

Recent studies on the cybersecurity of Polish SMEs have highlighted the current status, focusing on the following key aspects. In the Silesia region, the average cybersecurity score of 200 SMEs was 38.6 out of 70, with family businesses scoring lower than non-family businesses (36.72 vs 41.51). Technical safeguards, along with training, internal security meetings, and management involvement, were found to improve security levels (Šafár et al. 2025). Family SMEs, despite limited resources, employ strategies that combine advanced technologies with awareness-raising efforts; however, they have shown strategic shifts toward more conservative approaches during the COVID-19 pandemic, facing challenges such as resource constraints and varying levels of strategic planning (Siuta-Tokarska et al., 2023). Additionally, remote work has increased cybersecurity vulnerabilities, with 54% of Poles rating their cybersecurity knowledge as insufficient and 76% rating employer-provided training as poor, highlighting the need for comprehensive educational programs and stronger digital competency development (Ładny and Gutowski, 2023).

In conclusion, Poland's primary challenge lies in "raising basic risk awareness and establishing a minimal defense framework." For Korea, the key issue is that despite high threat awareness, security investment remains minimal without government support, highlighting the need for active government assistance to strengthen SMEs' practical cybersecurity capabilities. This suggests an urgent need for tailored support policies that consider the specific circumstances and ongoing foundational efforts in both nations. Ultimately, they share the common goal of establishing cybersecurity not merely as a cost or a regulatory burden, but as a core enabler for a successful digital transformation.

Poland's core cybersecurity legal framework is built upon the Act on the National Cybersecurity System (ANCS) of July 5, 2018, which implemented the EU's first NIS Directive into Polish law. This legislation established comprehensive requirements for operators of essential services (in sectors such as energy, transport, and banking) and digital service providers (including online marketplaces and cloud services), mandating them to implement security measures, manage cyber risks, and report incidents. The ANCS also created structural elements, including national and sectoral CSIRTs (Computer Security Incident Response Teams), with CERT Polska (operated by NASK, the Scientific and Academic Computer Network) serving as one of Poland's national CSIRTs, responsible for incident handling and supporting essential service operators.

Poland is currently updating its cybersecurity laws to align with the EU NIS2 Directive (2022/2555), which expands the scope of security requirements to additional sectors. The draft amendments replace previous entity categories with "essential entities" (podmioty istotne) and "important entities" (podmioty ważne), both of which have similar security obligations but different oversight regimes. These changes will significantly expand cybersecurity compliance requirements to cover a broader range of organizations, including medium-sized companies across various sectors. They will require risk assessments, rapid incident reporting, stronger authentication measures, and will impose substantial penalties for non-compliance.

Beyond the implementation of ANCS and NIS2, Polish organizations must also comply with other cybersecurity-related regulations. As an EU member state, Poland applies the General Data Protection Regulation (GDPR) directly, supplemented by its national Personal Data Protection Act, requiring companies to secure personal data and report breaches to the national data protection authority (UODO). The EU Cybersecurity Act (Regulation 2019/881) established a certification framework in which Poland actively participates - NASK operates an accredited certification body and issues Common Criteria cybersecurity certificates recognized throughout Europe.

Sector-specific regulations provide additional requirements in certain industries. The Electronic Communications Law implements the EU Electronic Communications Code, which imposes network security obligations on telecom operators. Meanwhile, financial institutions are subject to guidelines from the KNF (Polish Financial Supervision Authority) and must implement the EU's Digital Operational Resilience Act.

NASK plays a central role in Poland's cybersecurity ecosystem by operating CERT Polska, supporting essential service operators, providing certification services, conducting research, and offering educational initiatives. The private sector complements this governmental framework through compliance services, security solutions, incident response capabilities, and certification activities, creating an integrated approach to addressing the evolving landscape of cyber threats.

2. Overview and Assessment of Polish Cybersecurity Support for SMEs

Poland has established a range of public programs to enhance cybersecurity readiness among small and medium-sized enterprises (SMEs). These initiatives encompass various areas of support, including knowledge dissemination, technical services, certification processes, and ecosystem development. Despite these efforts, significant gaps remain in implementation and SME engagement. This chapter aims to provide a structured overview of the current support landscape by organizing the programs into functional categories and evaluating both their strengths and limitations.

2.1. Categories of Government Support Programs

Polish government initiatives can be broadly categorized into four types, each addressing a different aspect of cybersecurity capacity-building for SMEs. These include educational programs, certification initiatives, technical services, and broader ecosystem development efforts.

[Figure 3-1] Four Categories of Government Support Programs

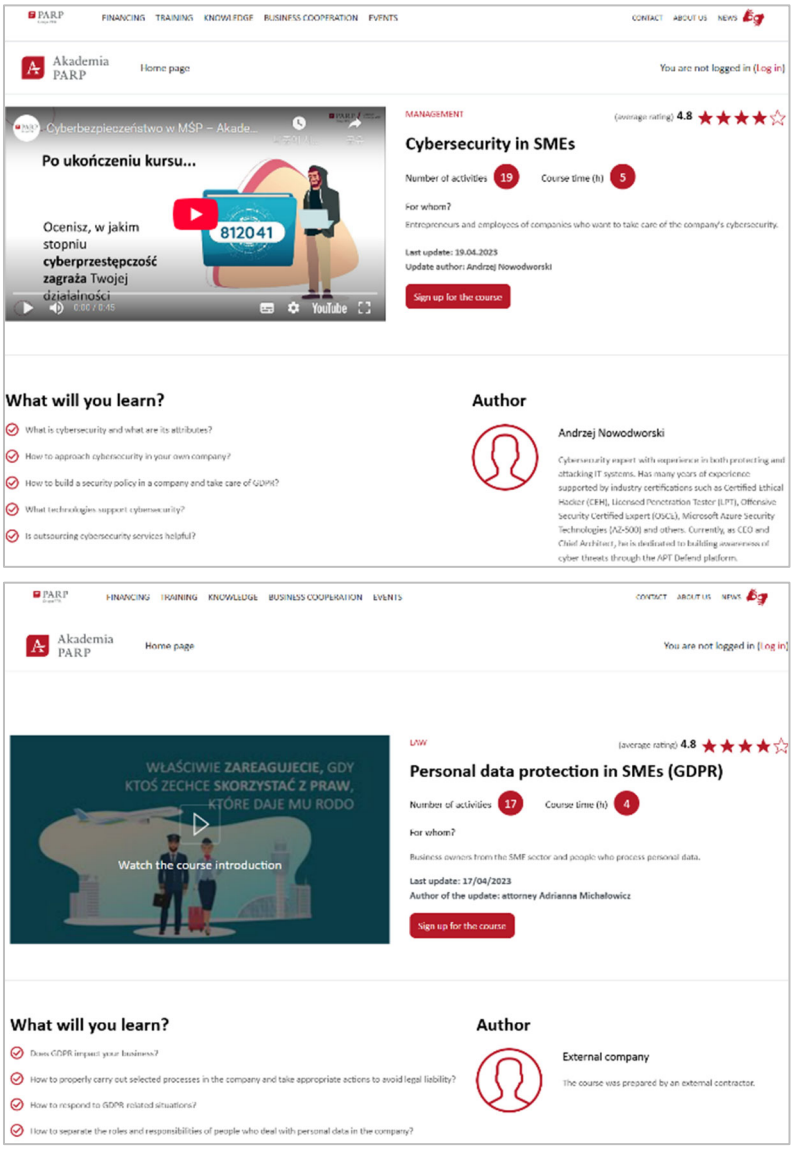
Knowledge & Capacity-Building	Certification & Compliance Support	Technical Assistance & Cybersecurity Services	Market & Ecosystem Development
• Free e-learning via *Akademia PARP* (by PARP) • Core topics: password hygiene, phishing, remote work, GDPR compliance • Includes certificates, webinars, and practical guides	• *Firma Bezpieczna Cyfrowo* program by NASK • Self-assessment → tailored action plan → cybersecurity certification • Enhances trust and credibility with partners	• Provided through EDIH CyberSec (run by NASK and private partners) • Services: vulnerability scans, penetration testing, ISO 27001 support • Includes industrial system protection and SOC access	• Investments and grants from the Polish Development Fund (PFR) • *#CyberMadeInPoland* cluster connects over 30 SMEs • Up to €1.8M in funding for product development, certification, and export

Source: Author (2025).

2.1.1. Knowledge and Capacity-Building

One of the most fundamental needs for SMEs is a basic understanding of cybersecurity threats and best practices. To address this, the Polish Agency for Enterprise Development (PARP) offers an online education platform known as Akademia PARP. This platform offers free e-learning courses specifically tailored for SMEs. The curriculum encompasses essential topics, including password security, phishing awareness, secure remote work practices, and compliance with legal requirements such as the GDPR.

