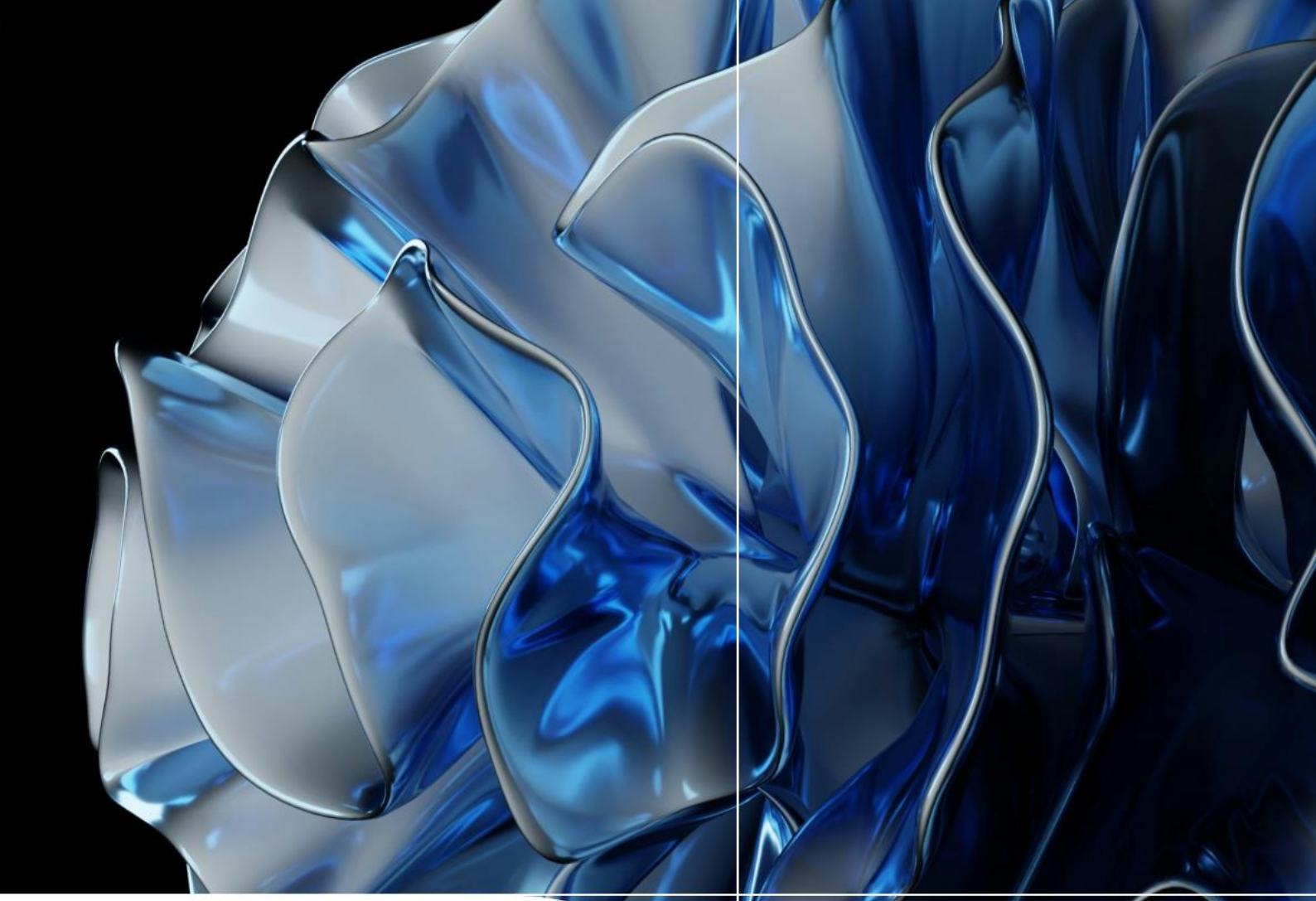


State Digitalisation Strategy

Draft for public consultation

Ministry of Digital Affairs
Republic of Poland

We Make the Future

Contents

Introduction

You are presented with a document constituting the first ever comprehensive digitalisation strategy for the country in the history of Poland. In recent years, digitalisation has gradually and rightly ceased to be perceived as a separate area of state activity or a sector of the economy similar to many others. Its horizontal character, affecting almost all areas of the functioning of society, the state and the economy, is increasingly being recognised. The sphere of digital technologies is a key field of intensifying geopolitical competition, and investments in this area indirectly (through dual-use technologies) or directly translate into the level of state security.

Poland faces the implementation of key objectives for the next decade. These objectives must take into account, among other things, the changing landscape of national security and the international environment, current trends and challenges in the area of technology and its regulation, as well as the specificity of Polish society and economy. Polish ambitions and activities fit into the context of the noticeable increase in the importance of digitalisation on the list of priorities of the European Union in recent years.

This strategy is a cross-sectoral strategic document in the field of computerisation of the state, defining the overarching goal of improving the quality of life of citizens through digitalisation by 2035. Its implementation is possible only through intervention in several areas that go beyond the traditionally defined section of administration – computerisation.[1] The objectives planned for implementation cover a broad spectrum of topics, starting from horizontal issues, through the level of the state and its citizens, ending with the economy and technological development. Such an approach made it possible to create a modern, cross-sectional vision of digital development that responds to current challenges, based on current European and global trends, resulting from the diagnosis of the current state of computerisation of the state and responding to formulated social expectations.

The initial chapters of the strategy include: a diagnosis of the state of computerisation based on the results of international indicators and studies; challenges and trends that influenced the determination of the directions of intervention; an analysis of strengths and weaknesses, as well as opportunities and threats to the digitalisation of Poland and an ambitious vision of digital transformation by 2035, along with a presentation of the overarching goal of the strategy and the conditions necessary for its implementation.

The next part the document covers horizontal areas which, due to their rank and importance, significantly influence the effectiveness of activities in other areas and constitute a starting point for the digital transformation of many areas of socio-economic life. Such areas include: electronic communications, competencies of the future, cybersecurity and coordination of digital transformation.

Other objectives of the strategy have been grouped into 17 areas, divided into the following levels: state, people, and

Act on departments of government administration of 11 September 2024 (Dz.U. /Journal of Laws/ of 2024, item 1370) 1

business and technology. The objectives within the state dimension focus on increasing and improving the quality of public e-services, digitalisation of administrative processes and court proceedings, optimisation of the functioning of systems and registers, development of digital identity, use of cloud computing and strengthening data openness and data exchange. The objectives within the people dimension concern not only the security of the digital space but, in line with the defined challenges and needs, they also include activities in the field of digital health, the development of creative industries and the development of academia and science in relation to the digital sector. The goals within the most cross-cutting business and technology dimension focus on: issues of digital business transformation, including activities supporting this process and relating to the development of e-services for entrepreneurs; priorities in the development of artificial intelligence and other breakthrough technologies, the development of space technologies, as well as financing and support for innovation and open source. This part also addresses the challenges as well as the goals and actions that address them in the areas of digital and green transformation.

The structure of all areas has been unified and includes an in-depth, detailed diagnosis (→ as is), goals corresponding to the formulated problems and deficits (→ as should be) and specific measures and actions that will allow the achievement of the desired state (→ which will enable the achievement of the goal). The document also includes measurable and real benefits that a citizen or entrepreneur will experience after the successful implementation of the planned activities and achievement of the intended goals. They constitute examples of how the quality of life will be improved, i.e. the overarching goal of the strategy.

The last chapter describes the strategy implementation system, relating to the method and principles of cooperation between entities affected by the computerisation process and its coordination, as well as the possibilities of financing activities. A special role in this respect has been assigned to the plenipotentiaries for computerisation and the Committee for Digital Affairs, which will replace the currently operating Council of Ministers Committee for Digital Affairs. The implementation of the ambitious vision of the strategy requires the implementation of coherent, harmonised and consistent actions, with close cooperation of stakeholders.[2] Monitoring of the strategy will involve measuring progress towards the stated objectives, throughout the life cycle of the strategy, and using the performance indicators included in the table at the end of the document. This task will be entrusted to the Minister in charge of computerisation, with the involvement of the other members of the Council of Ministers. Taking into account the principles of strategic management and the pace of technological development, regular evaluation and updating of the document is also planned.

The implementation of the strategy cannot take place in isolation from the strategic environment, both on the national and EU level. The objectives formulated in the strategy are reflected and detailed in many documents already in force or will be consistent with new versions of documents currently being developed, i.e. The Cybersecurity Strategy of the Republic of Poland (currently in force for 2019-2024, new document starting from 2025), National Broadband Plan (update in 2026), Digital Competence Development

[2] Based on the amendment to the Act on the computerisation of entities serving public functions of 20 February 20242 (Dz.U. /Journal of Laws/ of 2024, item 307) (UC 44).

Program, Data Opening Program (currently in force for the period 2021-27), Artificial Intelligence Development Policy (currently in force from 2020, planned update in 2025). However, due to the cross-sectional and cross-sectoral nature of the strategy, the directions of transformation included therein should be considered in the context of other sectoral strategic documents, including the Digital Transformation of Education Policy up to 2035, the Productivity Strategy up to 2030, Poland's Energy Policy up to 2040 or the migration strategy for the period 2025-30. Referring to the European strategic framework for digital transformation, the document takes into account and extends the objectives outlined in the 2030 Policy Programme “Path to the Digital Decade”. It covers areas not included in the EU objectives and also has a longer time horizon, reaching up to 2035.

The document was developed in the Ministry of Digital Affairs in cooperation with other government administration offices and taking into account the demands of social stakeholders and business communities. It will replace the Integrated State Computerisation Programme and will constitute a strategic basis for the expenditure of European funds earmarked for digitalisation, and will thus determine the direction of negotiations covering the upcoming financial perspective.

The challenges facing Poland in the areas of economic competitiveness, demography, security of the state and its citizens, and health mean that intensive investment in digitalisation in many areas is no longer a matter of choice. Instead, it is becoming a necessity, without which our country's position will clearly weaken. However, if digitalisation is given the priority it deserves, not only individual citizens – whose quality of life will improve – will benefit, but also Poland as a whole.

Krzysztof Gawkowski
Deputy Prime Minister,
Minister of Digital Affairs

Vision

Constantly accelerating technological development makes planning digitalisation activities for the next decade an extremely difficult task. It is made all the more difficult by the fact that digital technologies permeate almost every aspect of human life and, as a result, require close cooperation across the entire administration. This cooperation is possible when it is guided by a shared vision. This document outlines such a vision for the entire country as well as the actions leading to its implementation.

Our vision for 2035 focuses on people and how to most effectively improve the quality of life of citizens. In ten years, a visit to the office will be something unique – all key services will be available by phone, from anywhere in the country. State systems will automatically detect that some action should be taken and will offer a solution. A citizen or entrepreneur will never have to provide the same data twice – offices will exchange them on their own thanks to the full interoperability of systems and registers. Thanks to the planned improvement in coordination between different parts of the administration, we will avoid duplicate solutions and inconsistencies, and thus the waste of public money.

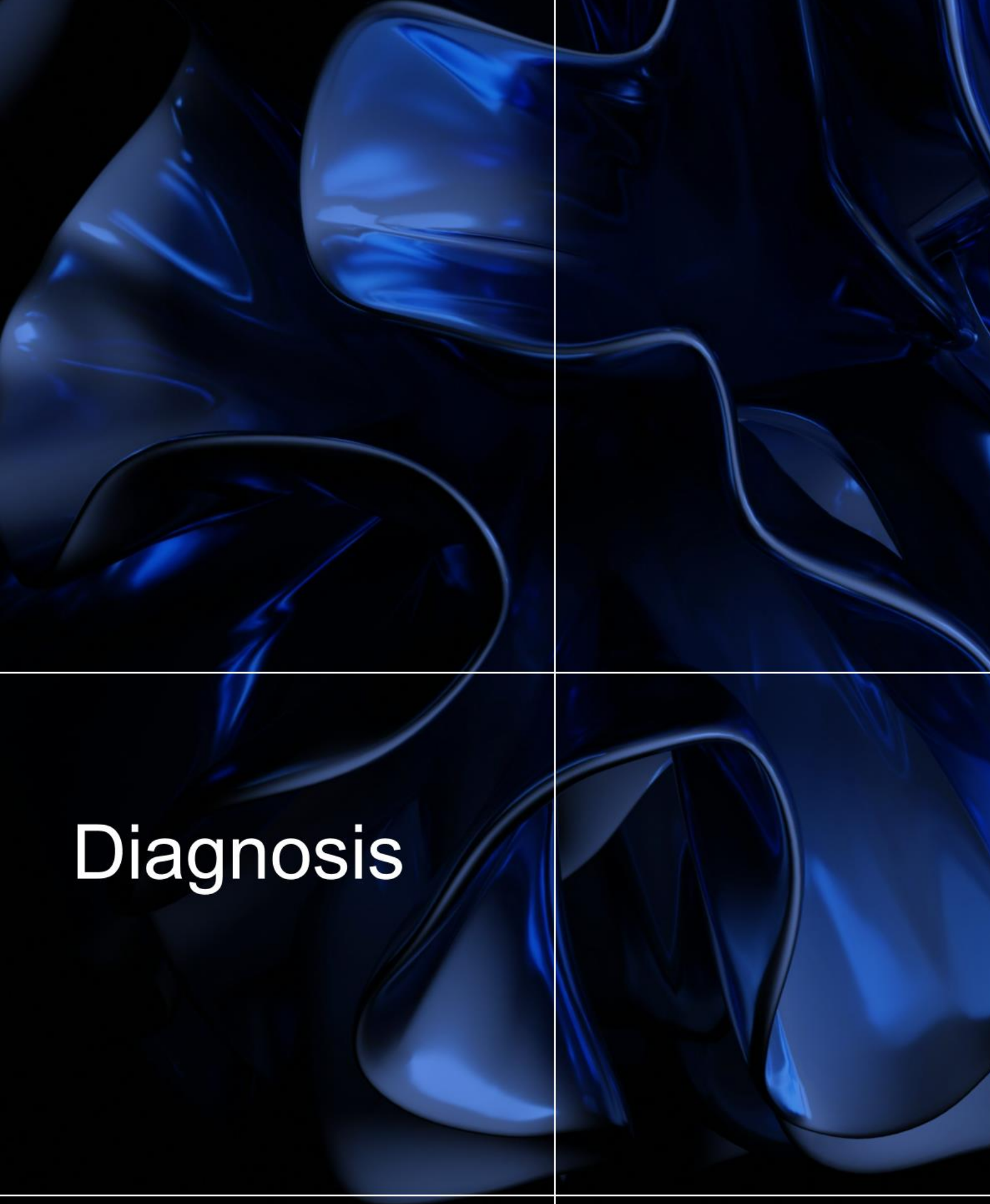
The intensive development of digital administration requires investment – in infrastructure, in the competences of public officers, and in ensuring the highest level of security of state systems and those that are of significant importance to the state. This is of particular importance given the serious deterioration in international security and the increase in cybercrime. However, we perceive security much more broadly – also in the context of mental health and the protection of citizens from harmful content. Therefore, we know that in 2035 Polish citizens must not only be highly competent in using digital technologies, but also be aware of how to use them in a healthy way, and sometimes - when it is advisable to simply disconnect. The development of the digital sphere must be sustainable – from a psychological, workforce and climate perspective.

The dissemination of technology seen in this way offers enormous opportunities to improve the quality of life and strengthen the Polish economy and international position. To achieve this, we will stimulate the adoption of technology – primarily artificial intelligence – in administration and among companies across various industries. We will provide a better framework for the development of technology at universities and in the economy, and we will stimulate the exchange of knowledge and personnel between business and science. We will improve the quality of work in academia and develop the infrastructure for Polish science.

Polish digitalisation has many areas we can be proud of, but we are not yet a leader in Europe, let alone the world. Streamlining the vision, implementing the actions envisaged therein and significantly increasing the funds allocated for digitalisation will help change this state of affairs. In ten years, Poland will be a true digital leader.

Selected goals for 2035

- All key services can be accessed via the mobile application.
- State systems and registries are fully interoperable.
- 20 million Poles have activated a digital identity wallet.
- Electronic payments are available throughout the administration.
- 50% of companies and 80% of offices use artificial intelligence technologies.
- All significant cybersecurity incidents are reported on time.
- There is high-speed Internet coverage in every corner of the country.
- As many as 85% of Poles have at least basic digital competences.
- The computing power available to scientists is at least ten times greater than today.
- All healthcare facilities exchange medical documentation in electronic form.



Diagnosis

Ministry of Digital Affairs
Republic of Poland

We Make the Future

Diagnosis

Digital Economy and Society Index (DESI)

The DESI results for 2017-2022 show that each year Poland ranked 24th among the 27 EU Member States. The digital gap is noticeable in all areas studied, such as digital competences, telecommunications, digital transformation of businesses and digital public services. However, progress in the field of digitalisation is becoming more and more visible. Over the past 5 years, Poland has improved its score from 24.9 points in 2017 to 40.6 points in 2022, thus ranking among the countries that are most rapidly catching up with the leaders. According to the analysis of the Polish Economic Institute (PIE), Poland's score in the DESI index during this period rose from 52.1% to 58.3% of the leader's score.[3]

DESI 2017-2022

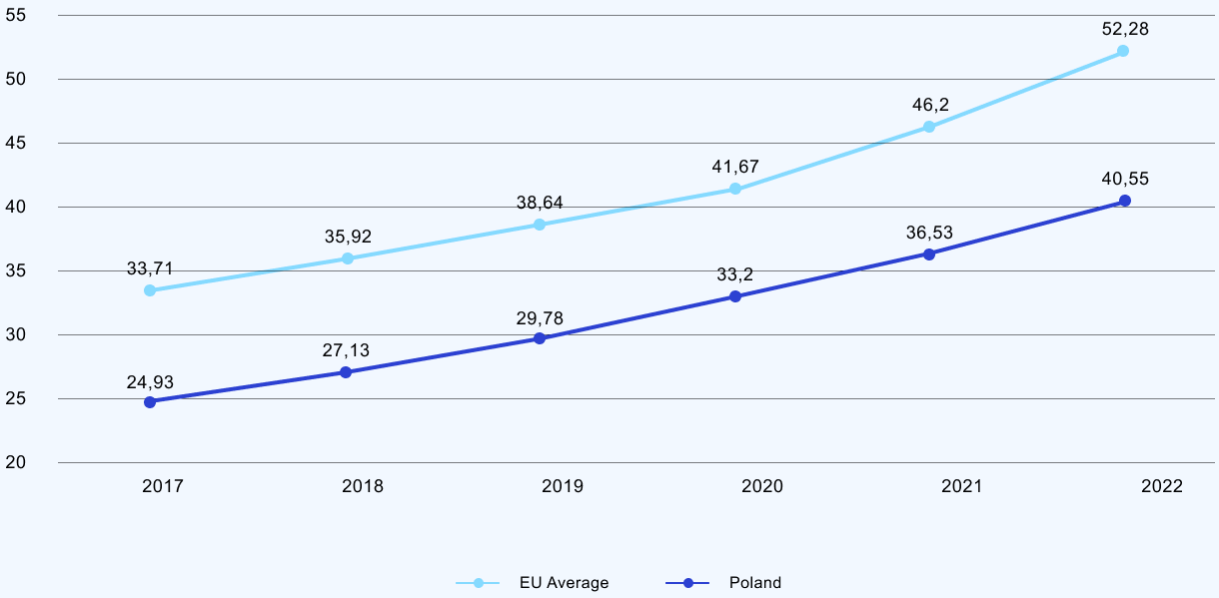


Figure 1 DESI 2017-2022, source: own study based on DESI 2017-2022 reports1

From 2023 onwards, in line with the EU's 2030 Policy Programme "Path to the Digital Decade", DESI is included in the programme's implementation report.[4] The European Commission has abandoned the idea of ranking Member States, but has instead provided a tool to compare countries' performance against each other and the EU average in individual

3 https://pie.net.pl/polska-wsrod-unijnych-liderow-postepu-w-rozwoju-cyfryzacji/

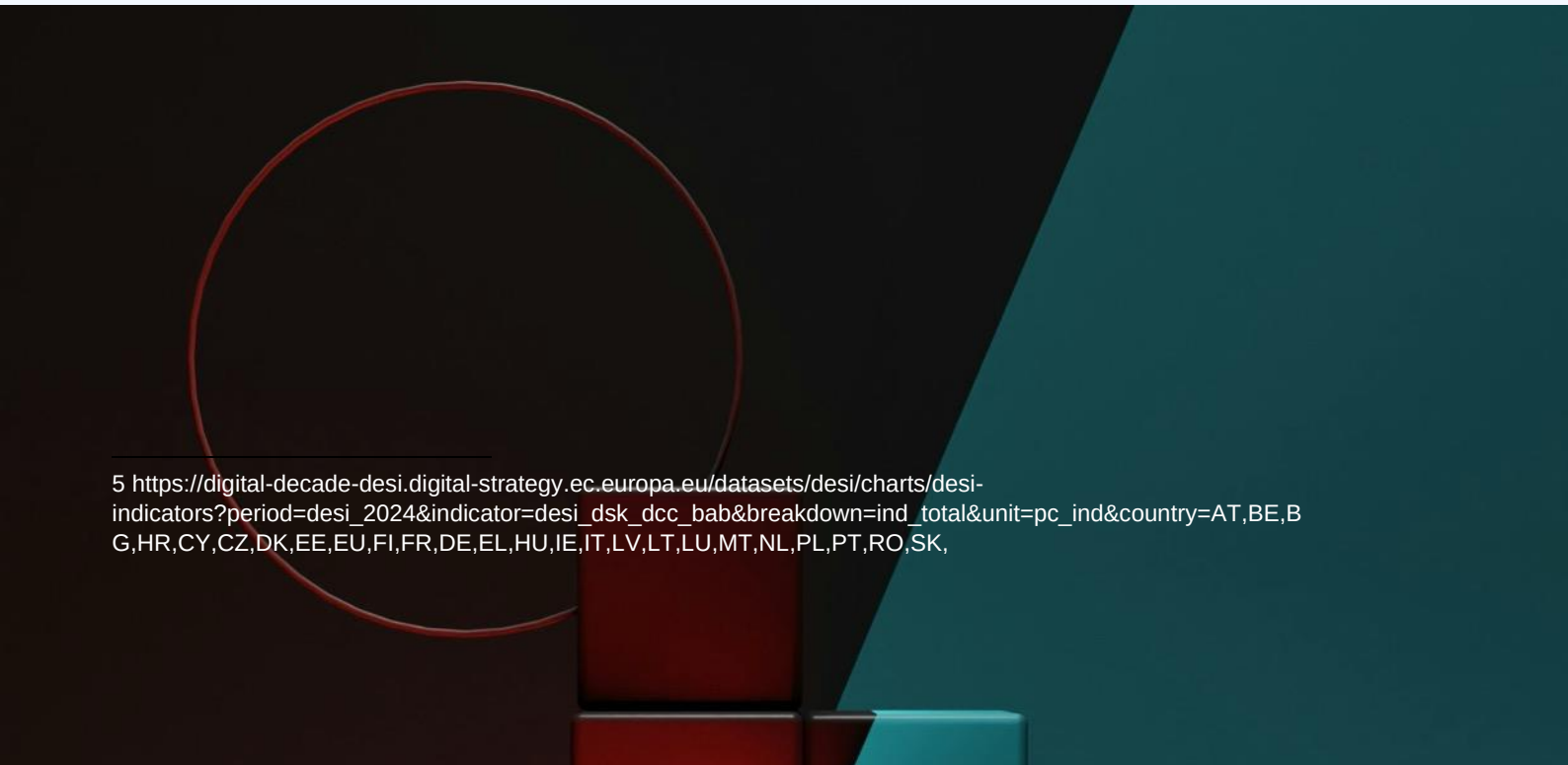
4 https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-country-reports

indicators.[5]
In 2024, Poland scored higher than the EU average in 6 out of 36 indicators: broadband connectivity, coverage of fixed very high capacity networks, coverage of FTTP (Fibre to the Premises) technology, cloud, pre-filled forms, and access to electronic medical records.

A recent report on the implementation of the 2030 Policy Programme “Path to the Digital Decade” [3] noted significant progress in the area of gigabit connectivity and digitalisation of SMEs. In the case of the very high capacity network coverage indicator, **Poland, with 81.1% of households covered, exceeds the EU average (78.8%)** and is on track to achieve 100% coverage by 2030. Although the KPIs for the digitalisation of enterprises are below the EU average, **the rate of growth of the digitalisation level of Polish SMEs between 2021 and 2023 was 5 times higher than in the EU**. According to Poland's 2024 Digital Decade Country Report, Polish SMEs have great growth potential; the authors also point out that 14% of them are involved in e-commerce. The persisting challenges in the area of digital transformation of enterprises are caused by a shortage of specialists, high costs and lack of adequate financing. The report also notes that **significant resources are dedicated to improving connectivity, enhancing enterprises’ use of digital technologies and developing digital public services** that should improve the competitiveness of the Polish economy and boost the whole society’s use of digital technology. The European Commission also noted Polish declarations regarding investments in the production of semiconductors and participation in projects to build quantum computers.

Despite positive trends, Poland is still performing unsatisfactorily in terms of digital skills and adoption of advanced technologies. Poland's result in the indicator of *at least basic digital skills* is 44%, which is below the EU average of 55.6%. Poland also scores below the EU average in indicators such as *above basic digital skills* (PL 20%, EU 27%) and at least basic digital skills in digital content creation (PL 60%, EU 68%).

The analysis of the National Action Plans carried out by the European Commission shows that in the current scenario, collective efforts fall short of the EU's level of ambition. The identified gaps include the need for additional investments, both at the EU and national level in several areas. Poland should consider aligning the level of ambition of the targets regarding the number of ICT specialists and the use of artificial intelligence and data analysis by enterprises with the EU goals.



5 https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators?period=desi_2024&indicator=desi_dsk_dcc_bab&breakdown=ind_total&unit=pc_ind&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK,

eGovernment Benchmark

The eGovernment Benchmark is an annual study monitoring the implementation of digital public services in all European countries.[6] In 2024, the Polish result rose to 69 points; countries such as the Czech Republic, Bulgaria, Greece and Croatia have similar results. The distance to the EU average is 7 points. Moreover, Poland is among the most improved EU27 countries over the past four years: +14 points.

eGovernment Benchmark 2018-2024

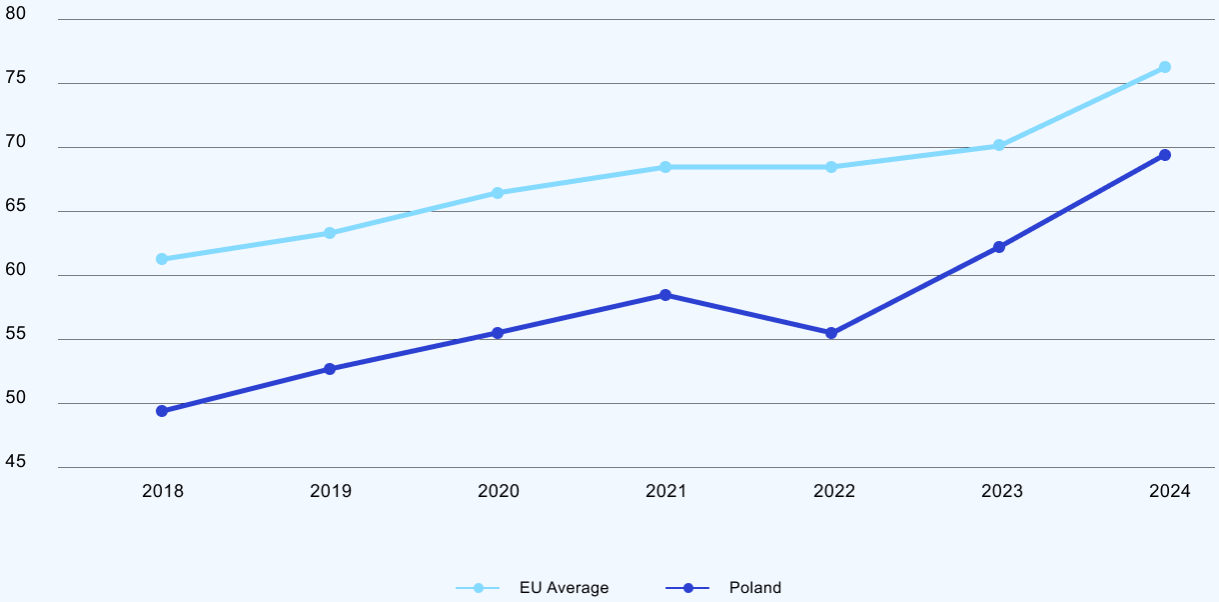


Figure 2 eGovernment Benchmark 2018-2024 results, source: own elaboration based on the results of the 2018-2024 study2

E-government indicators are concentrated around four dimensions: User Centricity, Transparency, Key Enablers and Cross-Border Services. In the 2024 report, Poland scores at or above the European average in 5 indicators: User Support, Transparency of Service Design, eID, eDocuments and Pre-Filled Forms. **The largest increases were recorded in Transparency of Personal Data, eDocuments, and Digital Post.** Poland achieved relatively highest results in the entire category concerning Cross-Border Services, as well as in the indicators of Transparency of Service Delivery, Transparency of Personal Data and Digital Post. In terms of classification in relation to life events, the largest point increase in 2024 was recorded in Justice (an increase of 27 points) and Health (an increase of 12 percentage points). Despite Poland's rising scores in every life event, there is still room for improvement, particularly in life events Justice and Transport, where scores are below the EU average.

6 https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-egovernment-benchmark

The report's conclusions suggest that a key to achieving the EU's digital transformation goals is to work towards the reduction of disparities between countries, user groups and levels of government in terms of the integration and efficiency of digital service provision. Moreover, European countries should strive to provide digital services proactively, which means that the citizen obtains the effect of the service as a result of the automatic operation of the administration.

Digital Public Administration Factsheet (DPA)

Digital Public Administration Factsheet is an EU report presenting the state of the digital transformation of public administration with particular emphasis on interoperability aspects.[7] The report is published annually and is based on data provided by EU countries, Eurostat indicators, the eGoverment Benchmark and the results obtained under the monitoring mechanism of the European Interoperability Framework (EIF).

Over the years 2018-2022, there was a gradual increase in all indicators relating to digital public administration in Poland. The largest, almost two-fold increase (from 21% in 2018 to 40% in 2022) concerned the percentage of people using the Internet to send completed forms when contacting public administration. At the same time, the lowest level was reached in the indicator of the percentage of people using the Internet to download official forms from public administration. In 2022, there was an increase of only 7 points compared to 2018, when the percentage was 20%.

7 https://joinup.ec.europa.eu/sites/default/files/inline-files/NIFO_2024%20Supporting%20Document_Poland_vFinal_rev.pdf

Interoperability principles

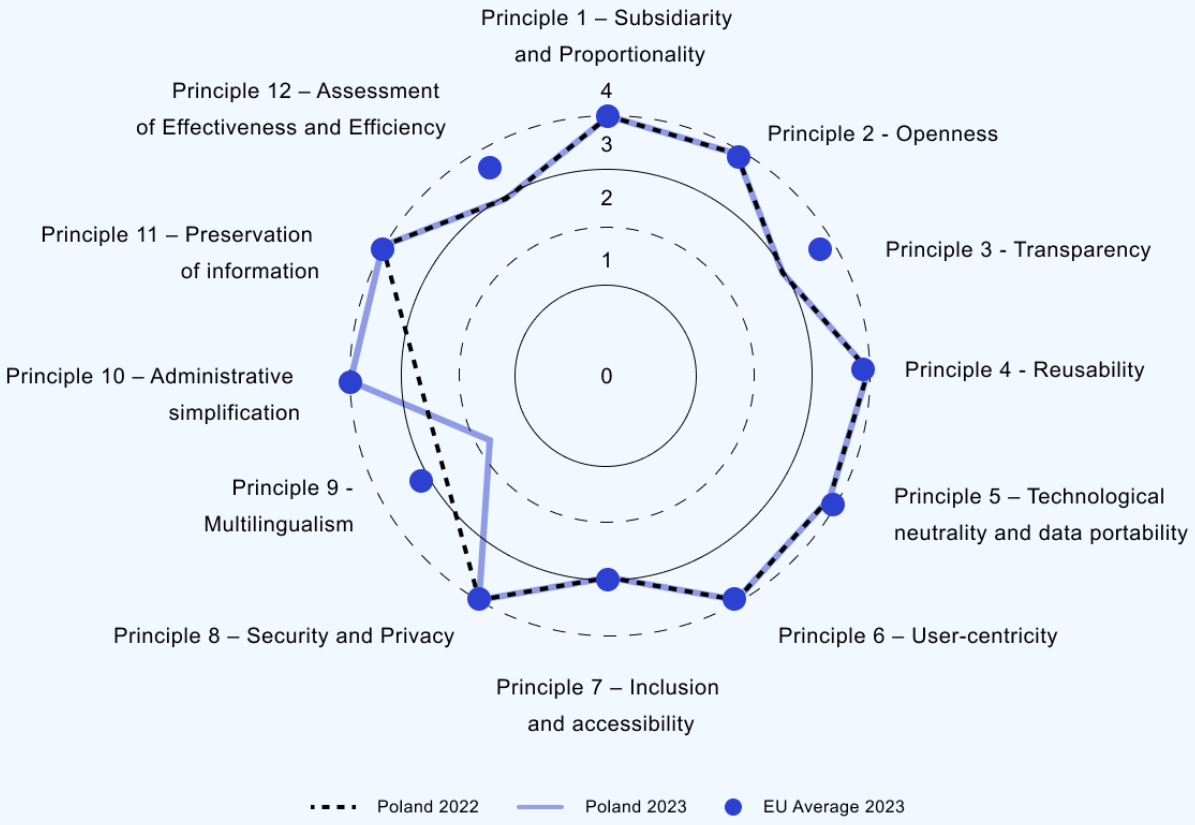


Figure 3 European Interoperability Framework, Scoreboard 1 - Interoperability Principles, *source: own elaboration based on Digital Public Administration Factsheet 2024*3

According to the Digital Public Administration Factsheet 2024 report, Poland has made significant progress in the digital transformation of public administration. The growth is evident in all areas studied. In terms of interoperability principles, Poland scores at the EU average except for Principle 3 – Transparency, Principle 9 – Multilingualism, and Principle 12 – Assessment of Effectiveness and Efficiency. The recommendations contained in the report indicate that Poland, when establishing European public services, should devote more efforts to the interoperability of ICT systems and technical infrastructure and take into account multilingualism. It should be noted that in 2023, Poland was recommended to implement new digital solutions and optimise administrative processes, and in 2024, Poland's score in Administrative simplification (Principle 10) increased to the maximum possible level.