[Figure 3-2] PARP's Online Education for SMEs

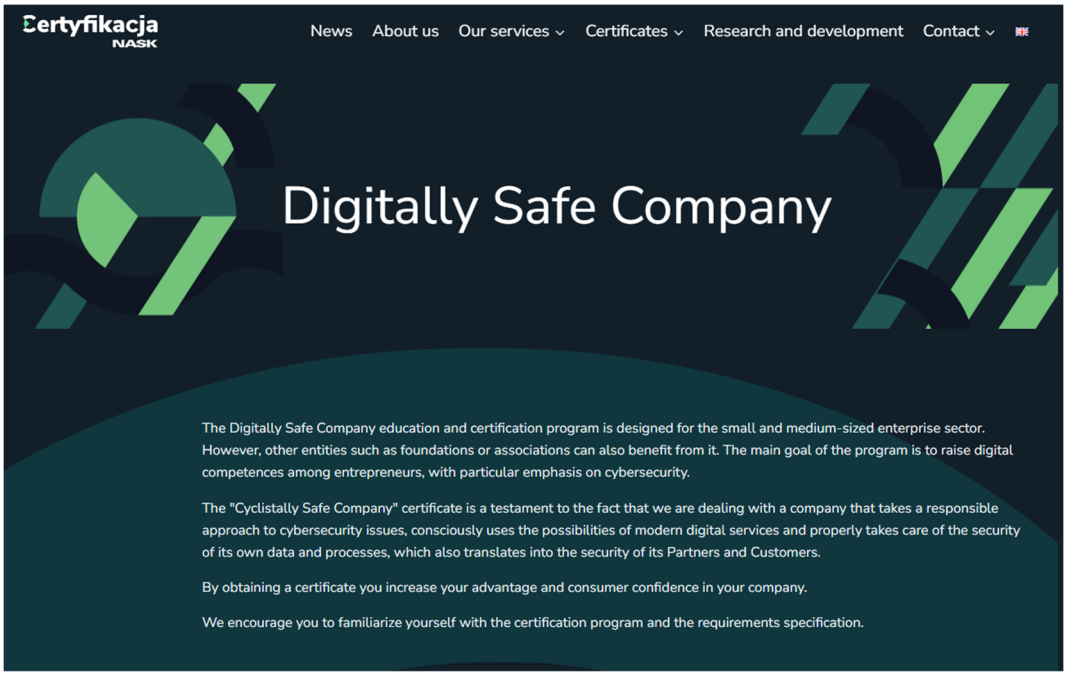


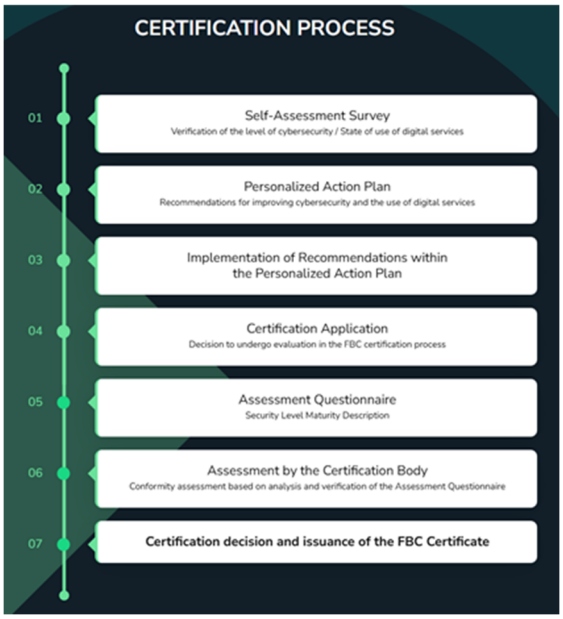
Source: PARP (2025).

Participants who complete the courses receive certifications, and PARP further supports learning through webinars and practical guides. These educational resources help reduce entry barriers for SMEs that often lack dedicated IT or security teams.

2.1.2. Certification and Standard Compliance Support

[Figure 3-3] NASK's "Firma Bezpieczna Cyfrowo" Program





Source: NASK (2025).

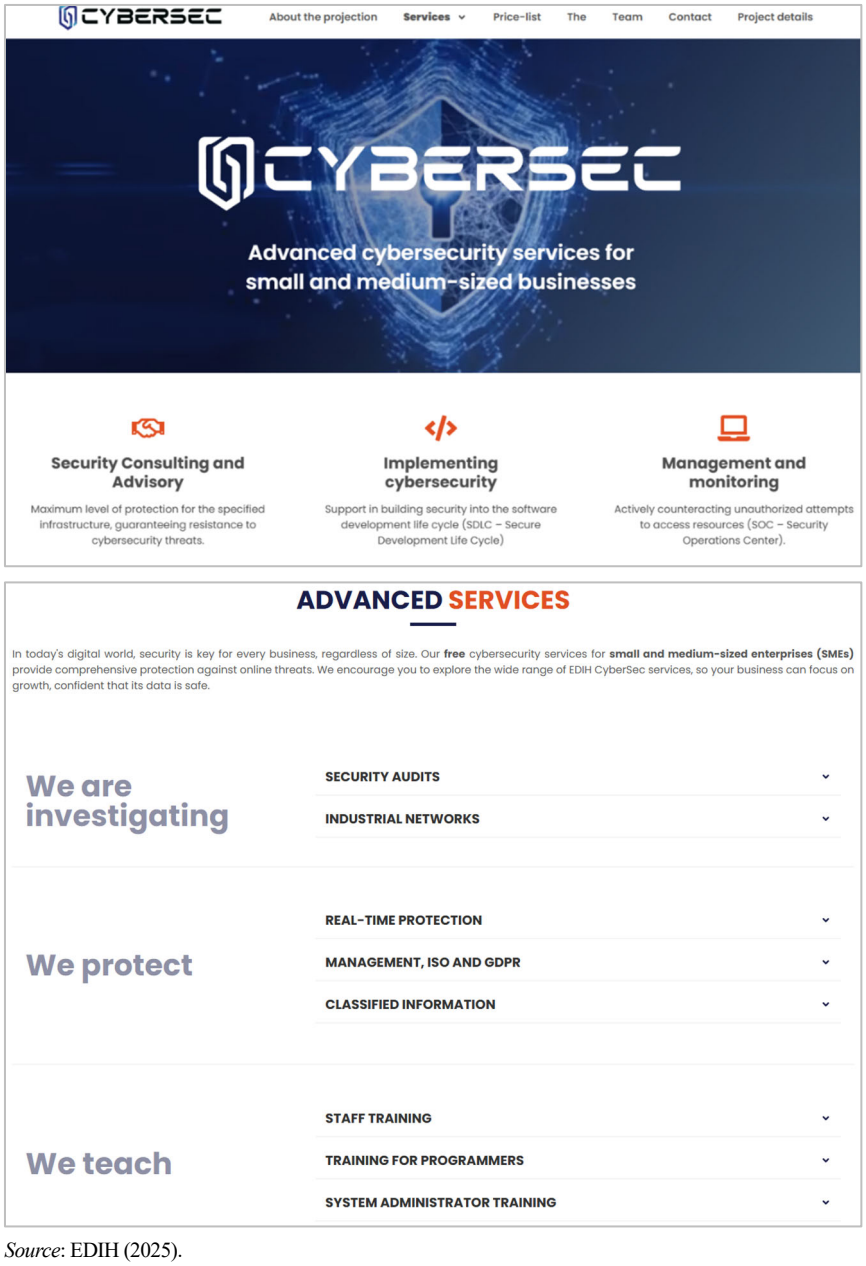
Beyond education, some SMEs are ready to formalize their cybersecurity efforts through certification. NASK's "Firma Bezpieczna Cyfrowo" (Digitally Safe Company) program offers a structured pathway to achieve this. Launched in 2022, the program begins with a self-assessment of the company's current cybersecurity posture. Based on this, SMEs receive a personalized action plan and access to educational resources. Once key improvements are implemented, businesses can pursue certification, which also serves as a marketing tool indicating their commitment to cybersecurity.

This initiative allows SMEs to gradually build maturity while gaining external validation, which can be especially valuable when engaging with larger corporate partners.

2.1.3. Technical Assistance and Cybersecurity Services

While knowledge and certification are important, many SMEs lack the technical capabilities to apply security measures effectively. To bridge this gap, the National Centre of Secure Digital Transformation was established as part of the EU's Digital Europe Program. This center operates through the European Digital Innovation Hub (EDIH CyberSec), in collaboration with NASK and private IT firms like ITTI.

[Figure 3-4] EDIH CyberSec (European Digital Innovation Hub) Cybersecurity Services



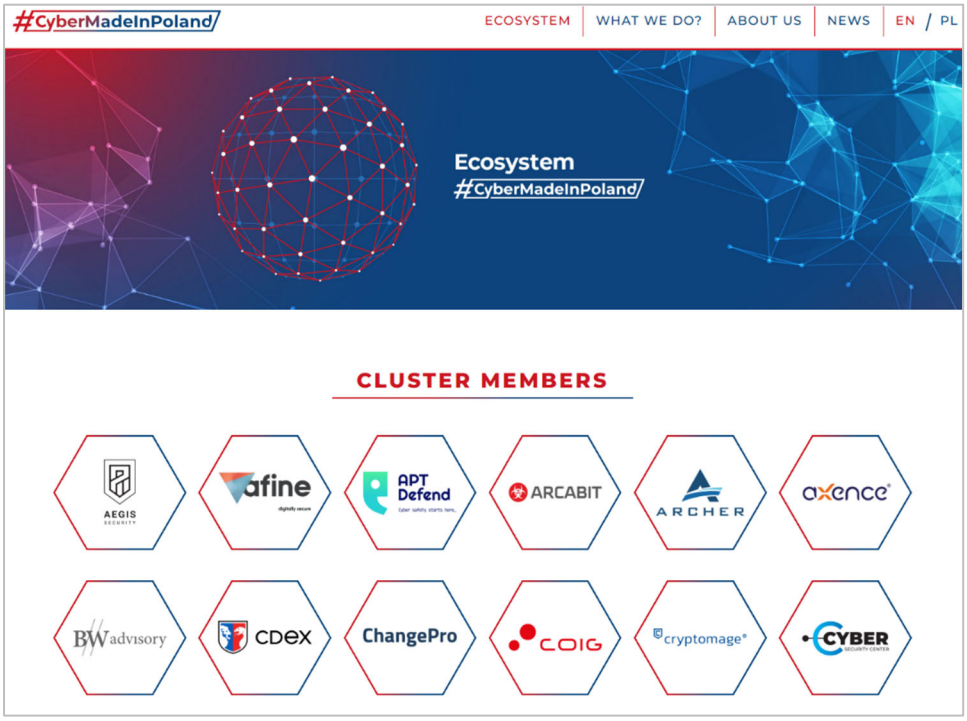
Source: EDIH (2025).