International Interoperability

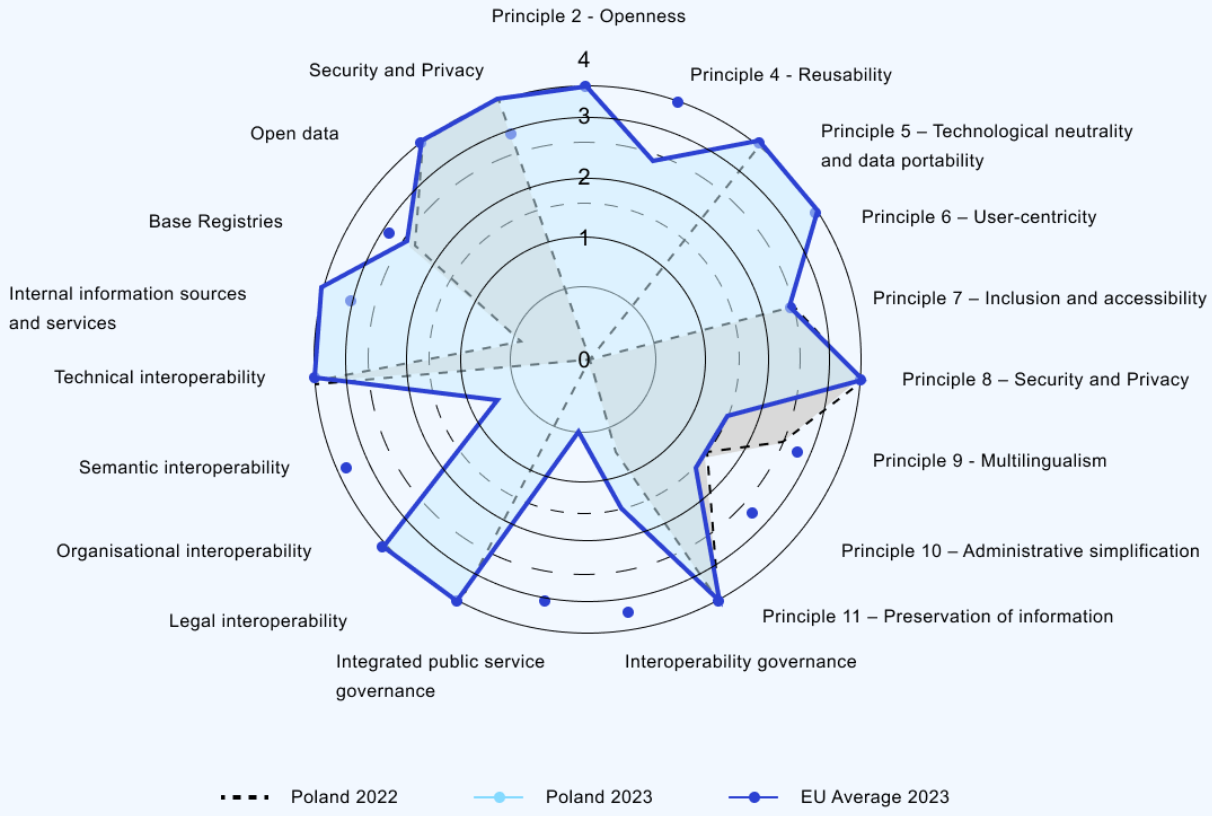


Figure 4 European Interoperability Framework, Scoreboard 4 - Cross-Border Interoperability, *source: own elaboration based on Digital Public Administration Factsheet 2024*4

In terms of cross-border interoperability, Poland should improve its results in indicators related to integrated public service governance as well as semantic interoperability, which in both cases scored below the EU average.

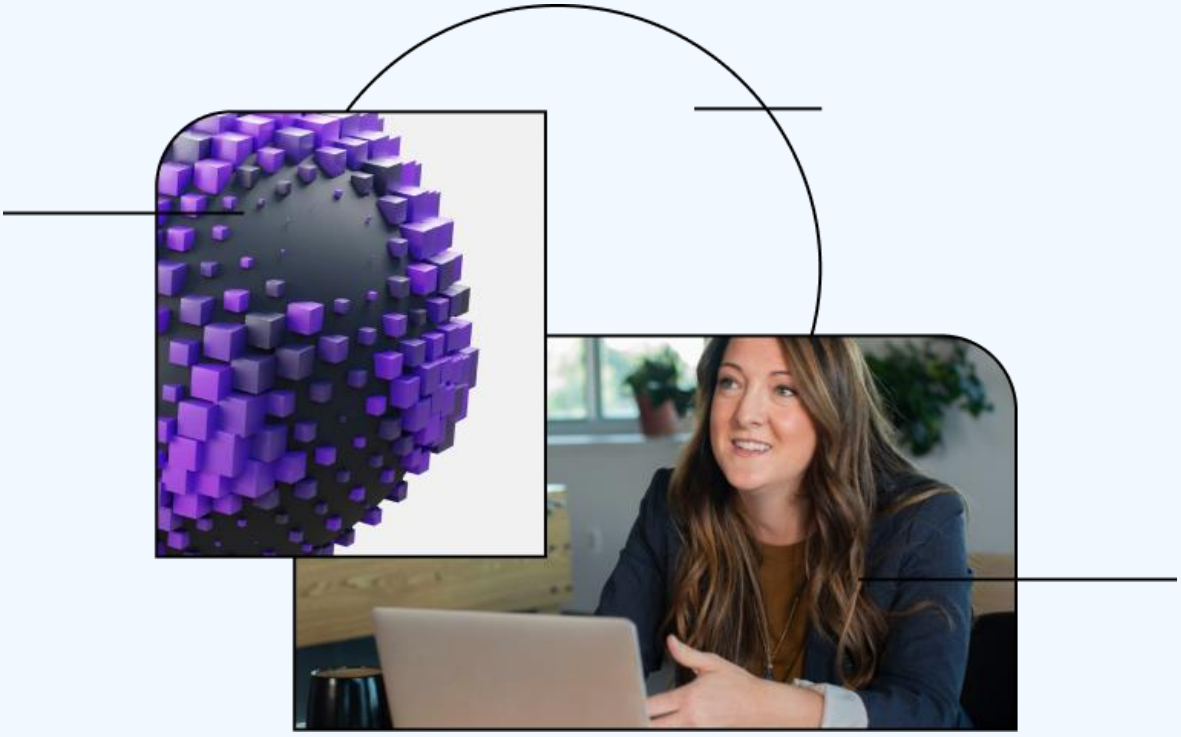
Digital Government Index (DGI)

In the 2023 OECD Digital Government Index report, assessing the progress of the digital transformation of the public sector in 2020-2022, Poland ranked 20th among the Organisation's 33 member states.[8] The result was 57.1%, with the OECD average of 60.5%. Poland achieved its best score, i.e. 11th position, in the category *Government as a platform*, which measures the deployment of common building blocks such as guidelines, tools, data, digital identity and software that will enable the transformation of processes and services across the public sector. The area in which Poland achieved the lowest score, ranking 29th, was Proactiveness, defined as the *governments' capacity to anticipate the needs of users and service providers to deliver government services proactively.*

8 https://www.oecd.org/en/publications/2023-oecd-digital-government-index_1a89ed5e-en.html

The Berlin Declaration

The Berlin Declaration on Digital Society and Value-Based Digital Government sets out several key principles and accompanying policy areas to ensure that the digital transformation aligns with common European fundamental rights and values. Report on the monitoring of the Berlin Declaration is a tool documenting progress in implementing actions under the declaration for signatory states.[9] The monitoring mechanism is based on key performance indicators, the evaluation of which uses data provided by Member States, eGovernment Benchmark, EIF, and DESI.



9 https://joinup.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf

Level of Policy Area Implementation

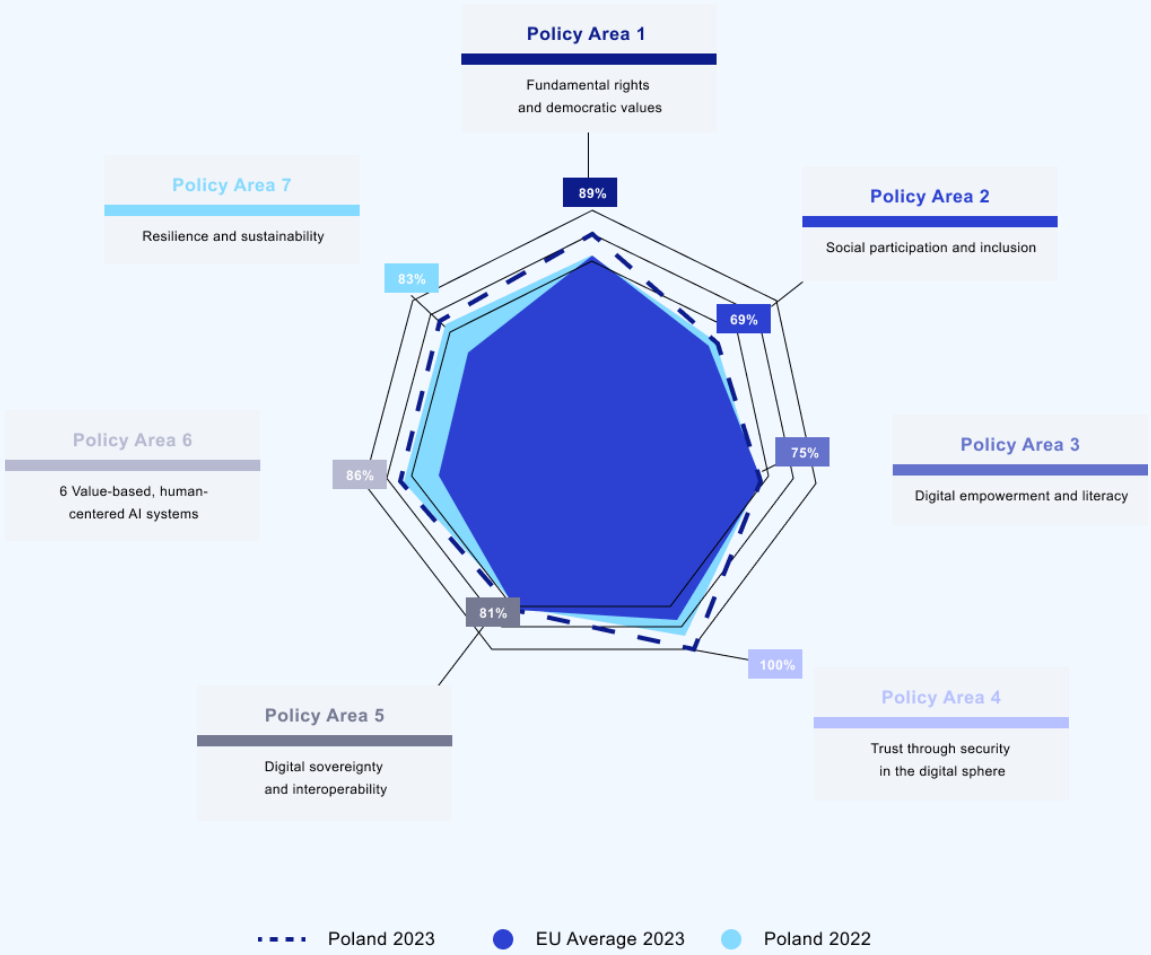


Figure 5 2023 Berlin Declaration Monitoring, Policy Areas level of implementation - Poland compared to the EU average, source: own elaboration based on the Report on the monitoring of the Berlin Declaration 2024[5]

In the report issued in 2024, it was noted that, overall, Poland's scores have shown stability and minor fluctuations compared to those of last year's summary. **The most significant increase, by 9 points, was recorded in Policy Area 1: Fundamental rights and democratic values.** This was followed by Policy Area 4: Trust through security in the digital sphere, which saw an increase of 4 points. A slight decrease of 2 points was recorded in Policy Area 2: Social participation and inclusion. Poland scored above the EU average in four out of the seven Policy Areas. **The biggest difference, by 13 points, was recorded in Policy Area 6: Value-based, human-centred AI systems for use in the public sector.** It was followed by a difference of 10 and 9 points, respectively, in Policy Area 4 and Policy Area 7: Foster resilience and sustainability in the digital society The areas in which Poland falls below the EU average are Policy Area 3: Digital empowerment and literacy, with a difference of 6 points, and Policy Area 5: Digital sovereignty and interoperability, with a difference of 4 points.

Poland stood out against the European Union in Policy Area 7: Resilience and sustainability with its initiatives for the development of digital health services, such as Patient Internet Account, the mojeIKP app, e-prescription and the launch of a chatbot on the patient.gov.pl website informing patients about e-services in the healthcare system. **In Policy Area 4:**

Trust through security in the digital sphere, the development of the mObywatel mobile app was rated well, and in Policy Area 6: Value-based, human-centred AI systems, effective coordination of activities related to the development of the Polish AI ecosystem (including strategic activities in the Committee of the Council of Minister for Digital Affairs).

Special Eurobarometer: The Digital Decade

To support the monitoring of the 2030 Policy Programme “Path to the Digital Decade” and the objectives of the European Declaration on Digital Rights and Principles, a study was commissioned by the European Commission to examine whether and to what extent the attitudes of European Union citizens towards digital technologies are evolving. The findings of the report, issued in 2024[1], show that almost three-quarters of Europeans (73%) consider that the digitalisation of daily public and private services is making their life easier, including 19% who say it is making their life “much easier”. Just under one in four respondents (23%) say that the digitalisation of daily public and private services is making their life more difficult.

The results show that in general, Poles' attitudes and perceptions of digital technologies are positive and rated at the same level or higher than the EU average. In terms of perceptions about the future of digital technologies, as many as 80% (+3 points compared to 2023) of Poles think that by 2030 digital technologies will be important in accessing or receiving healthcare services. The same view is held by 79% of EU citizens. Compared to 73% of Europeans, up to **81% of Poles think that the digitalisation of daily public and private services is making their life easier.**

How well do you think the EU protects your rights in the digital environment?