EDIH CyberSec offers a comprehensive range of technical services to SMEs, often at no cost or with significant subsidies. These services include vulnerability assessments, penetration testing, cybersecurity training, and support for implementing international standards, such as ISO 27001. Specialized support for industrial systems and access to Security Operations Center capabilities further enhance SMEs' ability to defend against cyber threats.

2.1.4. Market and Ecosystem Development

In addition to helping SMEs protect themselves, Poland has also invested in growing the national cybersecurity industry. The Polish Development Fund (PFR) supports this goal through various investment and grant programs. For instance, PFR Ventures provides funding to cybersecurity startups, and the establishment of the "#CyberMadeInPoland" cluster connects over 30 SMEs in the sector.

[Figure 3-5] PFR's Polish Cybersecurity Cluster (#CyberMadeInPoland)



Source: CyberMadeInPoland (2025).

Grants of up to EUR 1.8 million are available for product development, certification, and international expansion. These programs aim not only to strengthen domestic cybersecurity capacity but also to make high-quality, locally developed solutions more accessible to Polish SMEs.

2.2. SME Cybersecurity through Tailored Support and Sector Collaboration

This section presents observations on the current landscape of SME cybersecurity in Poland, focusing on two key aspects: the importance of tailored and accessible support mechanisms that reflect the diverse realities of SMEs, and the contrasting practices observed in large enterprises such as Microsoft and Allegro. These cases illustrate both the challenges that SMEs face in adopting cybersecurity measures and the potential value of sector-specific leadership and knowledge sharing within the broader ecosystem.

2.2.1. Tailored and Financially Supported Turnkey Cybersecurity for SMEs

One of the most notable challenges in SME cybersecurity is the gap between existing support programs and actual participation. In field interviews conducted at a manufacturing facility and within a special economic zone in Poland, some business representatives expressed a strong preference for turnkey solutions—pre-configured tools that require little customization or technical interpretation. They highlighted the appeal of support that can be immediately applied. While these insights do not represent all SMEs, they underscore a broader need for accessible, ready-to-use cybersecurity options that simplify implementation and reduce entry barriers.

This usability gap is further compounded by the wide variation in cybersecurity awareness across industries. Companies in digital sectors are generally more informed and better prepared, while firms in less tech-intensive sectors often struggle with low awareness—even among their managers. In such cases, the potential impact of cyberattacks on core functions such as payroll or production continuity is not always fully recognized.

Some SMEs operate using only basic digital tools, and while this may make their technical needs simpler, it does not eliminate the financial burden. Implementing and maintaining adequate cybersecurity still requires investment in tools, personnel, and ongoing support. For firms with limited financial and human resources, this creates a significant barrier. These constraints help explain why many SMEs have called for direct financial support to meet new regulatory obligations and adopt appropriate technologies.

At the same time, SMEs express diverse expectations regarding regulatory frameworks. Some prefer clear, prescriptive rules that reduce ambiguity, while others favor flexible guidelines that can be adapted to their specific contexts. This divergence highlights the need for a context-sensitive policy approach that acknowledges the diversity of SME environments rather than enforcing a uniform standard.

Furthermore, even well-designed programs often face challenges in execution. Follow-up mechanisms may be limited or misaligned with sector-specific realities, particularly for micro and small enterprises that operate with severe time, staffing, or compliance constraints. Policy strategies should therefore extend beyond good design and incorporate more granular, differentiated delivery models—for example, support tracks tailored to tech startups, traditional manufacturers, or family-run service businesses.

Rather than expecting SMEs to fit into rigid program templates, support mechanisms should prioritize adaptability and empathy. Providing flexible, stage-appropriate resources and maintaining iterative feedback loops will help align implementation with the real-world diversity of SME operations.

In summary, a one-size-fits-all solution is unlikely to work. Effective cybersecurity support for SMEs must combine tailored, turnkey tools, practical and context-aware training, and government-backed financial assistance. Ensuring equitable access, simplifying processes, and adjusting execution to fit the realities of SMEs will be key to improving cybersecurity adoption and resilience across the SME landscape.

2.2.2. Bridging the Cybersecurity Divide Through Sector Leadership and Knowledge Sharing

Field observations reveal a notable disparity between large enterprises and typical SMEs in Poland. For example, during stakeholder discussions related to the Legnica Special Economic Zone, it became clear that both SMEs and critical infrastructure providers in the region face broad and pressing cybersecurity needs. In contrast, visits to major companies such as Microsoft and Allegro revealed highly mature, sector-leading cybersecurity practices.

At Microsoft, the company demonstrated strong investment in AI and cloud-related technologies within Poland, signaling confidence in the country's digital infrastructure and talent pool. Discussions also reaffirmed that Polish cybersecurity professionals are internationally recognized for their technical expertise and real-world responsiveness.

Allegro provided an illustrative example of sector-specific leadership, not only maintaining a cybersecurity governance structure aligned with international standards but also demonstrating the potential to support individual e-commerce sellers through targeted security education and engagement. This would reflect a proactive approach to spreading security awareness beyond the firm itself and into its broader business ecosystem.

These contrasts reveal more than a capability; they expose an opportunity for sector-driven collaboration. Rather than treating large enterprises and SMEs as separate actors, Poland can benefit from establishing structured models for knowledge sharing, where companies like Microsoft and Allegro serve as sector mentors or digital anchors for their respective industries.

By building out mechanisms for knowledge transfer, sector-specific mentoring, and joint cybersecurity initiatives, Poland's SME support programs can become more grounded in real operational experience and technical relevance. This approach avoids the pitfalls of one-size-fits-all policies by fostering ecosystem-based preparedness, in which best practices flow from leaders to followers through trusted, domain-aware partnerships.

Ultimately, integrating corporate-sector leadership into national SME support frameworks—not just as beneficiaries but as active contributors—can significantly improve the reach, credibility, and resilience of Poland's cybersecurity ecosystem.

3. SMEs Supporting Program in Korea

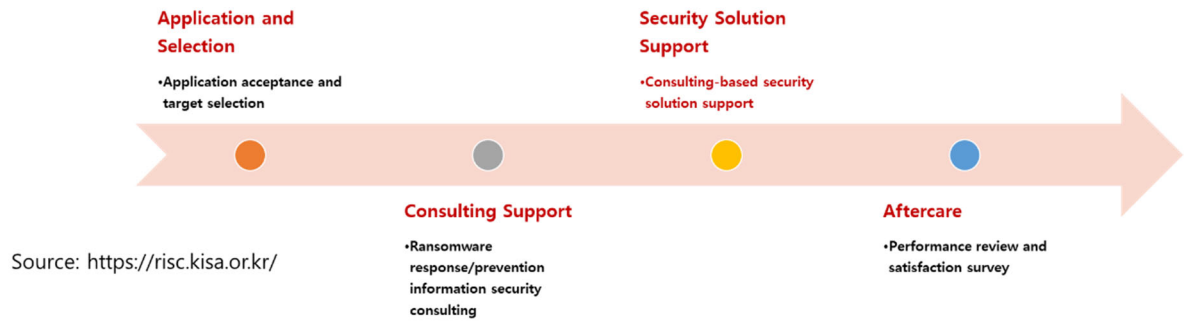
3.1. KISA's SME Support Programs

Information Protection Consulting and Security Solution Provision Program

The Information Protection Consulting and Security Solution Support Program is a Korean government initiative designed to address the fundamental knowledge gap in cybersecurity among SMEs. This program connects SMEs with professional consulting firms to establish essential cybersecurity knowledge and provides support for implementing tailored security solutions. The program follows a four-step process:

- **Application and Screening:** SMEs submit applications that undergo a screening process to determine eligibility and specific needs.
- **Specialized Consulting:** Qualified applicants receive consulting services with current emphasis on ransomware protection and prevention. Consultants identify specific threats and vulnerabilities within the SME's IT environment.
- **Solution Implementation:** Based on the assessment, appropriate security solutions are proposed and implemented.
- **Performance Evaluation:** Regular reviews and satisfaction surveys measure the program's effectiveness.

[Figure 3-6] Four-Step Process for Information Protection Consulting & Security Solution Provision for SMEs



Source: Author (2025).

Cloud-Based Security Service Provision

A distinctive feature of this Korean program is its focus on cloud-based Security as a Service (SECaaS) solutions, which offer several advantages for SMEs:

- Eliminates the need for complex on-premise security infrastructure management.
- Reduces initial capital expenditure requirements.
- Provides continuous updates and maintenance without specialized IT staff.
- Operates on a one-year subscription model aligned with the program's annual support cycle.