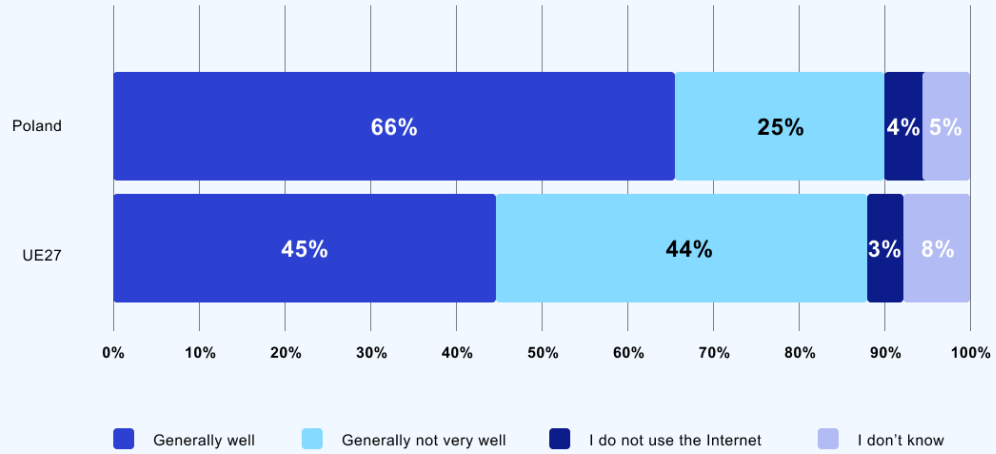
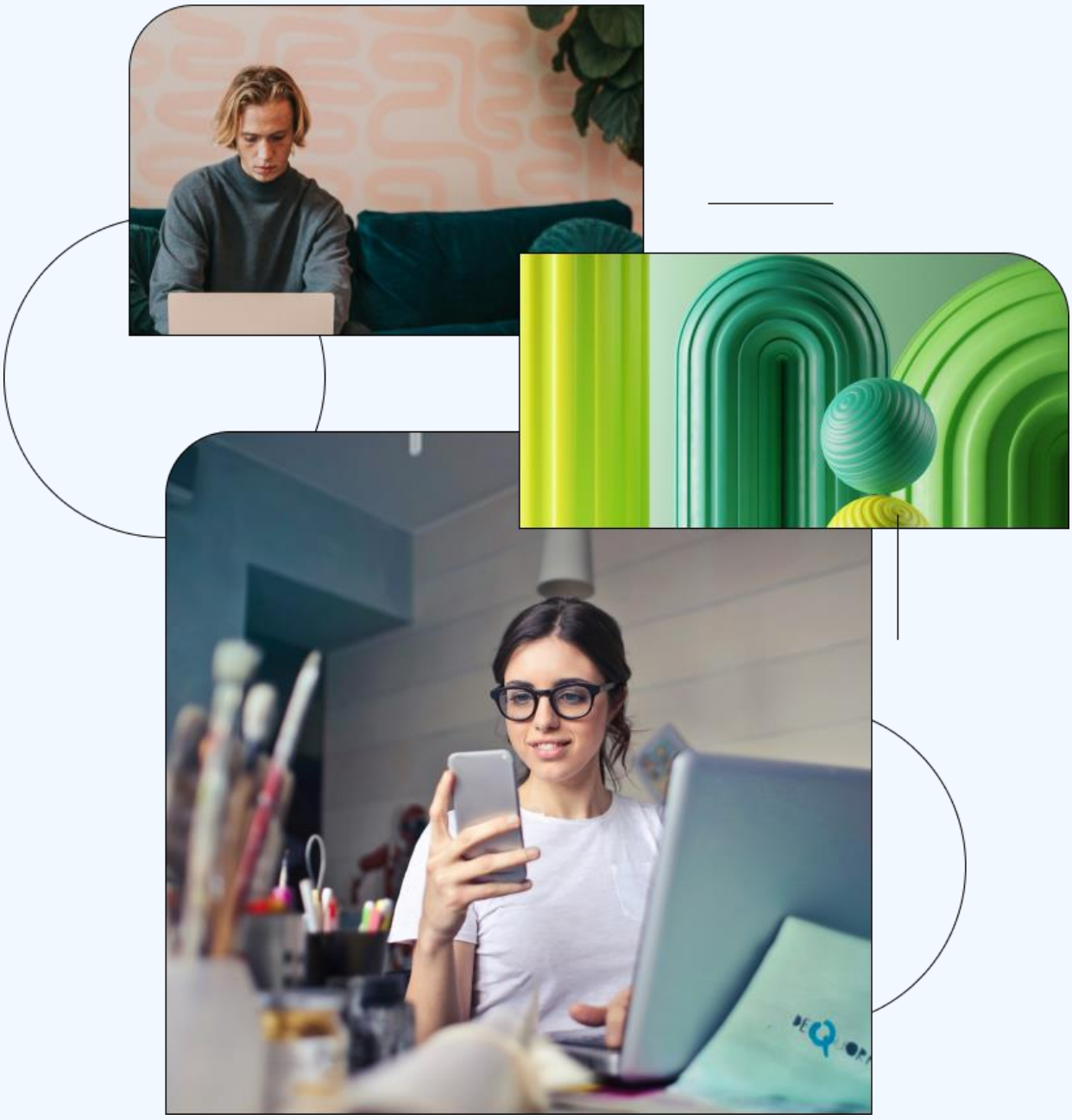


Figure 6 Special Eurobarometer 551, question QC7, source: own elaboration based on the Fact Sheet for Poland.6

Only 45% of EU citizens believe that the EU protects their rights well in the digital environment, while the same opinion is shared by 66% of Polish citizens. In terms of the perception of the application of digital principles in the country, **the lowest score concerns ensuring safe digital environments and content for children and young people. As**

many as 59% of Poles believe that they are applied generally well, while 33% believe that they are not applied very well overall (EU average 39% - generally well, 53% - generally not very well).



Challenges and trends

Ministry of Digital Affairs
Republic of Poland

We Make the Future

Challenges and trends

Over the past several years – partly due to the pandemic – Poland has seen significant development in the field of digitalisation, quickly catching up with EU leaders. Progress was particularly noticeable in the areas of digital public services and open data. On the other hand, in many areas, the gap to the leaders remains significant, especially with regard to the digital competences of citizens and the use of digital technologies in enterprises.

When planning the country's digital development for the coming years, however, we have to go beyond analysing Poland's position in international indicators. It is necessary to analyse and prepare responses to key trends and challenges, including:

Multipolarisation of the world.

The growing rivalry between great powers translates into the area of technology. Key technologies such as semiconductors, 5G, AI, and quantum technologies have become the subject of contemporary rivalry. Moreover, powers compete with each other for resources for their development – data and critical raw materials. Due to the pandemic, shrinking resources and economic instability, existing global supply chains are becoming significantly shorter, which presents both a challenge and an opportunity for Poland.

Emphasis on technological sovereignty.

The growing rivalry translates into a drive to restore EU and domestic production of key technological components and simplify supply chains. Technological sovereignty is important for further development, including maintaining production capacities in the EU. However, the EU's technological sovereignty has been accompanied by deepening cooperation with non-European countries with similar (like-minded) values and a philosophy of digital development. There is a noticeable technological and regulatory convergence between those centres in the world.

Splinternet.

The above phenomena are accompanied by the phenomenon of splinternet, i.e. the fragmentation of the open internet into fragmented networks under the control of governments or corporations. Such phenomena are negative in nature and undermine the social and economic foundations of the Internet. From a global perspective, a differentiated approach to digital regulation, taking into account different sensitivities without, however, violating fundamental rights and freedoms, is an important factor.

The growing importance of cybersecurity.

The intensification of international competition (also in the area of technology) translates into the need to pay more attention to the problem of cybersecurity, especially in relation to critical sectors. This issue is also of growing importance for citizens and institutions, increasingly exposed to cyberattacks and falling victim to the professionalisation of cybercriminal groups.

Hyperconnectivity,

both in relation to human interaction via information and communication technologies (ICT) and to human-machine and machine-machine interaction (Internet of Things). This trend directly translates into the growing importance of data and the load on telecommunications networks.

Distortion of Competition

against the dominance of large technology platforms whose market power reduces the scope of government control and poses a significant challenge from a regulatory perspective. It is exacerbated by the fact that many of the most important platforms (social or commercial) are of non-EU origin. The state must be committed to ensuring a level playing field for all market participants.

Rising psychosocial costs associated with the digital sphere.

Business models based on making users dependent on content and tracking algorithms, the propagation of unrealistic beauty standards, minors‘ access to harmful content, hateful content, widespread misinformation - all of these factors have a negative impact on children's and adults’ mental health, the weakening of social ties or the polarisation of public debate and they require a comprehensive response.

“Twin transformation”,

i.e. direct linking of digital transformation with energy transformation, also in terms of investment decisions. There is a growing awareness of the need to seek synergies between these processes – using green energy to meet the growing needs related to the ICT creation and use, while at the same time building green energy on digital technologies.

Spread and rapid development of artificial intelligence (AI),

which may become the foundation of changes in the digital sector in the coming years. The implementation of AI means new opportunities, including in the areas of research, content creation and services, but it is also associated with threats that require a coordinated response from state institutions.

The remoteness of digital infrastructure and services from the user.

The flexibility and scalability of cloud solutions mean that data is increasingly stored and operated in the cloud rather than using local infrastructure. The popularity of solutions delivered in a subscription model – infrastructure, platforms or services – is growing.

Automation and robotisation of the economy,

being the result of the drive to make businesses more efficient and the difficulties in finding suitably qualified employees.

The rapid ageing of Polish society,

which is a burden on the social benefits system and a challenge from the perspective of the need to develop the silver economy. It will translate into the need to increase the use of technology in the economy and to adapt the system of developing competencies of the future to the changed demographic structure.

Unfinished process of creating a single EU digital market

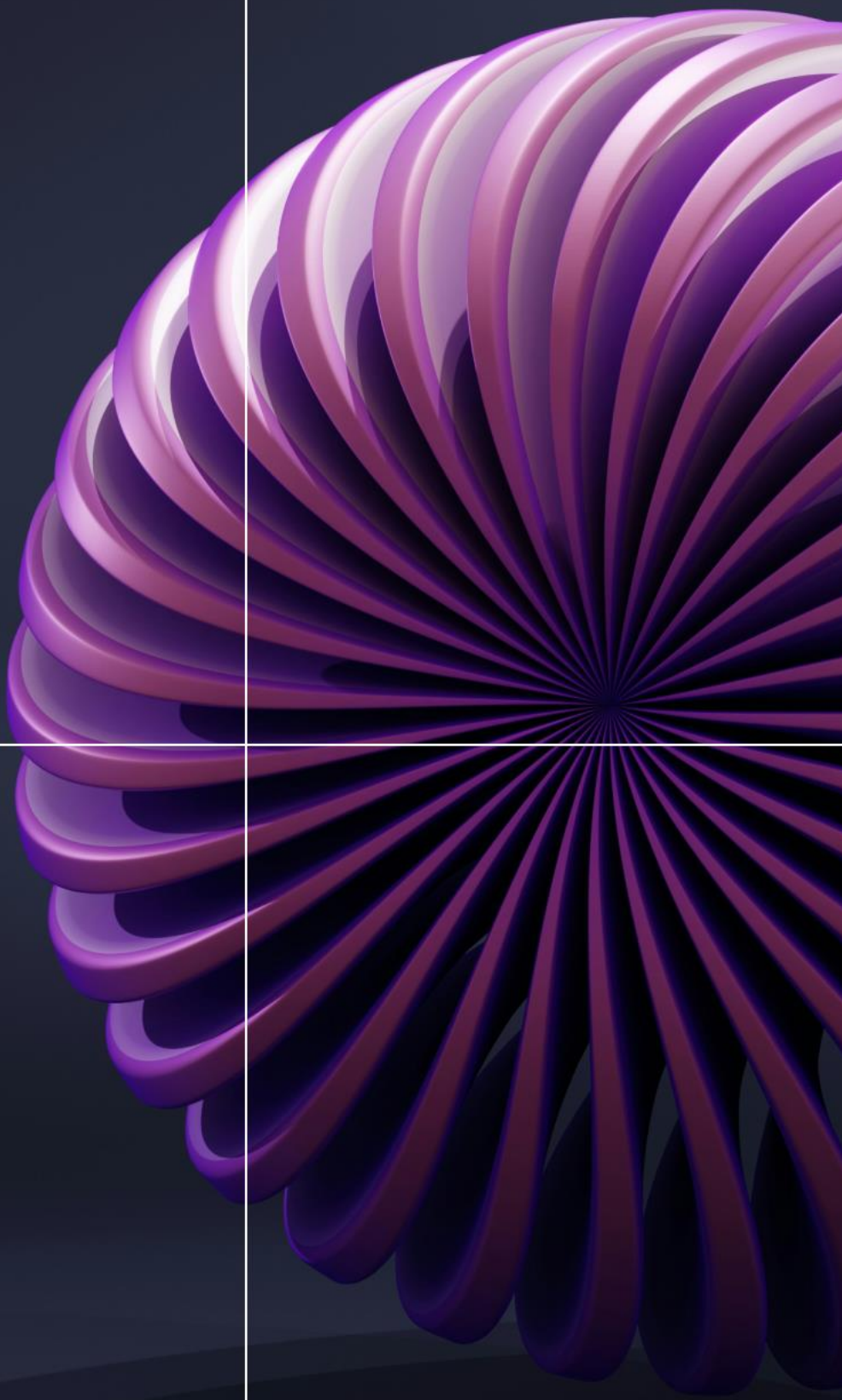
and difficulties with access to capital (including venture capital), which makes it difficult to scale ICT businesses.

Most of the trends and challenges mentioned have a global or at least EU dimension. However, the effective design of Poland's digital development must also take into account national and regional challenges and specificities. The pace of technological development also demands that such analysis is not incidental to the creation of successive strategies, but ongoing. Thus, a systemic deepening of knowledge and its inter-institutional exchange is necessary, without which it will be significantly more difficult to properly allocate limited resources and achieve a multiplier effect, or to introduce technical and legislative solutions that enable the deepening of cooperation throughout the administration.

The Polish administration must also have the ability to independently analyse market and technological trends to distinguish those that have a real impact on the economy and society from those that are primarily temporary media trends.

Effective implementation of conclusions from such analyses will require strengthening the digital competences of officials and training staff in the field of public policies related to digitalisation. It will not be possible without the coherence of Polish digital development processes. Due to the horizontal nature of digitalisation, the silo structure that is still a problem for the administration is particularly pernicious in this area. It is necessary to build awareness of the need for close cooperation between institutions responsible for building a digital state, including those from sectors sharing a ‘common border’ with digitalisation in the strict sense.

SWOT analysis



Ministry of Digital Affairs
Republic of Poland

We Make the Future

SWOT analysis

To set priorities in the area of state digitalisation for the next decade, it was necessary to conduct an in-depth analysis of the situation within the scope of competences of individual ministries, as well as the state as a whole. The diagnostic materials obtained from the ministries were supplemented with an analysis of strengths, weaknesses, opportunities and threats to the digitalisation of Poland, which was carried out by the Polish Economic Institute (PIE) on behalf of the Ministry of Digital Affairs (MC). PIE conducted a SWOT analysis for five areas closely related to MC's activities:

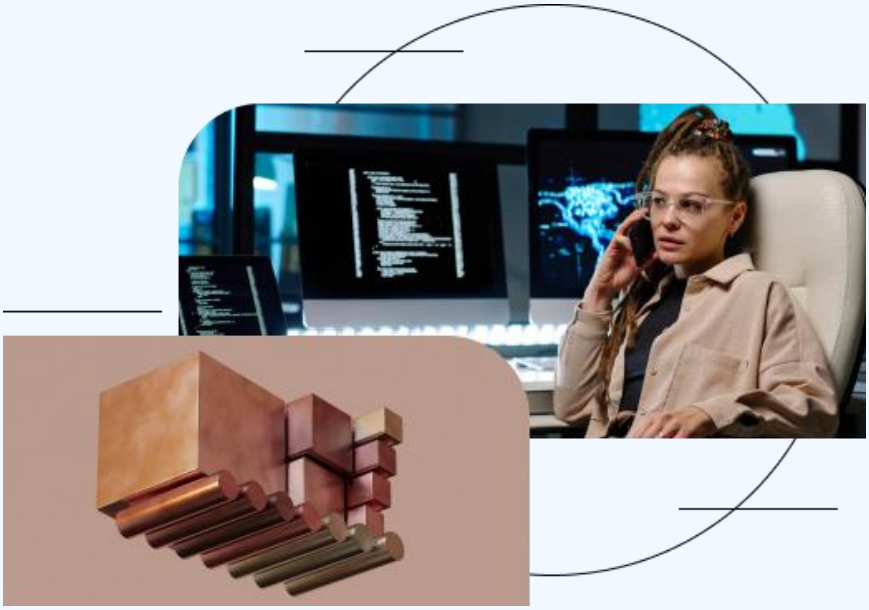
digital state;

competencies of the future;

infrastructure;

digital economy;

cybersecurity.



Digital state

When it comes to the development of public (and private) digital services, Poland is doing relatively well. Despite the low position in the DESI rankings, the gap to the leaders is smaller than in other areas, and some national solutions (e.g. mObywatel) are a good example for other countries. Since public trust in the technologies used is crucial for the development of digital services, it should be emphasised that there have been no major incidents violating that trust in recent years. According to PIE's study, Polish women and men have a positive attitude towards e-services, including the use of AI in public services. As many as 92.5% of respondents declare that digital public services are making it easier for them to run administrative errands. As many as 66.7% of respondents believe that the state should make greater investments in digital public services, but only 27.2% are ready to finance such investments through tax increases.

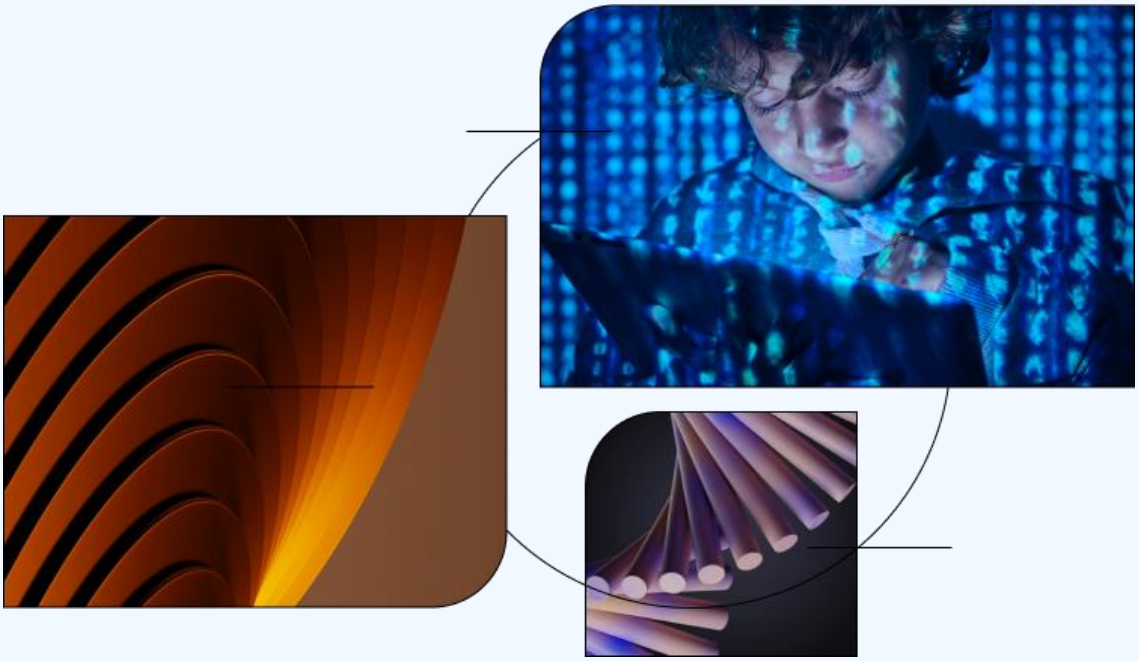
A significant difficulty is the significant dispersion of the services being created, including the duplication of ordered solutions at the local level. This suggests poor coordination of activities in this area. At the same time, many services have deficiencies at the UX (user experience) level, while in other centres there is a strong emphasis on this aspect - there are no developed standards or best practice flows. Another important challenge is the digitalisation carried out by local governments. At this level, there is often a lack of competences required to introduce digital services; there are difficulties in ensuring systems maintenance (due to an even more acute shortage of ICT specialists than at the central level); and there are fears of permanent job losses due to automation.

Strengths	Weaknesses
• A wide range of digital public services; • Access to structural funds; • Existing, well-functioning solutions (mObywatel, e-PIT); • Openness to change and application of new solutions.	• Technological debt (persistent old systems in administration); • Lack of competences and concerns in the administration, especially on the part of local governments; • Low level of trust in the state; • Uncompetitive salaries for ICT specialists in public administration. • Lack of full interoperability of systems and registers used in public administration.
Opportunities	**Threats**
• Positive public attitude towards digital public services and the use of AI in administration; • Partnership with businesses and use of the best market solutions; • Development of the local ICT market.	• Dependence on solutions provided by external suppliers; • Overlapping of different mechanisms and time perspectives in strategic documents; • Silo structure in public administration – lack of coordination of activities and common standards. • Geopolitical rivalry and the threat of hitting a nerve in the country's digital infrastructure; • Rapidly changing technological environment; separation of the private sector from the public sector in terms of technologies used.

Competencies of the future;

Nowadays, digital competences are necessary for personal development, social and civic activity, as well as functioning in the labour market. Although the development of those competencies in recent years has been supported by many initiatives, the gap to the EU average remains significant – only 44% of Polish citizens have at least basic digital skills, compared to the EU average of 56%. Strengths are limited, and some experts point to the persistence of the same barriers and challenges in the field of digital competences over many years. The Digital Competence Development Programme was supposed to be the answer to the problems diagnosed in this area. It took over 4 years to develop and adopt it, so the results are still to be seen.

The coming years will bring significant demographic challenges as well as a worrying trend of a decreasing percentage of STEM (science, technology, engineering, mathematics) graduates (on the other hand, there are more and more ICT graduates). Other factors also have an unfavourable impact, e.g. the low level of digitalisation of companies. On the other hand, the easy availability of examples of good practices adopted by other countries and the high level of expertise gained, among others, in social organisations involved in the development of digital competences in Poland, should be seen as an undoubted opportunity.



Strengths	Weaknesses
• High level of technical education at universities; • Relatively high (compared to Central and Eastern Europe) level of digitalisation in schools, including broadband equipment; • High level of expertise gained, among others, in institutions involved in the development of digital competences in Poland, should be seen as an undoubted opportunity.	• Low level of digital literacy among citizens in all age categories, even among the so-called digital natives - young people aged 16-19; • Relatively small number of ICT specialists and participation of women in ICT professions; • Insufficient quality of digital education. • Percentage of STEM graduates below the EU average; • Low educational activity of adults in Poland compared to other EU countries; • Too little emphasis on developing the soft skills of the future.
Opportunities	**Threats**
• Increased awareness among decision-makers and in society of the importance of digital competences for the quality of life of citizens and the condition of the economy; • Availability of examples of good practices applied by other countries.	• A rapidly changing range of digital competences that need to be replenished throughout life; • Ageing society and digital exclusion of elderly citizens; • Talent draining; • Lack of stability in support for the development of digital competences; • Mental health crisis and other risks associated with exposure to electronic media.

Infrastructure

Telecommunications infrastructure is an example of successful EU spending and regulation. Poland has wide access to modern networks and an extremely competitive market, providing very good conditions for consumers. However, new challenges are emerging - the potential use of alternative access technologies (due to the very high costs of covering the entire country with fibre optics); the need to stimulate demand for Internet access and ensure network maintenance in the face of rising costs; the creation of new ‘infrastructures’ - the cloud, quantum computers or private networks in enterprises.

An opportunity to increase investment funds and expand the operational range of telecom operators (who for years have been complaining about declining revenue) lies in the trend of separating infrastructure from services (which in Poland is visible in both mobile and fixed networks). However, telecoms have limited ability to enter new business areas and the low level of digitalisation of companies is not conducive to expansion in this direction. The risk also comes from the increasingly popular thesis of the need to agree on the consolidation of telecom operators in the EU - for the Polish market this could rather entail an increase in prices, with a doubtful positive impact on the quality of the available infrastructure.

Strengths	Weaknesses
• High competition and good offer for consumers; • Relatively wide access to optical fibres and good coverage of mobile services; • Significant public funds and extensive experience in managing them.	• Limited innovation of telecoms; • Delayed frequency procedures for 5G networks.
Opportunities	**Threats**
• The trend of separating infrastructure from services; • Satellite access with increasingly higher bit rates; • Development of new business models by telecoms; • Planned actions to stimulate demand for high bandwidth connectivity.	• Uneven access to infrastructure; • Failure to consider alternative technologies when providing access; • Low demand for the highest bandwidth connectivity; • Lack of participation in international 5G implementation projects; • A pervasive narrative about the need to consolidate the telecommunications market.

Cybersecurity

The area of cybersecurity is interconnected with all other areas, and the strengths, weaknesses, opportunities and threats interact with those identified in other sections. Poland has a significant supply of human capital – namely experts in institutions ensuring cybersecurity at the national level and startups dealing with cybersecurity. At the same time, however, a low level of digital competences (also among enterprises) may translate into increasing risks and a large number of "weak links". In many respects, the international dimension is key to cybersecurity. The proximity of a full-scale war in Ukraine and the aggressive stance of Russia and other international actors increases the number of cyberattacks, but at the same time, it allows competence to be developed when confronted with a real threat. The growing market - both in terms of domestic companies and the presence of global giants that allow benefitting from their knowledge, experience and infrastructure - is also a favourable factor for increasing the level of cyber security. Coordination of activities in the area of cybersecurity may be hindered by the dispersion of institutions responsible for it and the lack of a “one-stop shop" for the national cybersecurity system (KSC) entities and citizens. Legal issues, by contrast, present both a problem and an opportunity – on the one hand, delays in the creation of certain pieces of legislation and their increasing number complicate the legal system, but on the other hand, there is still the possibility of adopting good legislation and broadening the debate at European level.

Strengths	Weaknesses
• National CSIRTs (Computer Security Incident Response Teams) and other institutions responsible for ensuring cybersecurity at the national level; • A large number of specialists in the public and private sectors; • Initiatives to enhance cybersecurity at the national level (including AntiDDoS, ARAKIS-GOV, ARTEMIS, SKR-Z, S46, CTI); • A large number of study majors related to cybersecurity; • NATO membership (allied cooperation and collective defence) and EU membership (cooperation mechanisms and regulations).	• Low utilisation of cloud computing; • Low level of digital skills, competence gaps in public administration; • Low awareness of threats in society and administration; • Dispersion of institutions responsible for cybersecurity; • Proximity to a full-scale war in Ukraine, exposure to cyberattacks from the Russian Federation; • IT personnel shortages among SMEs.
Opportunities	**Threats**
• Growing awareness of data protection and privacy; • The growing importance of security in discussions about the direction of development, translating into opportunities for funding increase.	• Popularisation of smart devices (IoT – Internet of Things) and the development of Industry 4.0; • Popularisation of remote work; • Using generative AI for malicious activity in cyberspace; • The development of quantum technologies as a threat to information security; • Growing geopolitical rivalry; • Increase in the number of cyberattacks; • Difficulties in retaining specialists in the public sector; • Low priority for cybersecurity in Polish companies and administration.

Digital economy

In Poland, there is still significant space for the digitalisation of companies, automation and robotisation of production. Robotisation is at a low level compared to the countries of the region, and even more so compared to the European leaders. It seems, however, that demographic, regulatory (including the increase in the minimum wage) and market trends may accelerate changes in this area in Poland. A strength is the presence of cloud regions of the largest global cloud providers – and therefore their direct involvement in the development of the digital economy. Difficulties, on the other hand, include mental barriers (i.e. lack of motivation of entrepreneurs to implement new solutions – definitely more difficult to overcome than, for example, financial barriers), the "medium-sized country trap" (domestic market large enough to maintain the company, lack of external incentives for development) and, finally, insufficient availability of domestic capital (a barrier going beyond the digital sphere). Another risk, also going beyond the digital sphere, is the structure of the economy, with a large surplus of micro and small businesses (most likely regardless of the large percentage of falsely self-employed).

As a result, a dual economy may emerge, in which companies with foreign capital, integrated into global supply chains or exporters, use modern technological and digital solutions, while the other part is left behind. Such a threat is suggested by the development indicators of the ICT sector, also in relation to the flagship Polish export area – the gamedev industry (game development). They show a very low number of ICT specialists across the economy, indicating a low priority for digitalisation in most companies.

Demographic trends are also an important context for the future of the Polish digital economy. Already in 2023, 25 per cent of the working population (aged 18-64) were people aged 50 or over.[10] As shown by PIE's analysis, by 2035 the Polish labour market will shrink by 2.1 million workers, which represents 12.6% of the current employment. The most serious consequences of demographic changes will affect the education sector (reduction of the employee base by up to 29%) and healthcare (reduction by up to 23%). Industrial sectors (B-E sections) may lose up to 400,000 employees by 2035 (a decrease of 11%).

One of the potential solutions to mitigate the negative effects of the decline in labour supply is the use of modern technologies. Automation, the use of industrial robots, RPA (Robotic Process Automation) systems and artificial intelligence can support human work, increase its efficiency or even fully replace it.[11] Such solutions can automate some jobs or reduce the demand for work in sectors that struggle with labour shortages – those where this will not result in excessive negative social costs.

Despite the currently low level of adoption of new technologies in Poland, it can be assumed that the decreasing supply of workers and the consequent increase in labour costs will translate into the need for innovative investments in automation in Polish enterprises.[12] There is still great potential for automation in the Polish industry, as the current robotisation density

10 https://pie.net.pl/wp-content/uploads/2024/10/Podaz-pracy.pdf

11 https://pie.net.pl/wp-content/uploads/2024/10/Podaz-pracy.pdf

12 https://pie.net.pl/wp-content/uploads/2024/10/Podaz-pracy.pdf

is among the lowest in the European Union.[13] Also, artificial intelligence, as a technology that is both complementary and substitutive for highly skilled workers, offers great potential for taking over some tasks from humans while increasing the efficiency of performing other tasks, which may help offset the negative effects of demographic change.[14]

13 https://pie.net.pl/wp-content/uploads/2024/07/Robotyzacja-w-Polsce-w-2023.pdf

14 https://www.whitehouse.gov/wp-content/uploads/2024/03/ERP-2024.pdf

Strengths	Weaknesses
• Availability of technologies from the largest global players; • High ICT exports (services in particular); • Relatively high expenditures of Polish large companies on RD.	• Relatively low level of robotisation; • Lack of industrial strategy; • Low level of digital competence; • Low motivation of employers to implement innovative/digital solutions; • Low percentage of ICT specialists employed in the economy; • Low availability of domestic capital; • Low innovation of the economy.
Opportunities	**Threats**
• Raising the minimum wage as a potential driver for automation/digitalisation; • Rapid pace of economic development.	• Lack of a strong startup investment ecosystem; • Small inflow of ICT specialists relative to needs; • High costs of employing ICT specialists; • "Digital gap" among entrepreneurs - a group of automated companies, mostly large ones, exporting, owned by foreign companies

Goals and factors that enable their achievement

The conditions outlined above – alongside the experience of the Ministry of Digital Affairs to date, recommendations from numerous reports from the administration and market and advisory bodies, as well as the evaluation of the implementation of the strategic documents in effect to date – have guided us in developing the assumptions of the following strategy.

Given the horizontal nature of digitalisation processes and their strong impact on many aspects of human life, we consider the main goal of this strategy to be improving the quality of life through digitalisation.

To achieve this goal, it is necessary to meet several conditions, starting with ensuring appropriate legislation and **security in the digital sphere**, **supporting citizens in developing the competences** necessary to navigate in the digital world and **guaranteeing appropriate quality of access to networks and services**. Ensuring security and developing competences and connectivity should be considered both important strategic goals and fundamental factors that enable society to benefit from emerging digital technologies.

We also consider the **development of the Polish digital economy** (as well as the use of digital technologies to develop other industries) and its competitiveness, **building administrative efficiency based on technologies** and **securing the rights of Polish citizens in the digital domain** to be key priorities.

For the above goals and conditions to be effectively achieved, it is necessary to:

a) **Increase the coordination of work between public administration entities** – both at the central and local level – as well as the support from other public institutions. The lack of a single centre responsible for the digitalisation of the country in all areas requires improved coordination mechanisms between various entities operating in this field. Navigation in the rapidly changing sphere of technology also requires increasing the flexibility of the state's operation in that area.

b) **Allocate sufficient financial, human and organisational resources** to the development of a digital state, society and data-based economy. Investments in the digital sphere – ensuring cybersecurity, modernising administrative processes, streamlining e-services, increasing the number of implementations based on artificial intelligence or supporting the creation of innovations – are crucial, but they are costly and require the involvement of appropriately remunerated and competent staff.

c) **Make long-term plans for the country's digital development.** Although it is often impossible to precisely predict the direction of technological development, it is important to increase the analytical competences of the centres responsible for creating digital policy in Poland – this will make it possible to identify trends at an early stage, the inclusion of which may be beneficial for the country. It is also necessary to ensure the technological neutrality of solutions used by the state, which will help avoid long-term dependence on a single supplier.