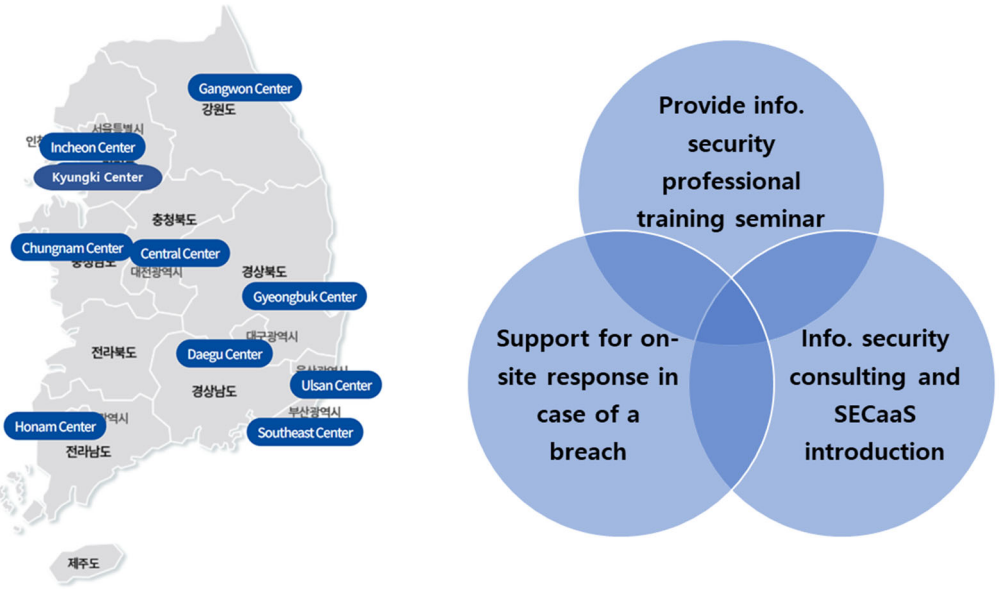
The program aims to achieve both immediate security improvements and long-term behavioral change:

- Build fundamental cybersecurity knowledge within participating SMEs.
- Address immediate security vulnerabilities through appropriate solutions.
- Familiarize SMEs with security technologies and their operational benefits.
- Shift perception of security solutions from optional add-ons to essential business tools.
- Encourage sustained investment in cybersecurity beyond the initial program period.

Local Information Protection Center Program

The Local Information Protection Center program addresses critical "blind spots" in Korea's national cybersecurity operations. Similar to challenges faced by many countries, Korea experiences various societal gaps—generational, economic, and gender-based—with particularly pronounced disparities between the Seoul/Gyeonggi metropolitan area and other regions. These disparities extend to information security capabilities, creating geographical and resource-based vulnerabilities in the national security posture.

[Figure 3-7] Geographical Location of Local Information Protection Center and Three Main Tasks



Source: Author (2025); KISA (2025a).

The program operates through a network of centers strategically positioned across ten regions throughout Korea, including Gangwon, Incheon, Gyeonggi, Chungnam, the Central region, Gyeongbuk, Daegu, Ulsan, the Southeast region, and Honam.

Each Local Information Protection Center implements several essential programs:

- **Regional Security Personnel Training:** Developing local cybersecurity talent and enhancing regional capabilities.
- **On-Site Incident Response:** Providing immediate support during security breaches.
- **Security Consulting and Solution Implementation:** Delivering the consulting and solution provision programs previously described.

To ensure effective resource distribution, the program stations Korea Internet & Security Agency (KISA) personnel directly in each region. These specialized staff leverage government funding to provide three categories of services to regional businesses, ensuring that cybersecurity expertise reaches beyond major urban centers.

The program recognizes and adapts to Korea's diverse industrial landscape:

- **Southeast Region (Busan and Ulsan):** Focuses on smart maritime and smart factory security solutions tailored for shipbuilding and heavy industries.
- **Incheon:** Specializes in cybersecurity for the biotech and semiconductor sectors.
- **Gangwon Region:** Emphasizes security for medical care and digital health industries.

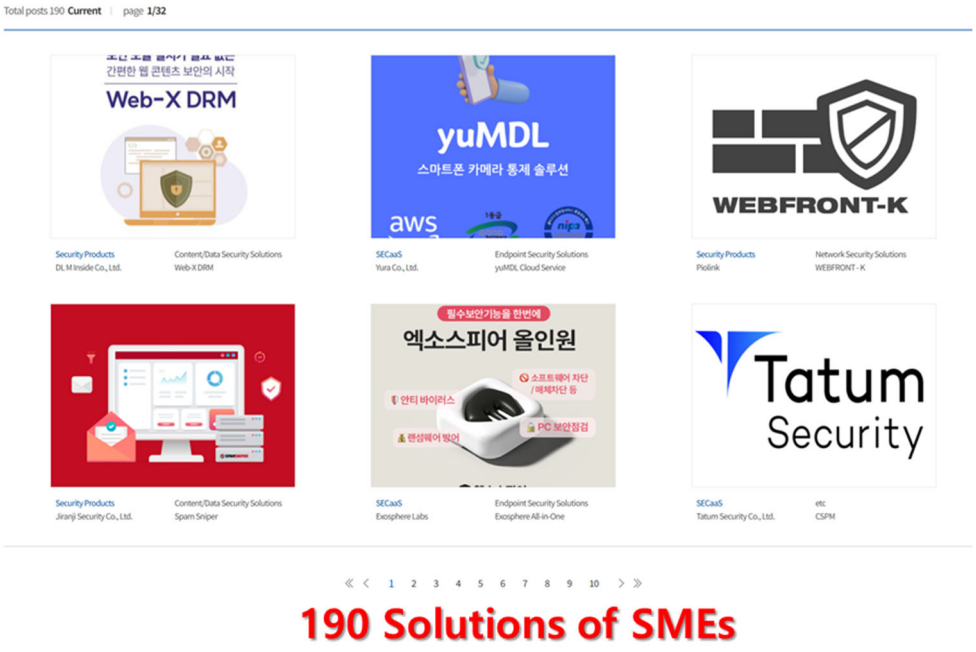
This regional specialization enables targeted information security applications that address industry-specific vulnerabilities and requirements. A key insight from the program is that effective cybersecurity implementation depends less on deploying different technologies and more on effectively communicating why security measures are necessary. The centers focus on helping regional stakeholders recognize the importance of protecting information systems within their specific industrial contexts.

The program has achieved significant results:

- **Tenant Companies:** 26 companies currently operating within the Gyeonggi and Southeast regional centers.
- **Product Testbed Utilization:** 60 companies have accessed testbed facilities.
- **Economic Impact:** 312 new jobs created through the program's activities.

The program offers SMEs access to a diverse portfolio of cloud-based security solutions. The current catalog includes 190 distinct security solutions, with the majority developed by SMEs in the cybersecurity sector in Korea. This approach serves dual purposes: supporting the security needs of SMEs while also strengthening the domestic cybersecurity industry.

[Figure 3-8] List of SecaaS Solutions for SMEs



Source: Author (2025); KISA (2025a).

ISMS Certification Simplification

The Information Security Management System (ISMS) serves as Korea's equivalent to the internationally recognized ISO 27001 standard. Recognizing the challenges SMEs face with comprehensive security certifications, the government has implemented significant streamlining measures:

<Table 3-2> Comparison of Simplified ISMS with Existing Framework

Category	Current System	Simplified System	Improvement
Certification Criteria	80 items	40-44 items	50% reduction
Certification Period	6 months	3 months	50% shorter
Certification Cost	KRW 10 million	KRW 5 million	50% cheaper

Source: KISA (2025b).

Under the previous framework, organizations needed to implement and demonstrate compliance with approximately 80 distinct control items spanning various aspects of information security and personal data protection. This comprehensive assessment typically required organizations to dedicate substantial resources over a 6-month certification timeline, during which they needed to prepare documentation, implement controls, and undergo rigorous audits. The financial burden was also considerable, with certification costs averaging around KRW 10 million (approximately USD 7,000), excluding the internal resources allocated to prepare for and maintain certification.

Recognizing these challenges, particularly for smaller organizations with limited resources, the Korean government launched a significantly streamlined ISMS-P certification process in July 2024. This reformed approach reduces the control items by 50%, effectively halving the compliance requirements to approximately 40 items. The certification timeline has been correspondingly shortened from six months to three months, allowing organizations to achieve compliance in half the time previously required.

The financial aspect has also been addressed, with certification costs reduced to approximately KRW 5 million (approximately USD 3,500). This 50% cost reduction makes the certification more accessible to a broader range of organizations, particularly those operating with constrained budgets.

Cloud Service Accreditation Program (CSAP) Simplification

The CSAP is a mandatory certification for cloud services intended for use by government and public institutions in Korea. Similar to the ISMS-P initiative, this program is being adapted to better accommodate SMEs:

Simplified CSAP Features

- Streamlined assessment criteria tailored to SME capabilities.
- Reduced documentation requirements.
- More accessible certification process.

Strategic Objectives

- Enable SMEs to more easily obtain required certifications.
- Lower barriers to entry for SMEs providing SaaS solutions.
- Increase SME participation in government/public sector cloud service provision.

The simplified versions of both ISMS-P and CSAP represent significant steps toward creating a more inclusive cybersecurity ecosystem that acknowledges the resource constraints of smaller businesses while maintaining appropriate security standards.

3.2. Overview of Cybersecurity SMEs & KISIA

Korea Information Security Industry Association (KISIA)

KISIA operates as a private industry association dedicated to promoting and developing the information security sector in Korea. The organization is primarily funded through membership fees contributed by participating companies. While these fees provide a foundation for operations, they are supplemented by various forms of government support that enable KISIA to expand its industry development initiatives.

[Figure 3-9] Roles of KISIA for Supporting Cybersecurity SMEs

Source: Author (2025).

Talent Development

KISIA implements specialized educational programs designed to address the cybersecurity skills gap in Korea. These initiatives focus on developing the technical and professional talent needed to support growth in the information security industry, helping to meet workforce demands across the sector.

Procurement Assistance

The association serves as a critical intermediary in the public procurement ecosystem for cybersecurity products and services. Recognizing the particular challenges that technical complexity and specialized requirements pose in the information security sector, the organization functions as a quasi-governmental entity providing comprehensive procurement support. This service includes a systematic review of government procurement specifications to identify provisions that may be unnecessarily restrictive, technically impractical, or disproportionately disadvantageous to smaller market participants. Upon identifying problematic requirements, the association collaborates with procurement authorities to recommend suitable modifications that maintain essential security standards while facilitating broader market participation.

This advocacy function helps establish procurement environments that balance security needs with fair competition principles. Additionally, the association provides specialized guidance to help SMEs successfully navigate the government procurement landscape, offering expertise on qualification requirements, proposal development, technical documentation, and compliance considerations. Through these multifaceted services, the organization helps create more equitable market access while simultaneously ensuring government agencies can benefit from the full spectrum of innovative security solutions available in the marketplace.

SME-Focused Training

KISIA delivers specialized training initiatives tailored to address the unique requirements of small and medium enterprises in the cybersecurity domain. These educational programs are strategically designed to accommodate the resource limitations, technical capabilities, and operational priorities characteristic of smaller organizations. The curriculum places particular emphasis on ransomware defense technologies and management approaches, providing practical implementation guidance that addresses this critical and evolving threat. Training content is carefully adapted to align with typical SME infrastructure environments and resource constraints, ensuring that security practices can be realistically implemented within existing operational frameworks. Additionally, the programs offer cost-effective professional development opportunities for technical personnel, enabling SMEs to enhance their internal security capabilities without significant financial investment.

Industry Advocacy

KISIA functions as the consolidated representative voice for Korea's cybersecurity small and medium enterprises in governmental forums and policy discussions. In this capacity, the organization systematically identifies common challenges, operational barriers, and growth impediments affecting member companies, and effectively communicates these issues to relevant policymaking bodies. The association actively participates in regulatory consultation processes, providing evidence-based input on proposed legislation and standards to ensure the practical implementation and proportionality of regulations for smaller market participants. Through formal participation in national cybersecurity planning committees and working groups, KISIA ensures that SME perspectives and capabilities are appropriately considered in the development of national security frameworks and initiatives.

Statistics of Korea’s Cybersecurity and Physical Security SME

The security sector in Korea demonstrates a robust presence of small and medium enterprises across both cybersecurity and physical security domains:

- **Information Security Companies:** 814 enterprises.
- **Physical Security Companies:** 894 enterprises.
- **Total Security Sector SMEs:** Approximately 1,708 companies.

<Table 3-3> Overview of the Security Sector in Korea Considering the Stock Market

Category	Information Security		Physical Security		Total	
	No. of Companies	(%)	No. of Companies	(%)	No. of Companies	(%)
Unlisted	730	89.7	851	95.2	1,581	92.6
KOSDAQ	63	7.7	34	3.8	97	5.7
KOSPI	20	2.5	6	0.7	26	1.5
KONEX	1	0.1	3	0.3	4	0.2
Total	814	100.0	894	100.0	1,708	100.0

Source: MSIT & KISIA (2024).

Twenty-six KOSPI-listed corporations fall outside the SME classification due to their size and capitalization. The prevalence of SMEs in this sector underscores their crucial role in Korea's security infrastructure. The security sector exhibits strong and consistent growth patterns, with the information security segment demonstrating particularly impressive expansion:

- **Information Security CAGR:** 14%.
- **Overall Security Sector:** Steady growth trajectory.

<Table 3-4> Security Industry Growth Trajectory from 2016 to 2023

Year	Information Security (KRW M/ USD M)	Physical Security (KRW M/ USD M)	Total (KRW M/ USD M)
2016	2,454,024M / 1,752.87M	6,588,787M / 4,706.28M	9,042,811M / 6,459.15M
2017	2,744,940M / 1,960.67M	6,840,822M / 4,886.30M	9,585,762M / 6,846.97M
2018	3,082,926M / 2,202.09M	7,034,918M / 5,024.94M	10,117,844M / 7,227.03M
2019	3,618,773M / 2,584.84M	7,561,734M / 5,401.24M	11,180,507M / 7,986.08M
2020	3,921,387M / 2,800.99M	8,302,865M / 5,930.62M	12,224,252M / 8,731.61M
2021	4,549,734M / 3,249.81M	9,311,446M / 6,650.99M	13,861,180M / 9,900.80M
2022	5,615,295M / 4,010.93M	10,563,226M / 7,545.16M	16,178,521M / 11,556.09M
2023	6,145,479M / 4,389.63M	10,685,568M / 7,632.55M	16,831,047M / 12,020.75M

Source: MSIT & KISIA (2024).

This growth rate indicates a vibrant and expanding market that continues to create opportunities for new entrants and existing players.

3.3. Korean SME Technology Protection Framework

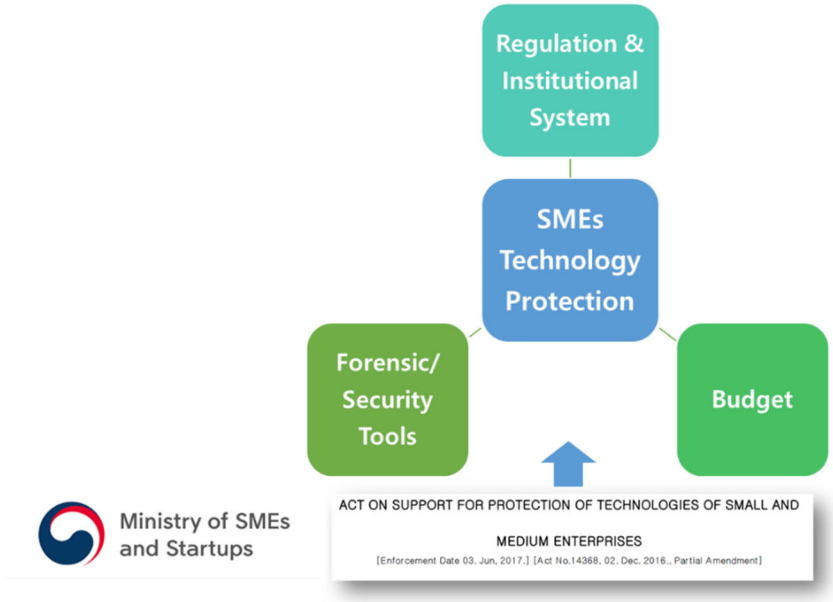
Korea has established a robust and comprehensive framework for safeguarding the technological assets of SMEs through the Act on Support for Protection Technology of SMEs, which was enacted in 2017. This legislative foundation was developed in response to the growing recognition that SMEs

face disproportionate risks from information leakage and unfair technology transactions, particularly in their dealings with larger corporations that possess greater legal and financial resources.

The framework addresses these vulnerabilities through a strategically designed multi-layered approach that combines regulatory protections, institutional support systems, and specialized security services. The regulatory components establish clear legal boundaries and consequences for technology misappropriation, creating deterrents against intellectual property infringement and establishing formal recourse mechanisms accessible to smaller businesses.

Supporting these regulations, the framework has established dedicated institutional systems staffed by specialists in technology protection who understand the unique challenges faced by SMEs. These institutions offer expert guidance on protective measures and facilitate access to various support programs tailored specifically to the SME ecosystem. The operational elements of the framework include technology escrow services that securely document and store critical intellectual property, transaction record registration systems that provide legally admissible evidence in cases of dispute, forensic investigation capabilities to analyze suspected breaches, and specialized security tools tailored to the technical environments and resource constraints of SMEs.

[Figure 3-10] Legal Framework for Protection of SMEs' Technologies



Source: Author (2025).

This comprehensive approach is sustained through dedicated government budget allocations that ensure the continuity and accessibility of protection services. The funding structure reflects the Korean government's recognition that protecting technological innovation within the SME sector represents a critical national economic interest and security priority. As will be presented in the following section of this report, the framework is implemented through four distinct phases that provide end-to-end protection throughout the technology lifecycle. These phases—Prevention, Escrow, Incident Response, and Damage Relief—create a continuous support system that addresses the full spectrum of protection needs from proactive safeguards to post-incident recovery.

The Korean SME technology protection system operates through four distinct stages, as shown in [Figure 3-11].

[Figure 3-11] Four-Phase Process for Protection of SMEs Technologies

- **Technology Protection Framework**

Prevention Phase	Escrow Phase	Response Phase	Relief Phase
• Technology Protection Voucher • Technology Protection Insurance • Technology Protection Service	• Technology Data Escrow • Transaction Record Registry	• Integrated Support Center • Technology Protection Team • Digital Forensics Support	• Legal Support Team • Damage Assessment Support

Source: Author (2025).

Prevention Stage

- **Technology Protection Voucher Program:** Provides tiered financial support (KRW 30-70 million) to approximately 250 companies annually based on evaluation scores.
- **Insurance Support System:** Covers 70-80% of premium costs for technology protection insurance, with rates varying based on domestic or export orientation.

[Figure 3-12] Operation Cases of Cybersecurity Technology Voucher Program for SMEs (as of 2024)

- **Technology Protection Voucher**
  - Scale: 250 companies
  - Features: 3-tier customized support

Best for: Companies requiring complex security solutions or comprehensive protection systems

Subsidy Category	Early Stage (Level 1)	Growth Stage (Level 2)	Advanced Stage (Level 3)
Score Range	Under 45 points	45-75 points	75 points or more
Voucher Amount	30 million KRW	50 million KRW	70 million KRW
Government Support	80% (Base+30%)	60% (Base+10%)	50% (Base)

Source: Author (2025).