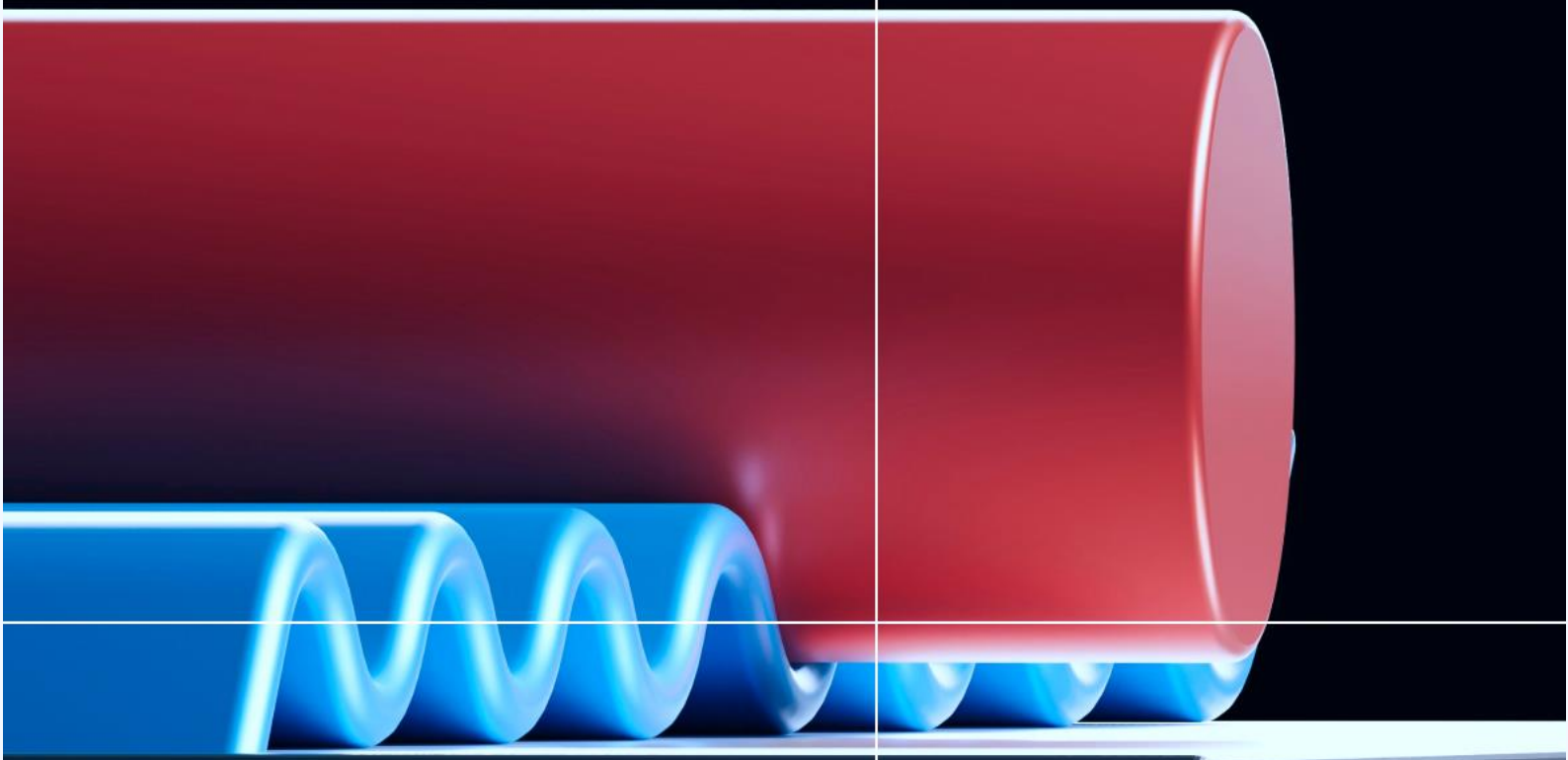
d) **Support equitable digital transformation** that will ensure sustainable development and increased competitiveness of the economy (also in connection with the energy transformation and workers' rights), social inclusion, digital accessibility for people with disabilities and the implementation of digital rights and principles which are included, among others, in the European Declaration on Digital Rights and Principles in the Digital Decade. A properly designed digital transformation must include, among other things, links to the energy transformation, guarantees of workers' rights and support for the retraining of people whose jobs are threatened by technological change.

e) **Design digital transformations in the spirit of technorealism** – recognising that technological development is not the solution to all problems. Although it has the potential to truly improve the quality of life, it is also associated with threats which must be responded to and prevented by the state.

f) Assume that the introduction of new digital solutions **must never be at the expense of security**, both in terms of cybersecurity and in terms of citizens' fundamental rights, psychological well-being and social cohesion.

g) **Ensure partnership-based international cooperation as well as cooperation between the state and business.** The digital economy is global, and a significant part of Polish digital law originates from the European Union. Therefore, without good international cooperation, the development of the digital state will encounter significant obstacles. It is also necessary to ensure fair and partnership-based relations with companies in the ICT sector. Relationships with the largest global technology companies deserve special attention. Although functioning without their products is often impossible, at the same time they must honestly contribute to the development of the state, also in the area of taxes.

To systematise the directions of intervention, 4 horizontal areas have been identified which, due to their rank and importance, significantly influence the effectiveness of activities in other areas and constitute a starting point for the digital transformation of many areas of socio-economic life. Those are: electronic communications, competencies of the future, cybersecurity and coordination of digital transformation.



Horizontal areas

Ministry of Digital Affairs
Republic of Poland

We Make the Future

Horizontal areas

1.1 Electronic Communication

Diagnosis – what is it like?

In Poland, still approx. 24% of households have access to a network with a capacity below 100 Mb/s, which cannot be upgraded to a gigabit capacity. Meanwhile, 5G services are available only in 54% of the country and cover 82% of households. At the same time, as the quality of e-communication services and their accessibility continues to improve, it is becoming increasingly challenging to stimulate demand for internet use - at the end of 2023, only 65.5% of households subscribed to a fixed internet access service.

Providing universal access to very fast Internet for all citizens is one of the determinants of the digital revolution.

It enables the construction of the digital capital of society, the dissemination of digital qualifications, the support of digital competences among children and young people in the education process, and the dissemination of digital public services. This process cannot take place without ensuring a secure, efficient and sustainable digital infrastructure. In this respect, the gradual elimination of the so-called white spots for next-generation access (NGA) networks is becoming an increasing challenge due to the need for investments to reach the most difficult – in terms of accessibility, topography and population density – address points, which generate the need for significant financial outlays. Due to the potentially low profitability for telecommunications entrepreneurs, investments in those areas must be financed primarily from public sources.

Satellite technologies can be used to supplement the terrestrial infrastructure, and are particularly useful in sparsely populated areas.

The visible trend of convergence of terrestrial and non-terrestrial networks, especially satellite ones, should also be noted. It is assumed that the next generation of cellular networks (6G) will be integrated with satellite networks. Currently, there is increasing cooperation between mobile operators and satellite operators regarding the testing of the reception of satellite signals via mobile devices. After 2030, we can expect fully integrated services in end devices. This means that users will be able to access telecommunications

services regardless of their location. Network convergence will also enable the further development of IoT and autonomous services, particularly those related to transport.

Satellite communications should also be considered a dual-use resource (civilian and military), which, in the event of a potential threat, enables a response to difficult-to-predict situations and the provision of timely information. Therefore, in the long term, it is necessary to consider building and developing national capabilities in the area of satellite communications. This will provide further opportunities for the development of secure state communications for civilian and military purposes.

Objective 1: All users in the country have access to ultra-fast telecommunications services - mobile and fixed-line.

What will make it possible to achieve the objective:

a) Continuation of financial support to telecommunications entrepreneurs for the development of infrastructure, especially in the so-called white spots – problematic areas in terms of accessibility, topography and population density;

b) Using alternative technologies to provide connectivity in the most difficult areas for investment, where it is not possible to obtain gigabit capacity using wired technologies;

c) Eliminating legal and systemic barriers to the development of telecommunications networks by amending the so-called Mega-Law, which will cover investment barriers identified by both the Ministry of Digital Affairs and those reported by the telecommunications industry.[15] In addition, the implementation into the Polish legal system of the provisions of the EU Gigabit Infrastructure Act (GIA) regulation to support the development of public telecommunications networks, which provides for the launch of, among others, an open single information point (“one-stop shop"), where each operator can submit, also in electronic format, applications for all necessary investment permits or for the renewal of permits or the granting of rights of way, and obtain information on the status of its application;[16]

d) Providing local government units with substantive support in conducting investment processes in the area of telecommunications and appointing broadband coordinators in all municipalities and poviats by 2026;

e) Continuing educational and information projects on the role of telecommunications infrastructure (fixed-line and mobile – including 5G and 6G) for the socio-economic development of the country and counteracting disinformation in the field of mobile networks;

f) Maintaining and developing the internet.gov.pl (SIDUSIS) portal, which provides everyone with information on the availability of Internet access services at a given address point in an easy and accessible form;

g) Maintaining and developing the SI2PEM portal to ensure the availability of knowledge about EMF (electromagnetic field) levels and to popularize this

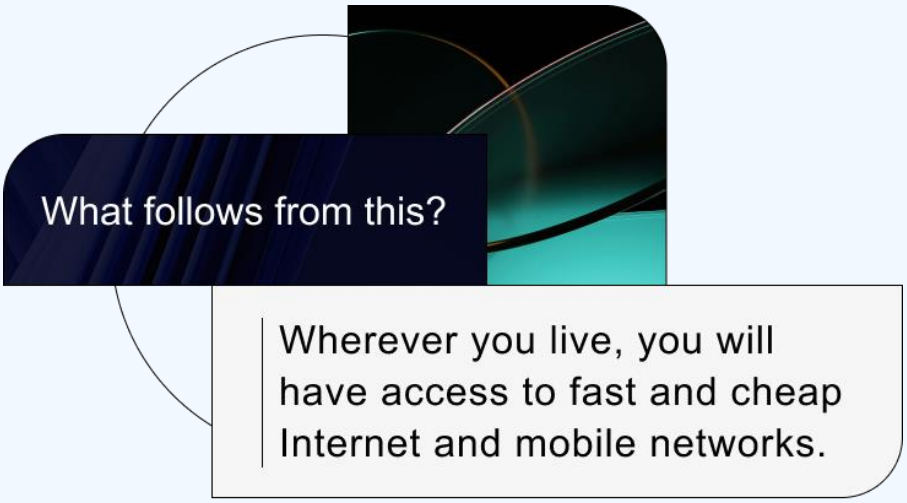
The Act of 7 May 2010 on supporting the development of telecommunications services and networks (Dz.U. /Journal of Laws/ of 2024, item 604, as amended) 15

16 https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R1309

knowledge in order to develop the mobile network and eliminate concerns about the impact of mobile network infrastructure on health and the environment;

h) Supporting the development of local government and private 5G networks – conducting information activities, including preparation of publications, brochures, reports, as well as the organisation of training courses on the implementation of 5G technology and the promotion of innovations – startups and companies working on 5G implementation solutions;

i) Ensuring the appropriate quality of telecommunications networks – implementing system and technical tools to measure the parameters of telecommunications services, as well as implementing effective intervention mechanisms to improve the quality of telecommunications services.



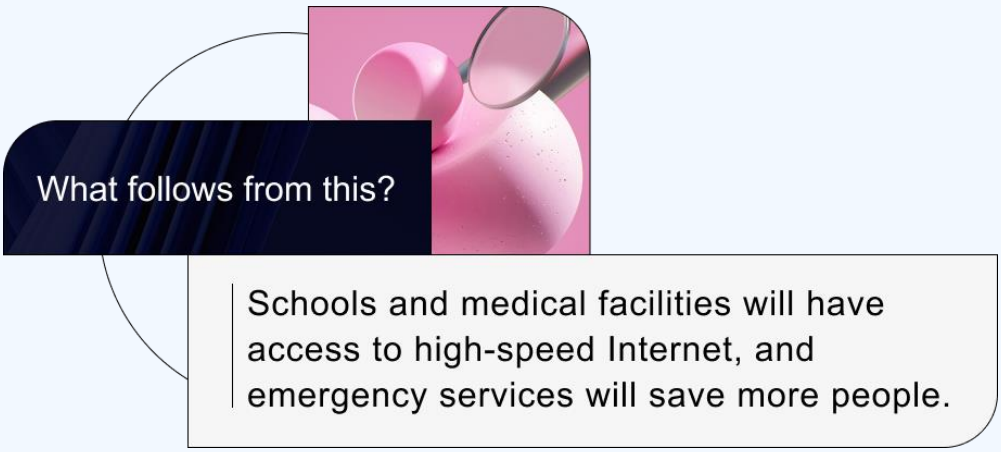
Objective 2: Secure electronic communications are free for specific end-user groups

What will make it possible to achieve the objective:

a) Modernisation of the National Educational Network (OSE) – providing schools with access to a network capable of handling gigabit traffic, also in classrooms. Inclusion in the OSE programme of kindergartens, teacher training centres, educational psychology assessment centres, youth educational centres, youth sociotherapy centres, special training and education centres, special educational centres for children and youth as well as rehabilitation and educational centres.

b) Construction of the National Medical Network – a network built in a similar way to OSE, but connecting at least hospitals and major healthcare institutions.

c) Implementation of the Advance Mobile Location (AML) service, free of charge for end users, which enables the precise location of emergency callers based on data originating from a telecommunications terminal device in the mobile network and transmitted to regional emergency notification centres using the public mobile network.



Objective 3: Telecommunications services are widely used by society, government and businesses.

What will make it possible to achieve the objective:

a) Introduction of connectivity vouchers programme – a set of economic incentives for end users to use certain services.

b) Financial and organisational support for entities involved in the implementation of next-generation mobile networks thanks to the creation of the Mobile Network Applications Fund (5G and 6G), which will enable cooperation between public institutions, research institutes, universities and industry to develop applications for mobile networks and provide appropriate funds for that purpose.

Objective 4: The country's digital transformation goals are supported by a sovereign, secure satellite communications system

What will make it possible to achieve the objective:

a) Development, construction and launch of a telecommunications satellite into geostationary orbit and a constellation of high-throughput broadband communications satellites in low Earth orbit. The satellite capabilities should be fully programmable, equipped with radio transmission control functions in terms of throughput and coverage, and be capable of laser communications between each other in different orbits;

b) Development and construction of a technology demonstrator for the GOVSATCOM system in the scope of providing satellite communications services to public administration, emergency management and security services;

c) New investments and innovations to develop and expand the national potential for high-speed telecommunications based on satellites and terrestrial infrastructure for the provision of cost-effective, high-quality broadband telecommunications services by operators;

d) Development and construction of a technology demonstrator (ultimately a satellite constellation in low Earth orbit with the ability to communicate with a satellite in geostationary orbit) in the scope of using innovative technological possibilities for secure transmission and storage of data in space.

1.2 Competencies of the future

Diagnosis – what is it like?

Broadly understood, competencies of the future are of fundamental importance for the development of the digital sphere in the country. Citizens must not only be able to use digital technologies, but also do it in a healthy way, know the rules of digital hygiene and be able to recognise disinformation. Digital competencies themselves are crucial for the effectiveness, innovation and competitiveness of the Polish economy. According to Eurostat data, in 2023 only 44% of Polish citizens had at least basic (EU average - 56%), and 20% - above basic digital skills (EU average - 27%).[17]

The deficit of digital competencies is most evident among the elderly (aged 65-74), where 87% of the respondents did not have at least basic digital skills (EU average - 72%) and in the age group of 55-64, where 76% of the respondents lacked basic digital skills (EU average - 56%), similarly as among farmers and people with disabilities - 77%. There were also large disparities between respondents living in cities and villages: the percentage of rural residents with at least basic digital competencies was 33% (EU average - 47%), which represents 22 percentage points less than in the case of people living in cities. Digital competencies should enable citizens to understand and navigate an environment that uses technologies in almost every aspect of life. People with low digital skills are much more vulnerable to disinformation and failure to verify information received by digital means.

In 2023, the share of ICT specialists in the total number of people employed in Poland was 4.3% (EU average - 4.8%).[18] Given the expected increase in demand for this category of employees and the percentage of 10% planned for the EU as part of the 2030 Digital Decade, this situation should be considered unsatisfactory.

In Poland, similarly to the EU, women accounted for 19% in the group of ICT specialists.[19] This imbalance works to the disadvantage of women themselves, as well as the ICT sector and the economy. According to the data, the Polish education system does not guarantee that secondary school graduates will obtain a basic level of digital competencies - in 2023, only 58% of people aged 16-19 had at least basic digital skills (EU average - 66%).[20] Higher education does not provide an adequate supply of ICT specialists - in 2022, only 4.3% of all

17 Eurostat: https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i21/default/table?lang=en&category=isoc.isoc_sk.isoc_sku

18 Eurostat: https://ec.europa.eu/eurostat/databrowser/view/isoc_sks_itspt/default/table?lang=en&category=isoc.isoc_sk.isoc_sks.isoc_skslf

19 Eurostat: https://ec.europa.eu/eurostat/databrowser/view/isoc_sks_itsps/default/table?lang=en&category=isoc.isoc_sk.isoc_sks.isoc_skslf

20 Eurostat: https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i21__custom_12512302/default/table?lang=en&page=time:2023

https://ec.europa.eu/eurostat/databrowser/view/educ_uoe_grad02__custom_12849024/default/table?lang=en

graduates (EU average - 4.5%) completed their education in the field of ICT.[21] The share of women among ICT graduates was 22% (EU average – 21%).[22] In the context of supporting digital innovations by university graduates, education in the areas of STEM, breakthrough technologies and fields supporting their development should also be taken into account.

There is no systemic solution for improving the digital competences of public administration employees, which would increase the level of e-government service provision and citizen satisfaction.