Escrow Stage

- **Technology Escrow Service:** Securely stores critical technical data (production methods, designs, reports, source code) through third-party organizations at moderate costs (KRW 300,000 initial fee, KRW 150,000 annual fee).
- **Transaction Record Registration System:** Documents technology transactions through trusted third parties to provide verified evidence for potential disputes.

Incident Response Stage

- Offers 24/7 consultation services and reporting mechanisms.
- Coordinates with law enforcement for legal responses.
- Provides free forensic support for evidence collection.
- Offers financial support of KRW 5 million for response activities.

Damage Relief Stage

- **Legal Support Program:** Connects approximately 70 companies annually with legal professionals for 60 hours of consultation per company.
- **Damage Assessment Support:** Covers approximately 90% of damage assessment costs.

3.4. Technology Market Platform

The government operates a Technology Market platform showcasing SME technologies that have passed rigorous evaluation. This initiative offers significant benefits:

- Enables direct contracting without competitive bidding requirements.
- Allows SMEs to sell at list price to government agencies.
- Provides three-year browsing periods for quality assessment.
- Includes purchasing liability protection for government agencies.

[Figure 3-13] Technology Market for Promoting the Cybersecurity SMEs

Source: Author (2025).

This platform has proven particularly beneficial for software products, providing smaller businesses with streamlined access to government procurement opportunities that are typically not

available through traditional market channels. This systematic approach to protecting technological assets throughout their lifecycle demonstrates Korea's commitment to strengthening its SME ecosystem. The framework acknowledges that while technology protection remains fundamentally an SME's responsibility, government support systems provide an essential safety net, enabling more secure operations and sustainable innovation.

4. Comparative Analysis: Poland and Korea

4.1. Structural Comparison of SME Cybersecurity Support Systems

The comparative analysis reveals fundamental differences in how Poland and Korea have structured their SME cybersecurity support systems, reflecting their distinct national contexts and strategic priorities.

Legal and Regulatory Frameworks

Poland operates within a comprehensive EU-integrated legal framework, built upon the Act on the National Cybersecurity System, the implementation of the GDPR, and the EU Cybersecurity Act. This approach ensures strong alignment with European standards and facilitates cross-border business operations. In contrast, Korea has developed a domestically tailored framework centered on the Act on Promotion of Information and Communications Network Utilization, the Personal Information Protection Act, and notably, the specialized Act on Support for Protection of Technologies of SMEs, which provides unique legal protections specifically designed for small and medium-sized enterprises.

Regional Support Infrastructure Development

The notable difference lies in the approaches to regional support infrastructure. Poland maintains general SME support programs; however, development of cybersecurity-specific measures for SMEs is currently underway. Korea, in contrast, operates a network of 10 regional information protection centers, featuring region-specific industry focus with local personnel deployment, which demonstrates a more systematic approach to geographic accessibility.

Certification and Standards Approaches

Poland maintains standard EU certifications that ensure international alignment and global market compatibility, reflecting its integration within the European market. Korea has taken a different path by implementing simplified ISMS certification with a 50% reduction in requirements, prioritizing accessibility for SMEs over international standardization.

Technology Protection Mechanisms and Market Access

While Poland relies on the EU intellectual property protection framework supplemented by EDIH technical services, including vulnerability assessments and penetration testing, Korea has developed a comprehensive four-phase IP protection system with technology escrow services,

specialized legal support, and insurance subsidies that provide end-to-end protection throughout the technology lifecycle. In Poland, these EDIH services can serve as valuable security measures for SMEs; however, they do not constitute a codified, government-backed protection framework comparable to Korea's system.

<Table 3-5> Comparative Analysis of Key Program Elements

Program Element	Poland	Korea
Legal Framework	• Act on the National Cybersecurity System • GDPR implementation • EU Cybersecurity Act	• Act on Promotion of Information and Communications Network Utilization • Personal Information Protection Act • Act on Support for Protection Technology of SMEs
Regional Support Infrastructure	• General SME support programs are active • Efforts underway to develop cybersecurity-specific measures for SMEs	• Network of 10 regional information protection centers • Region-specific industry focus with local personnel deployment
Certification Processes	• Standard EU certifications ensuring international alignment	• Simplified ISMS (50% reduction in requirements) • Streamlined CSAP for cloud services
Technology Protection	• EU IP protection framework • EDIH technical services, including vulnerability assessments and penetration testing	• Comprehensive four-phase protection system • Technology escrow service with specialized legal support and insurance subsidies
Technical Services	• EDIH CyberSec provides comprehensive technical support • Free/subsidized professional services through the EU Digital Europe Program	• Cloud-based Security-as-a-Service model • Portfolio of 190 security solutions
Industry Association Role	• #CyberMadeInPoland cluster connecting 30+ SMEs • Substantial funding support (EUR 1.8M grants)	• KISIA as a centralized industry representative • Comprehensive advocacy and support functions
Educational Programs	• PARP's Akademia PARP: free e-learning, certifications, webinars	• Regional center training programs • SME-focused ransomware defense training

Source: Author (2025).

4.2. Implementation Approaches Comparison

The following table summarizes the key differences in implementation philosophies and operational approaches between the two countries, highlighting how each nation has adapted its cybersecurity support strategies to align with domestic priorities and institutional frameworks.

<Table 3-6> SME Support Characteristics in both Poland and Korea

Aspect	Poland	Korea
Support Philosophy	• EU-integrated approach with emphasis on international standards and cross-border cooperation	• Regionally distributed approach with focus on accessibility and administrative simplification
Service Delivery	• Technical excellence through EDIH with professional-grade services	• Simplified frameworks with turnkey solutions and local support
Geographic Coverage	• Centralized expertise with special economic zone coordination	• Nationwide distribution through dedicated regional centers
Industry Development	• Cluster-based development with substantial grant funding	• Industry association coordination with consistent sector growth
Certification Strategy	• Maintains EU standard alignment for international compatibility	• Adapts enterprise standards for SME capabilities
Technical Assistance	• Professional-grade services through EU program integration	• Integrated consulting with implementation support

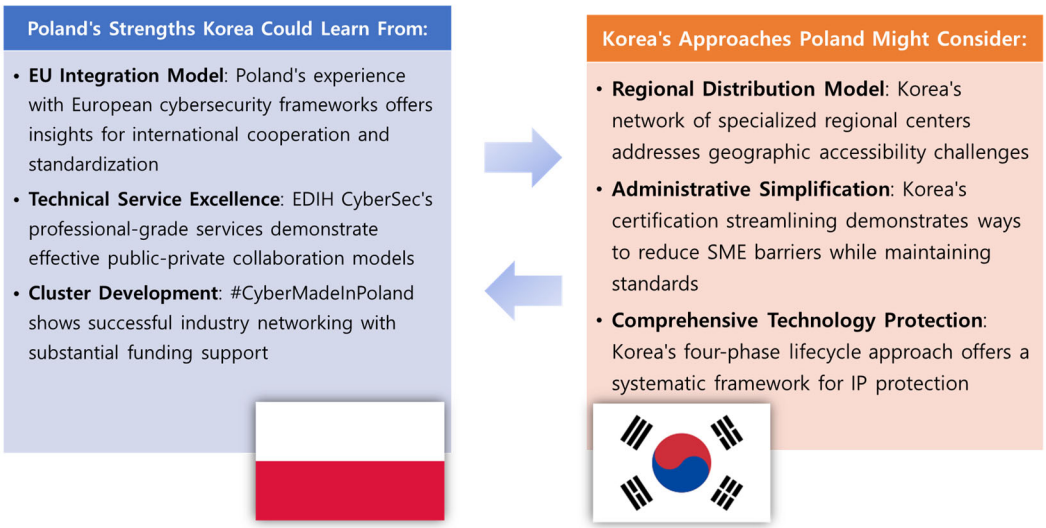
Source: Author (2025).

5. Bilateral Learning Opportunities and Collaborative Directions

The comparative analysis reveals that both Poland and Korea have developed distinctive approaches to supporting SME cybersecurity, each reflecting their unique national contexts, regulatory environments, and strategic priorities. Rather than suggesting that one model should be directly transplanted to another country, this analysis identifies valuable learning opportunities that could inform bilateral cooperation and mutual improvement of SME support systems.

5.1. Areas for Mutual Learning

[Figure 3-14] Mutual Learning Areas Identified Through Study Visits and Interviews



Source: Author (2025).

- **Poland's Distinctive Strengths Korea Could Learn From:** Poland's approach to SME cybersecurity support exhibits several notable characteristics that reflect its integration within the European Union framework and an emphasis on technical excellence. The country's experience offers valuable insights into international cooperation models and standardization approaches.
- **EU Integration Model:** Poland's experience with European cybersecurity frameworks, particularly through the implementation of the EU NIS Directive and GDPR, provides valuable insights for developing international cooperation mechanisms. Korea could benefit from understanding how Poland navigates multi-national regulatory coordination while maintaining effective domestic SME support.

- **Technical Service Excellence:** The EDIH CyberSec program demonstrates an effective model of public-private collaboration, delivering professional-grade vulnerability assessments and penetration testing services. This approach demonstrates how government programs can utilize EU funding to deliver high-quality technical services that might otherwise be prohibitively expensive for SMEs.
- **Cluster Development Approach:** The #CyberMadeInPoland initiative, connecting over 30 SMEs with substantial grant funding (EUR 1.8 million), illustrates successful industry networking and collaborative development. This cluster-based model demonstrates how government support can foster peer-to-peer learning and collaborative innovation within the SME cybersecurity sector.
- **Korea's Approaches Poland Might Consider:** Korea's systematic approach to SME cybersecurity support offers several innovations that address common challenges faced by small businesses across different national contexts. These approaches demonstrate how administrative processes can be adapted to SME capabilities while maintaining security effectiveness.
- **Regional Distribution Model:** Korea's network of 10 specialized regional information protection centers addresses the geographic accessibility challenge that many countries face. Each center's industry-specific focus (maritime/heavy industry in the Southeast, biotech/semiconductor in Incheon, medical/digital health in Gangwon) shows how regional expertise can be developed to serve local industrial needs more effectively.
- **Administrative Simplification:** Korea's systematic reduction of certification requirements (50% reduction in ISMS criteria, timeline, and costs) demonstrates that security standards can be made more accessible without compromising effectiveness. This approach addresses the resource constraints that often prevent SMEs from pursuing formal security certifications. Given that Poland needs to operate an institutional system consistent with the EU, it should consider the applicability of domestic certifications such as ISMS. Furthermore, the effectiveness of a simplified ISMS, as implemented in Korea, should be continuously monitored.
- **Comprehensive Technology Protection Framework:** Korea's four-phase lifecycle approach (Prevention, Escrow, Incident Response, Damage Relief) offers a systematic framework for intellectual property protection that extends beyond traditional cybersecurity measures. This comprehensive approach recognizes that SME vulnerabilities often extend beyond technical security to include business and legal risks.

5.2. Collaborative Exploration Areas

Both countries face similar fundamental challenges in translating available cybersecurity support into actual SME implementation and adoption. These shared challenges create opportunities for collaborative research and knowledge exchange that could benefit both nations' approaches to SME cybersecurity support.

Joint Research Opportunities

- **Implementation Gap Analysis:** Both Poland and Korea experience disconnects between program availability and SME participation. Collaborative research could explore the factors that influence SME decision-making regarding cybersecurity investment and identify more effective engagement strategies that work across different cultural and economic contexts.
- **Turnkey Solution Development:** Field interviews in Poland revealed SME preference for pre-configured, ready-to-implement solutions, while Korea's experience with cloud-based Security-as-a-Service models offers practical insights. Joint research could explore how different countries can develop culturally appropriate "turnkey" solutions that address SME resource constraints.
- **Leveraging Regional Economic Zones for Distributed Support:** While Korea is actively implementing efforts through its distributed regional approach, Poland's existing special economic zones present untapped potential for decentralized cybersecurity support delivery. Comparative research could explore how Poland might leverage its regional economic zones to provide localized SME cybersecurity assistance, creating a more distributed model that brings support closer to regional SMEs and enhances their security posture through zone-specific coordination and resources.

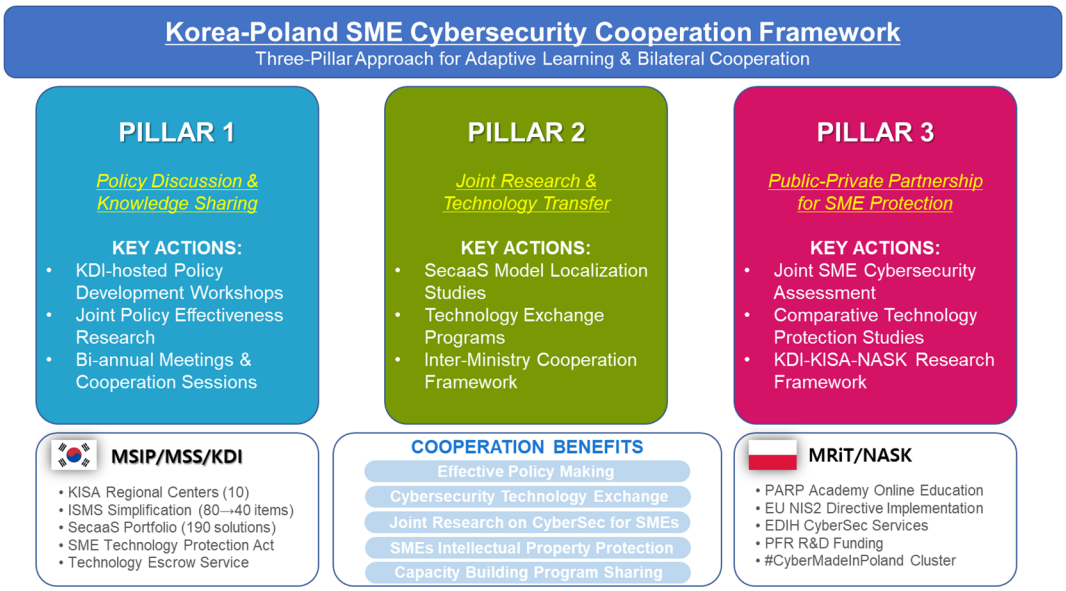
Knowledge Exchange Programs

- **Best Practice Documentation and Sharing:** Regular exchanges between Korean regional center specialists and Polish EDIH CyberSec professionals could facilitate knowledge transfer regarding effective SME engagement techniques, technical service delivery, and program adaptation strategies.
- **Policy Innovation Collaboration:** Both countries could benefit from collaborative development of SME-friendly regulatory frameworks that balance security requirements with practical implementation constraints. This could include joint research on simplification strategies for certification and regulatory harmonization approaches.
- **Industry Development Strategies:** Korea's cybersecurity industry association model and Poland's cluster approach (#CyberMadeInPoland) represent different but potentially complementary strategies for building robust domestic cybersecurity ecosystems. Collaborative exploration could identify hybrid approaches that combine the strengths of both models.

5.3. Future Bilateral Cooperation Framework

The analysis suggests that the most productive approach to bilateral cooperation would focus on adaptive learning rather than direct policy transfer. Both countries have developed effective solutions within their respective contexts, requiring an understanding of how successful elements from each system might inform improvements in the other while respecting distinct national, regulatory, and cultural factors. As a future bilateral cooperation framework, a three-pillar SME cybersecurity support plan is presented as shown below.

[Figure 3-15] Korea-Poland SME Cybersecurity Cooperation Framework



Source: Author (2025).

Pillar 1: Continuous Policy Dialogue and Knowledge Sharing Platform

Establishing both online and offline mechanisms for ongoing policy content sharing and effectiveness evaluation is essential for sustained bilateral learning. This platform would facilitate regular exchanges of policy updates, implementation experiences, and outcome assessments between both countries.

Korea's experience with KISA's regional information protection centers and ISMS simplification process offers valuable insights for distributed support systems. At the same time, Poland's EU NIS2 directive implementation and PARP Academy online education platform demonstrate effective compliance and educational approaches.

Key Actions:

- Establish KDI-hosted policy development workshops with Poland's Ministry of Economic Development and Technology.
- Conduct joint policy effectiveness research comparing Korea's certification simplification with Poland's EU standard application.
- Implement bi-annual policy briefing sessions and annual cooperation meetings for continuous knowledge exchange.

Pillar 2: Joint Research and Technology Transfer Initiative

Small-scale collaborative research projects should be developed to create technologies and knowledge transfer systems that benefit SMEs in both countries. This framework would enable

Korean cybersecurity SME capabilities to be disseminated in Poland while leveraging Poland's distinguished technical workforce to strengthen Korea's information security capacity.

Korea's comprehensive approach includes a four-phase SME technology protection system and 190 cloud-based security solutions through its SecaaS portfolio. At the same time, Poland offers professional technical services through EDIH CyberSec and substantial R&D funding through PFR.

Key Actions:

- Launch feasibility studies for localizing Korea's SecaaS model to Polish manufacturing environments.
- Facilitate technology exchange programs between Korean companies (WINS Technet, AhnLab, Somansa, and others) and the Polish #CyberMadeInPoland cluster.
- Develop a joint technology cooperation framework between the Korean Ministry of Science and ICT and Poland's Ministry of Economic Development and Technology.

Pillar 3: Public-Private Partnership for SME Protection

Given both countries' similar geopolitical positions, cooperation should encompass both government and private sector collaboration to enhance SME digital transformation capabilities. This pillar aims to ensure that SMEs in both countries can safely protect their intellectual property and customer personal information while pursuing digital transformation.

Korea's comprehensive SME Technology Protection Act provides a robust framework, including technology escrow services and insurance premium support. In contrast, Poland's implementation of EU directives offers sophisticated compliance mechanisms through CERT Polska and Common Criteria certification.

Key Actions:

- Conduct joint assessment of SME cybersecurity implementation status in both countries by defining Key Performance Indicators (KPIs) to facilitate systematic performance management.[1]
- Develop comparative studies of technology protection mechanisms and practical guidelines for SME digital transformation.
- Establish a research cooperation framework through KDI-led policy research and KISA-NASK data sharing partnerships.

To implement this cooperation framework, the following initiative is proposed as the most likely to yield practical results. The Korea–Poland Cybersecurity Exchange and Research Program encompasses technology exchange between Korean companies and the Polish #CyberMadeIn

[1] Examples of KPIs may include the level of improvement in SME security capabilities, the growth rate of participation in government support programs, and the percentage of SMEs obtaining relevant certifications.

Poland cluster, as well as a research cooperation framework through KDI-led policy research and KISA–NASK data sharing partnerships. This program is expected to serve as a practical and effective platform for mutual information and knowledge sharing. In subsequent stages, it will be necessary to develop and implement detailed plans through consultations between KDI and MRiT.