21 Eurostat: https://ec.europa.eu/eurostat/databrowser/view/educ_uoe_grad03__custom_12512661/default/table?lang=en

22 Eurostat: https://ec.europa.eu/eurostat/databrowser/view/educ_uoe_grad03__custom_12512714/default/table?lang=en

Objective 1: At least 85% of Polish society has at least basic digital skills, and 50% has above basic digital skills

What will make it possible to achieve the objective:

a) Providing adults, in accordance with their needs, with opportunities to develop digital skills in Digital Development Clubs (KRCs) established in interested municipalities. Each adult will be able to take advantage of classes held in the KRCs and receive advice from educators employed in the clubs;

b) Initiating activities to support people with disabilities, including financial support for the purchase of equipment necessary to acquire digital competencies; organising training sessions dedicated to people with disabilities; supporting non-profit organisations in implementing activities to improve digital competencies among people with various disabilities and special needs;

c) Motivating society to expand digital competencies by highlighting the benefits and opportunities provided by them. Relevant campaigns will be conducted both at national and local levels;

d) Providing access to training, including those ended with the evaluation of acquired competences, e.g. in the micro-credentials model, and educational materials at www.kompetencjecyfrowe.gov.pl, which will map online places, events and materials for developing digital competencies;

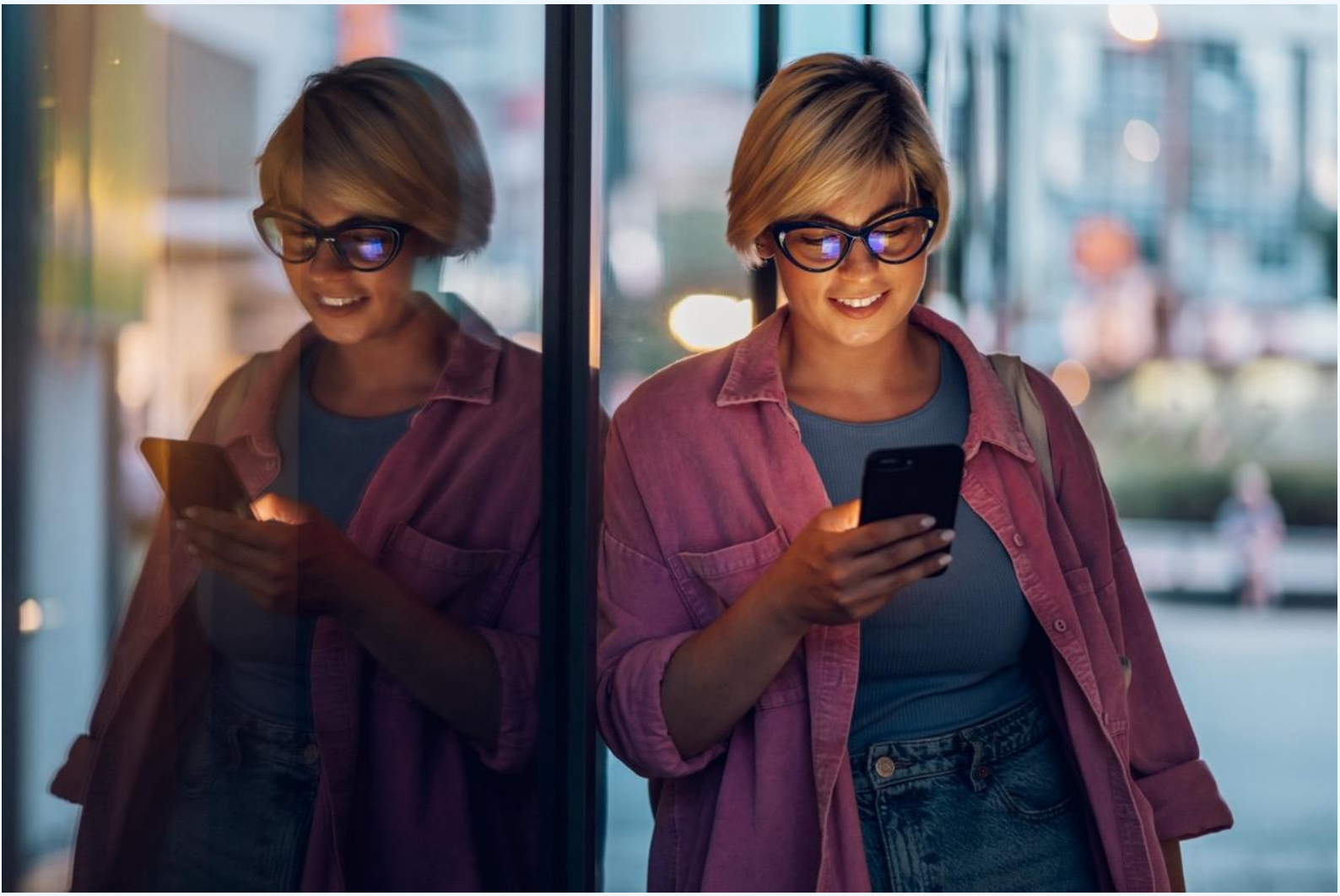
e) Building awareness of how to navigate safely in the digital world. It will be based on the prevention of cyberbullying and addictions, raising awareness of threats and the ability to respond to them, promoting the conscious use of digital technologies (including AI), emphasising the need for critical thinking and the application of digital hygiene principles, addressing ethical issues emerging with the development of AI and equipping society with competencies appropriate for safe and satisfactory functioning in the digital world;

f) Systemic counteracting of disinformation combined with increasing citizens' awareness of the operation of disinformation mechanisms; developing critical thinking competences, information verification skills and the ability to use the media at all levels of education;

g) Cooperation, mobilisation and activation of entities that create the ecosystem of digital competencies development in Poland, i.e. non-profit organisations, enterprises, educational and cultural institutions, social partners, public administration, etc.

h) Ensuring that students develop such digital competencies that each student has at least basic, and preferably above basic digital skills, in accordance with the Digital Transformation of Education Policy. The digital education system is to be

supported by appropriately prepared teaching staff and in the conditions of current state-of-the-art digital technologies.



Objective 2: The number of male and female ICT specialists meets the needs of the Polish economy

What will make it possible to achieve the objective:

a) Supporting students, especially girls, in developing their interests in computer science, initiating programmes supporting the development of competencies in new areas of breakthrough technologies, such as AI and quantum technologies, expanding the Information Technology Talent Development Program to primary schools and supplementing it with a breakthrough technologies component. An additional element will be promotional activities aimed at parents, students and teachers;

b) Eliminating barriers that limit the presence of women in ICT, promoting ICT education and professions, and combating stereotypes that inhibit the inflow of women to digital professions;

c) Conducting information campaigns presenting possible career paths in ICT;

d) Creating modern training and fast-track mechanisms enabling those willing to change profession to become an ICT specialist;

e) Initiating projects supporting the development of advanced competencies in new digital technologies for employees, in particular in the SME, industry and services sectors;

f) Increasing the number of STEM graduates, with particular emphasis on majors necessary for the development of breakthrough technologies, and the number of PhDs conducted in academia in STEM specialisations;

g) Increasing the number of interdisciplinary specialists and AI/STEM/ICT experts, combining these areas with other majors necessary for the development of breakthrough technologies;

h) Monitoring women’s participation in ICT, as well as changes in awareness and attitudes related to the image of science subjects, ICT professions and gender roles, and the role of women in ICT.

Objective 3: Effective and high-quality digital education is available at all levels of education, taking into account the needs of people from particularly vulnerable groups

What will make it possible to achieve the objective:

a) Improving the quality of fostering the digital competences of the young generation through the development of digital didactics, adapting the core curriculum to technological and methodological progress, and preparing teachers to carry out classes in accordance with the applicable core curriculum and the methodology of using new technologies in teaching;

b) Raising digital qualifications and competencies in artificial intelligence (AI) among all teachers, lecturers, academic and scientific staff;

c) Commissioning studies (including postgraduate and further training) in the field of computer science teaching, digital competencies of teachers and the application of modern teaching methods using digital technologies;

d) Using digital technologies in schools to improve the quality of education, to break away from the facile form of knowledge transfer, to support teamwork, team projects, gamification and ensure contact with state-of-the-art digital technologies such as AI, robots, micro-controllers, 3D printers, VR/AR (virtual/augmented reality), etc.;

e) Introducing into the core curriculum the formation of skills for the safe use of public and private e-services (in the areas of health, science, administration, communication, finance, cultural resources, etc.) and topics related to artificial intelligence - explaining how it works, programming, how to use this technology in a safe, ethical and responsible way;

f) Introducing topics related to disinformation, critical thinking, media literacy and information verification into school curricula as well as in teaching and training programmes for teaching staff;

g) Introducing issues related to digital accessibility into the core curriculum at all levels of education.

What follows from this?

The Polish school will prepare students to use digital technologies independently and safely and will support the discovery and development of IT talents.

Objective 4: Public administration staff have the digital competencies necessary to provide public e-services with the highest level of maturity and efficient administration.

What will make it possible to achieve the objective:

a) Providing access to high-quality training, practical workshops and e-learning course packages, ended with the evaluation of competences acquired, such as the micro-credentials model, including in the areas of digital public services, electronic identification, digitalisation management, process digitalisation, cybersecurity, artificial intelligence, cloud systems, data management and analysis and opening data, smart cities and villages, open-source (open software) in administration, digital accessibility management and its implementation, etc.;

b) Introducing systemic support for administration employees who want to retrain as ICT specialists;

c) Introducing the primacy of staff education in public administration in the areas of diagnosed ICT needs (e.g. cybersecurity, artificial intelligence).

Objective 5: The knowledge, skills and awareness of Polish society respond to the challenges and trends accompanying digital transformation and sustainable development.

What will make it possible to achieve the objective:

a) Including the impact of using ICT services on the environment in education programmes and educating on how to use technology in a more sustainable way. Conducting socio-educational campaigns to raise awareness in the above-mentioned areas;

b) Increasing the level of education of society in the field of breakthrough technologies by organising training courses, workshops and non-formal education;

c) Creating a social communication plan in public media (as part of the public mission) to develop citizens' awareness and knowledge of digital issues.

Objective 6: Polish enterprises have digital competences that are key to running a business effectively, maintaining a competitive position in the market and strategically developing the company using digital solutions.

What will make it possible to achieve the objective:

a) Raising awareness of business owners and their employees about the benefits of implementing technologies of various levels and applications, depending on the company's needs, through profiled expert advice, access to information and educational materials on digital transformation as well as the "Digital Start for Business" package;
b) Building trust in digital technologies by strengthening knowledge about the balance of costs, benefits and risks of implementing digital solutions, cybersecurity and the ability to critically assess the quality and credibility of information sources and identify disinformation;
c) Eliminating concerns about process downtime in a company and the risk of unsuccessful investments in digital solutions through systemic support including reliable diagnostics, assessment of expected effects and selection of the best tools for the company's digital development.

1.3 Cybersecurity

Diagnosis – what is it like?

The growing level of threats in cyberspace, new types of threats and the increase in the activity of cybercriminal, hacktivist and state-linked groups have an impact on the daily functioning of citizens, businesses and public institutions. Poland is one of the countries most frequently attacked in cyberspace, with the number of cyber incidents increasing every year. This is related to, among other things, the spread of technologies (e.g. AI) that enable cyberattacks and the increasing digitalisation of our everyday lives as well as the digitalisation of economies and states. Poland and other Western countries are also targets of hybrid activities by Russia, Belarus and other countries, most of which take place in cyberspace. In the military dimension, cyberspace has become an operational domain on a par with land, sea, air and space. Our country's cybersecurity is also of fundamental importance due to its central role on NATO's Eastern Flank.

The war between Russia and Ukraine, in which Poland serves as a logistical hub of support for the defending Ukraine, has involved numerous cyberattacks, for example on transport infrastructure, which is an important lesson in the context of military mobility and the ability to collectively defend ourselves. We do not remain passive in the face of threats, but we actively counteract them. This includes not only systemic changes that we are introducing through new legal acts but also developing the capacities of institutions responsible for cybersecurity at the national level, equipping them with appropriate technical tools, as well as ensuring an adequate number of cybersecurity specialists (IT services under the Cybersecurity Fund) and universal digital hygiene training at all levels.

Poland will continuously take measures to increase the level of national and international cyber security by systemic means, to increase the level of information protection, as well as to reduce the risks associated with cyberspace.

We will, therefore, comprehensively develop the national cybersecurity system – through legislative changes, increasing the resilience and capabilities of entities in that system and introducing new mechanisms for activity coordination. The fundamental issue is the need to establish a central institution responsible for cybersecurity at the national level. The dissemination of technical solutions to enhance cybersecurity, the development of national technological and industrial capabilities in the area of cybersecurity and the enhancement of the competence of professionals and society as a whole will also be of key importance. Efforts to increase the level of cybersecurity must be undertaken in close cooperation with the relevant ministries and state institutions. The same applies to combating cybercrime, without which digitalisation will not be successful. Actions aimed at ensuring synergy

between the military and civilian dimensions of cybersecurity, as well as between cybersecurity and crisis management, should also be considered very crucial.

Objective 1: The existing national cybersecurity system is mature and effective.

What will make it possible to achieve the objective:

a) Establishing a central institution responsible for cybersecurity at the national level and coordinating the activities of other entities that ensure cybersecurity at the national level, with appropriate political position, competences, human resources, budget and infrastructure;

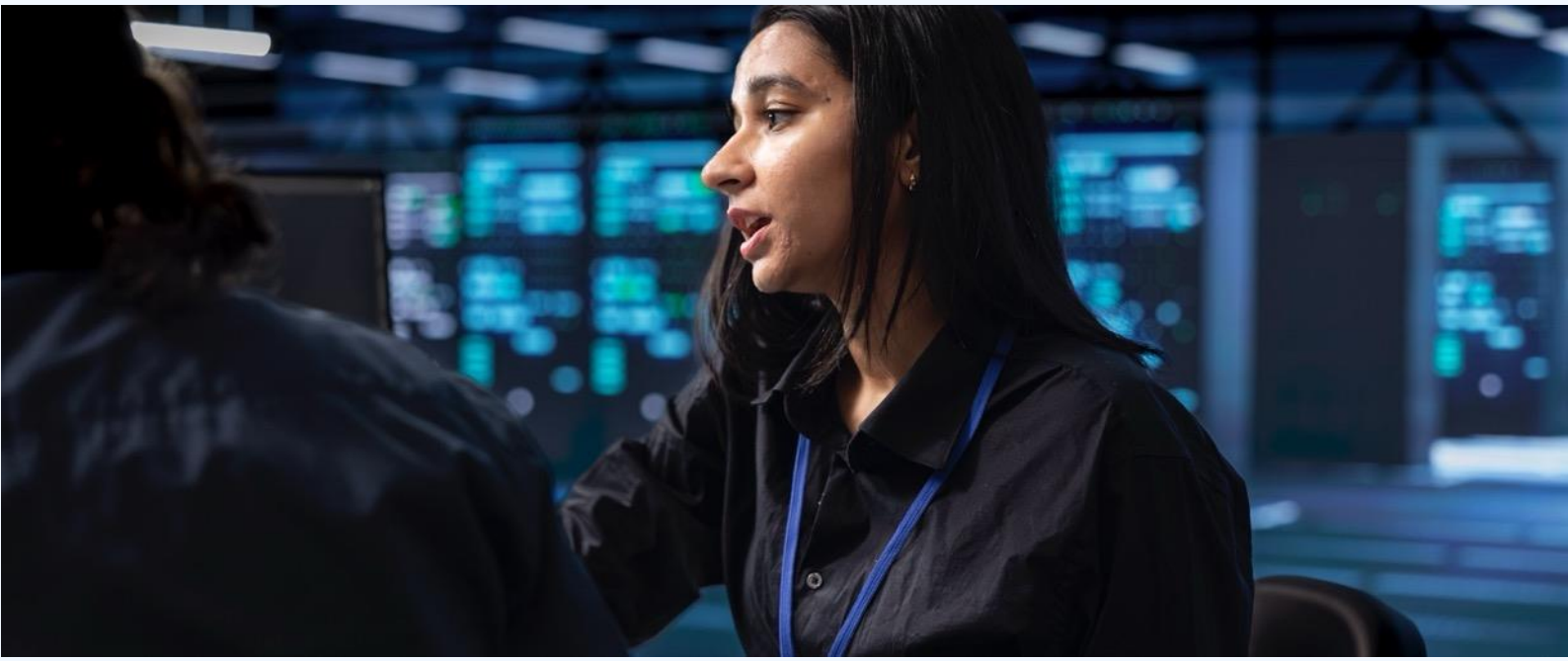
b) Strengthening the role of the Government Plenipotentiary for Cybersecurity and the Joint Cybersecurity Operations Centre. This will increase the efficiency of the system and ensure a more efficient response to threats in cyberspace;

c) Developing the S46 System as a basis for the exchange of information between key, important entities and state institutions;

d) Strengthening the capacity of institutions responsible for ensuring cybersecurity at the national level, with particular emphasis on computer security incident response teams (CSIRTs) of the national level;

e) Creation of sectoral CSIRTs and cooperation with sectoral information exchange and analysis centres;

f) Assisting in the modernisation and expansion of cybersecurity infrastructure in IT networks to the national cybersecurity system entities, including support for local government units in the construction of local government structures responsible for cybersecurity.