6. Conclusion

This study has examined the cybersecurity innovation ecosystem and support frameworks for Small and Medium Enterprises in Poland, with a comparative analysis drawing on Korea's experience. The research reveals that while Poland has established promising initiatives through organizations such as PARP, NASK, and PFR, a significant implementation gap remains, particularly for micro-enterprises and businesses outside major urban centers.

Korea's SME support ecosystem offers valuable reference points for knowledge sharing with Poland. Key elements of Korea's approach that could provide useful insights include regionally distributed information protection centers, simplified certification frameworks, cloud-based security service provision, comprehensive technology protection mechanisms, and streamlined procurement pathways for SME solutions. The proposed policy recommendations focus on bridging the implementation gap by:

- Creating more accessible support infrastructure through regional centers.
- Developing more realistic security standards through simplified certification.
- Reducing implementation barriers through cloud-based security services.
- Protecting SME innovations through comprehensive technology protection frameworks.
- Creating economic incentives through streamlined procurement access.
- Simplifying implementation through "turnkey" solution packages.

This comparative analysis reveals significant opportunities for mutual learning between the two countries. While Korea can offer insights into distributed support models and streamlined implementation approaches, Poland's EU-centered systematic information security governance framework provides valuable lessons for Korea. Poland's institutional approach, through organizations like PARP, NASK, and PFR, demonstrates a sophisticated integration of education, technical support, certification, and industry promotion that Korea can adapt to enhance its own SME support ecosystem.

The study concludes that both countries would benefit from establishing a collaborative framework to jointly develop practically effective cybersecurity innovation ecosystems that deliver tangible results for SMEs. This partnership should focus on continuous knowledge exchange, combining Korea's implementation-focused approaches with Poland's comprehensive governance structures to create more robust and effective support systems.

The experience of both countries demonstrates that effective cybersecurity for SMEs requires more than just educational resources or technical solutions; it demands a comprehensive ecosystem approach that addresses knowledge, implementation, certification, protection, and economic incentives in an integrated manner. Through sustained bilateral cooperation and knowledge sharing, both Poland and Korea can transform cybersecurity from a perceived barrier to digital transformation into an enabler of secure and sustainable growth for their respective SME sectors.

References

Act of 5 July 2018 on the National Cybersecurity System (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa). 2018.

Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (정보통신망 이용촉진 및 정보보호 등에 관한 법률). Amended to Act No. 18787, effective January 2024.

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

BoanNews. “82.5% of Cyberattack Damage in Korea Targets SMEs, Yet Security Budgets Slashed [한국 사이버공격 피해 82.5%가 중소기업...예산은 대폭 삭감].” July 8, 2025. https://m.boannews.com/html/detail.html?idx=133399.

CyberMadeInPoland. *#CyberMadeInPoland Initiative Report 2023 [#CyberMadeInPoland – Raport z inicjatywy, 2023].* Warsaw: Klaster Cyberbezpieczeństwa, 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, 27 December 2022.

EDIH CyberSec. *2024 Service Catalog (Katalog usług 2024)*. Warsaw: European Digital Innovation Hub (CyberSec), 2025.

European Commission and Ministry of Economic Development and Technology, Republic of Poland. *Advancing the Digital Transformation of Polish Enterprises: Current State Report.* July 2024.

Kang, Eun-Soo. “Measures to Strengthen Information Protection for SMEs [중소기업의 정보보호 강화 방안].” *National Assembly Research Service, Issues and Perspectives,* No. 2156, November 3, 2023.

Korea Internet and Security Agency (KISA). “Personal Information & Information Security Management System [개인정보 및 정보보호관리체계인증].” Accessed September 23, 2025. https://isms.kisa.or.kr/.

Korea Internet and Security Agency (KISA). “Regional Information Security Support Center [지역정보보호센터].” Accessed July 8, 2025. https://risc.kisa.or.kr/.

Korea SME Technology Market. “Korea SME Technology Market [중소기업기술마켓].” Accessed July 8, 2025. 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].” Accessed July 8, 2025. https://www.ultari.go.kr/portal/ptm/main.do.

Ładny, Piotr, and Piotr Gutowski. "Cyber Security of Remote Work in Poland and the EU – Selected Aspects." *European Research Studies Journal* 26, no. 4 (2023): 160–172.

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 and Korea Information Security Industry Association (KISIA). *2024 Survey on Information Security Industry in Korea [2024년 국내 정보보호산업 실태조사].* October 2024.

NASK. *Digitally Secure Company – Program Documentation (Firma Bezpieczna Cyfrowo – Dokumentacja Programu).* Warsaw: NASK, 2025.

PARP (Polish Agency for Enterprise Development). *Cybersecurity Training Resources for SMEs (Cyberbezpieczeństwo – materiały szkoleniowe dla MŚP).* Warsaw: PARP, 2025.

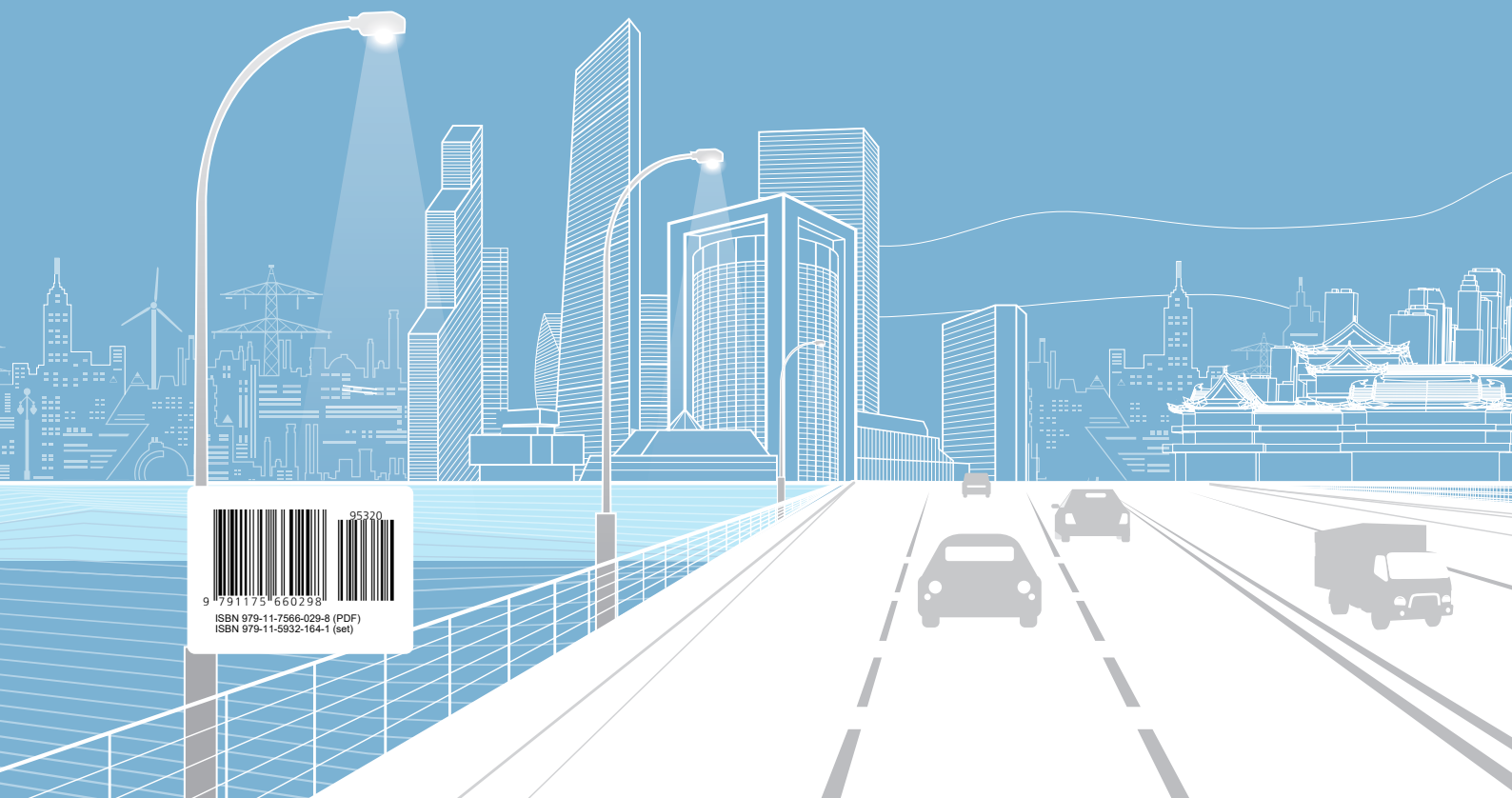
Siuta-Tokarska, Barbara, Justyna Juchniewicz, Małgorzata Kowalik, Agnieszka Thier, and Elwira Gross-Gołacka. "Family SMEs in Poland and Their Strategies: The Multi-Criteria Analysis in Varied Socio-Economic Circumstances of Their Development in Context of Industry 4.0." *Sustainability* 15, no. 19 (2023): 14140. https://doi.org/10.3390/su151914140.

Šafár, Leoš, Marek Pekarčik, Patryk Morawiec, Paulina Rutecka, and Monika Wieczorek-Kosmala. "Mapping Cybersecurity in SMEs: The Role of Ownership and Firm Characteristics in the Silesian Region of Poland." *Information* 16, no. 7 (2025): 590. https://doi.org/10.3390/info16070590.

Ministry of Economy and Finance (MOEF)
Sejong Government Complex, Doeuom 6-Ro, 42, Republic of Korea
Tel. 82-44-215-7742
www.moef.go.kr

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

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



ISBN 979-11-7566-029-8 (PDF)
ISBN 979-11-5932-164-1 (set)