Objective 2: Information systems in the public (including military) and private spheres have a high level of resilience.

What will make it possible to achieve the objective:

a) Introduction of a mechanism for taking into account cybersecurity requirements for ICT products and ICT services in public procurement, and the specifications of these requirements;

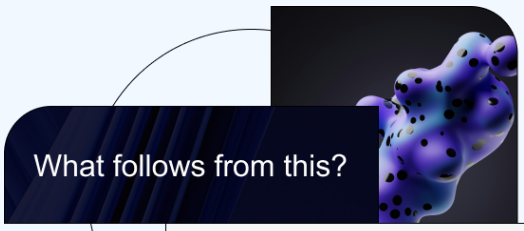
b) Introduction of a mechanism to exclude urgent purchases related to cybersecurity from the requirements of public procurement law, which will help avoid lengthy tender procedures that adversely affect the country's cybersecurity;

c) Introduction of coordinated solutions for the management of vulnerabilities, including their identification, cataloguing and disclosure;

d) Developing national cryptographic solutions and standards (including in the area of post-quantum cryptography), as well as initiating research, development and innovation programs and projects in this area, so that Poland can safely migrate to post-quantum cryptography and use quantum technologies for the benefit of state security;

e) Launching a cloud for processing classified information (classified cloud);

f) Developing Cyber Threat Intelligence and Cyber Foresight to respond to current challenges. Those actions can be used for risk management purposes and to introduce mechanisms to correct operational goals.



What follows from this?

We will develop a plan for migration to post-quantum cryptography, which will secure citizens' communication with institutions and companies (e.g. banks) when "Q-Day" arrives - quantum technologies become mature enough to break existing encryption methods.

Objective 3: The national technological and industrial base in the area of cybersecurity has well developed potential and is characterised by a high degree of technological sovereignty.

What will make it possible to achieve the objective:

a) Increasing the security of supply chains on a national and international level (both in terms of hardware and software), guided by the interests of national security and the Polish economy;

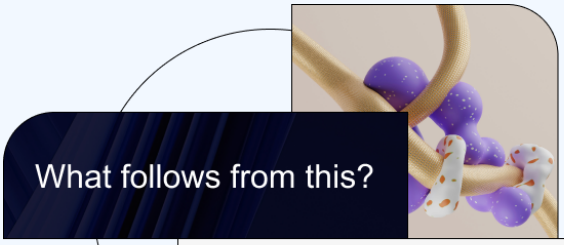
b) Exclusion of ICT products, types of ICT services or specific ICT processes from high-risk suppliers (using the legal mechanism of the KSC Act);

c) Developing a national cybersecurity certification system to provide procedures necessary for the correctness of certification processes;

d) Implementation of research, development and innovation programmes and projects in the field of cybersecurity, which will enable the development of national technological and industrial competencies and increase Poland's technological sovereignty;

e) Implementation of initiatives using breakthrough technologies (including artificial intelligence) for cybersecurity purposes;

f) Implementation of research, development and innovation programs and projects in the field of cybersecurity that will enable securing AI models and systems implemented in Poland.



What follows from this?

We will enable the exclusion of high-risk suppliers when threats to national security are identified. Therefore, we will provide citizens with access to safe and secure ICT products, services and processes.

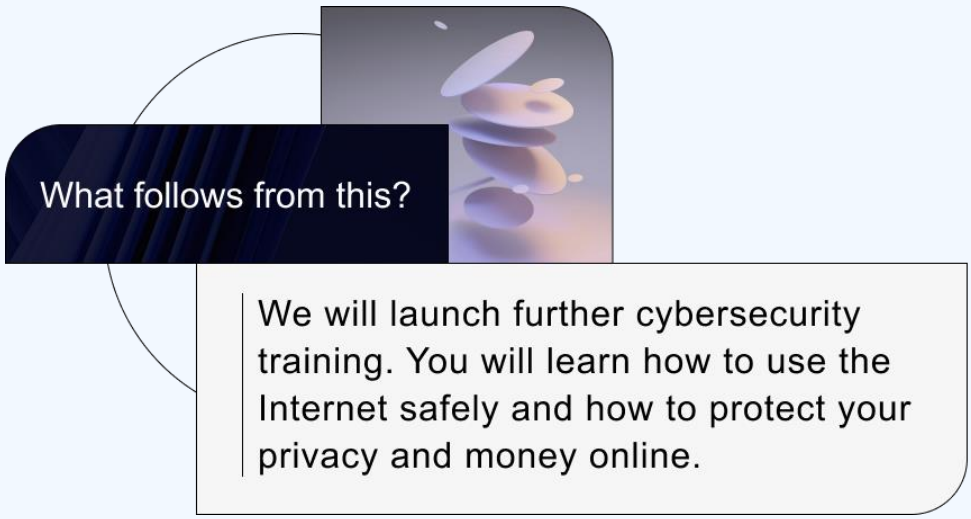
Objective 4: The personnel of the national cyber security system entities and the public are aware of cyber threats and have relevant cyber security knowledge and competence.

What will make it possible to achieve the objective:

a) Increasing public awareness and knowledge of cybersecurity through the implementation of cybersecurity education and training activities, skills and awareness raising, including good practices and digital hygiene;

b) Strengthening the competences of the staff of entities of the national cybersecurity system;

c) Ensuring the functioning of the Cybersecurity Fund and ICT benefits.



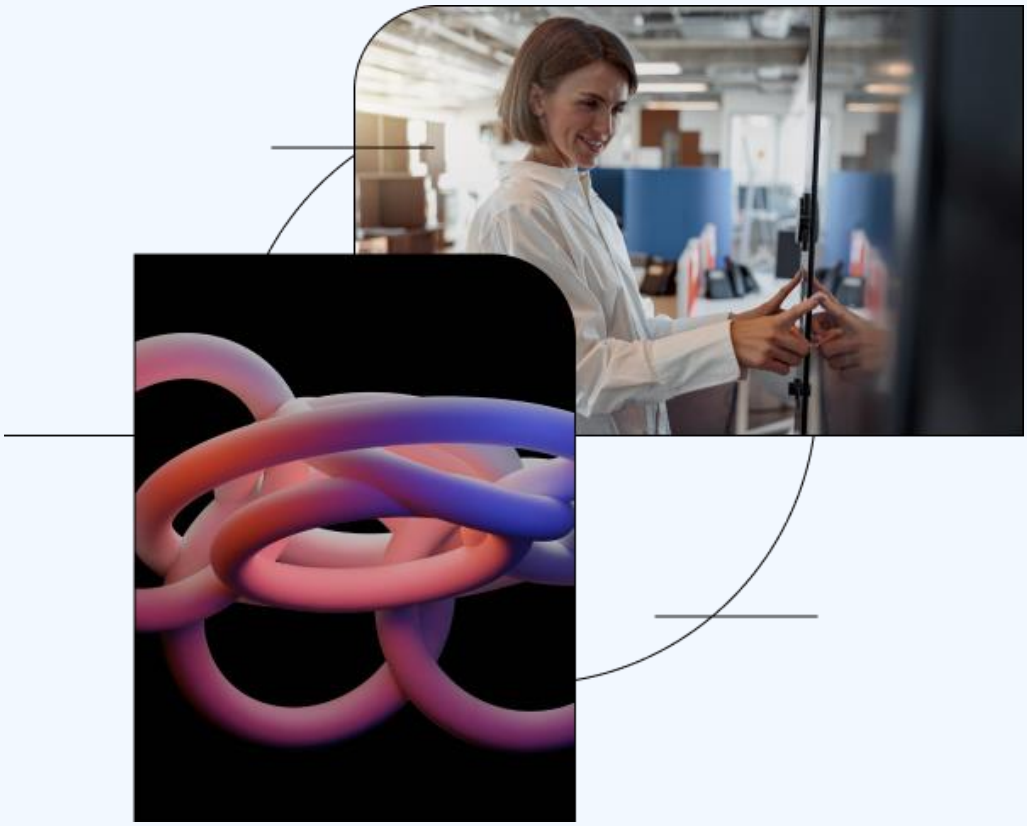
Objective 5: Poland has a strong international position in the area of cybersecurity.

What will make it possible to achieve the objective:

a) Active international cooperation on the strategic and political level, e.g. participation in works (including legislative activities) on raising the level of cybersecurity at the international level, Poland's performance of key roles in international organisations or participation in international investments increasing cyber resilience;

b) Active international cooperation at the operational and technical level, e.g. multilateral exchange of information and experiences and active participation in drills;

c) Coordination by the Government Plenipotentiary for Cybersecurity of activities in the international arena in the framework of civil-military cooperation in the area of cybersecurity.



1.4 Coordination of the country's digital transformation

Diagnosis – what is it like?

The horizontal nature of digitisation processes renders effective inter-ministerial and cross-sectoral cooperation and the systematisation of knowledge on the activities undertaken in different areas of state activity indispensable. Although initiatives to date have brought some improvements in this regard, effective digitisation management requires greater coordination. Comprehensive, coherent and structured information on the state of computerisation of public entities and its effects is still lacking. This is crucial, as monitoring and controlling the implementation of e-government projects across the country improves the efficiency of project delivery while coordinating ICT spending enables cost optimisation and strategic prioritisation of investments based on the country's needs. At the same time, it allows increased transparency and accountability in public spending and indirectly translates into increased competitiveness of the country in the international arena.

For the efficient coordination of Poland's digital transformation, not only the internal dimension is important.

It is also necessary to improve coordination in the area of digital diplomacy – a new area of the state's foreign policy related to the rapid development of digital technologies and their dissemination in international relations. This area includes, among other things, international governance of artificial intelligence and other digital technologies, attracting foreign investment, and relations between states and global technology corporations. In Poland, digital diplomacy is poorly developed – there is a lack of appropriate conceptual foundations, organisational coordination or a coherent national strategy in this area. Effective digital diplomacy requires joint action by the ministries of foreign affairs, development and digitalisation.

We recognise that one of the pillars of digital transformation is the State Information Architecture (SIA), a method of managing the computerisation of the state, based on architectural models and encompassing basic principles, standards, guidelines and architectural recommendations, including those related to interoperability, accessibility, user orientation, reusability of data, technical components, documentation and experiences. Changes in legislation that can help to effectively implement AIP are crucial, as well as promoting its relevance and objectives and its benefits, as the knowledge deficit of AIP negatively affects the digital transformation of the country.

Objective 1: The exchange of information on the state of digitalisation of public administration units and the IT projects they implement is efficient and effective

What will make it possible to achieve the objective:

a) The activities of the Committee for Digital Affairs [KdsC], which has broader competences than the previously existing Council of Ministers Committee for Digital Affairs. The KdsC is to ensure coordination of state activities related to computerisation and support for the digital development of the state. Its tasks will include consideration of draft government documents related to computerisation, monitoring, giving opinions and publishing information on IT projects of public use, monitoring the implementation of strategies and other documents of a strategic nature related to computerisation;

b) Activities of plenipotentiaries for computerisation, appointed in particular in ministries and the Chancellery of the Prime Minister. Their basic tasks will include coordinating the implementation and execution of strategies in matters falling within the competence of the government administration department headed by the relevant minister.

Objective 2: IT projects are implemented and managed in a coordinated, transparent and efficient manner

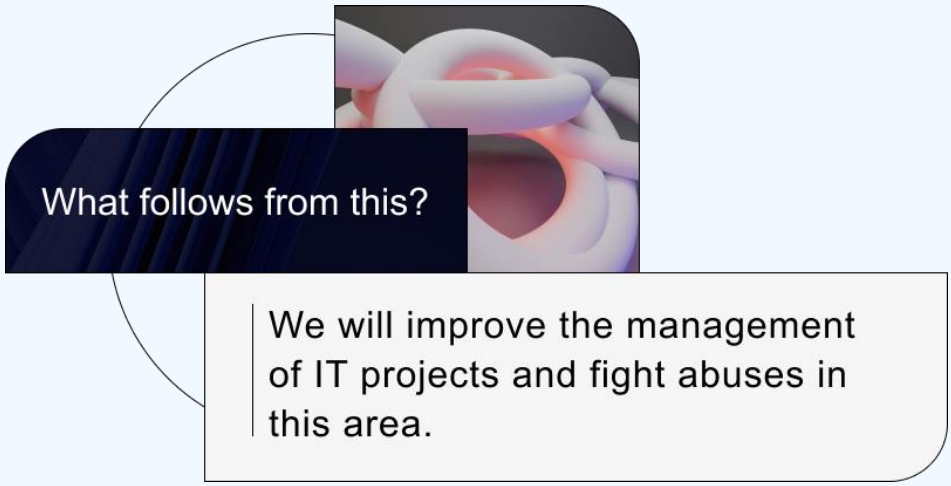
What will make it possible to achieve the objective:

a) Implementation of a common methodology for managing IT projects implemented in all public administration units, allowing effective monitoring of their progress and effects;

b) Establishment and operation of a repository of project management standards, functional and non-functional documents;

c) Full reporting on entities and individuals conducting IT projects for the state, which will enable increased transparency and optimisation of fund spending;

d) Conducting a comprehensive diagnosis of the effectiveness of awarding and implementing public procurement contracts (from the perspective of the ordering party and the contractor) regarding IT projects. It will test the possibility of introducing specific rules for those projects within the framework of public procurement law, through more flexible legal solutions that take into account the need for modifications and technological changes.



Objective 3: The State Information Architecture is a common and well-established method of strategic management of the state's computerisation.

What will make it possible to achieve the objective:

a) Implementing the principles for and developing and implementing architectural standards, guidelines and recommendations in public administration, and obliging public entities implementing public e-services to apply them;

b) Implementing the adopted method for describing the AIP, including a glossary, clarifying the scope for which the method will be used and preparing for the AIP a vision mapping the desired state of the country’s digitalisation in terms of the implementation of public e-services. The AIP vision aims to present a universal approach to the planning and effective delivery of public e-services, with a strong emphasis on the ICT system interoperability that is required in this regard;

c) Updating the modelling methodology and AIP reference models (metamodels) in the legislative, organisational, semantic and technical layers, enabling a coherent and integrated approach to the creation and modification of processes and ICT systems implementing the strategy objectives;

d) Keeping up-to-date and expanding the AIP repository, which is an ICT system that collects, in particular, architectural models and architectural principles, standards, guidelines and recommendations;

e) Improving access to the information in the AIP repository insofar as permitted by data protection laws (information to be made available contextually in relation to the needs of individual stakeholders) and co-operating and exchanging current information relevant to the development and maintenance of the AIP, including on identifying reusable components from each AIP layer;

f) Analysing the differences between the current state of the country’s digitalisation and the target vision set out in the AIP to define IT projects whose implementation will increase the efficiency of the country's digital transition;

g) Establishing oversight and monitoring mechanisms for AIP implementation, including:

- Appointing Chief Enterprise Architects in all ministries (plenipotentiaries for computerisation may serve in this capacity) to support the dissemination, implementation and development of AIP and participating in the work of a task force at the Committee for Digitalisation to support the Committee’s tasks in this area,
- making the implementation and financing of public-use IT projects conditional on a positive assessment by the Committee for Digitalisation, particularly in terms of

compliance with the principles, standards, guidelines and architectural recommendations of the State Information Architecture (AIP),

- Expanding the inventory obligation to cover all public administration ICT systems and public registers, including field-specific systems, e.g. accounting and human resources, with such inventory to be done using inventory systems for ICT systems (SIST, SIST JST),
- Verifying, as part of the work of the Committee for Digitalisation, the compliance of draft legislation with the principles, standards, guidelines and architectural recommendations of the State Information Architecture (AIP).

Objective 4: Digital diplomacy is effective and efficiently coordinated.

What will make it possible to achieve the objective:

a) Developing a joint public administration strategy document to set out goals and directions in the area of digital diplomacy. Selecting priority international organisations and countries and developing “geographic” digital policies outlining action plans in North America, Africa and Asia;

b) Building competencies in the office serving the minister in charge of computerisation in terms of attracting foreign investment in modern technologies in Poland and promoting Polish digital technologies in the world, as well as allocating appropriate resources for this purpose. Among other things, this will enable the development of capabilities to ensure technological sovereignty in cooperation with international partners;

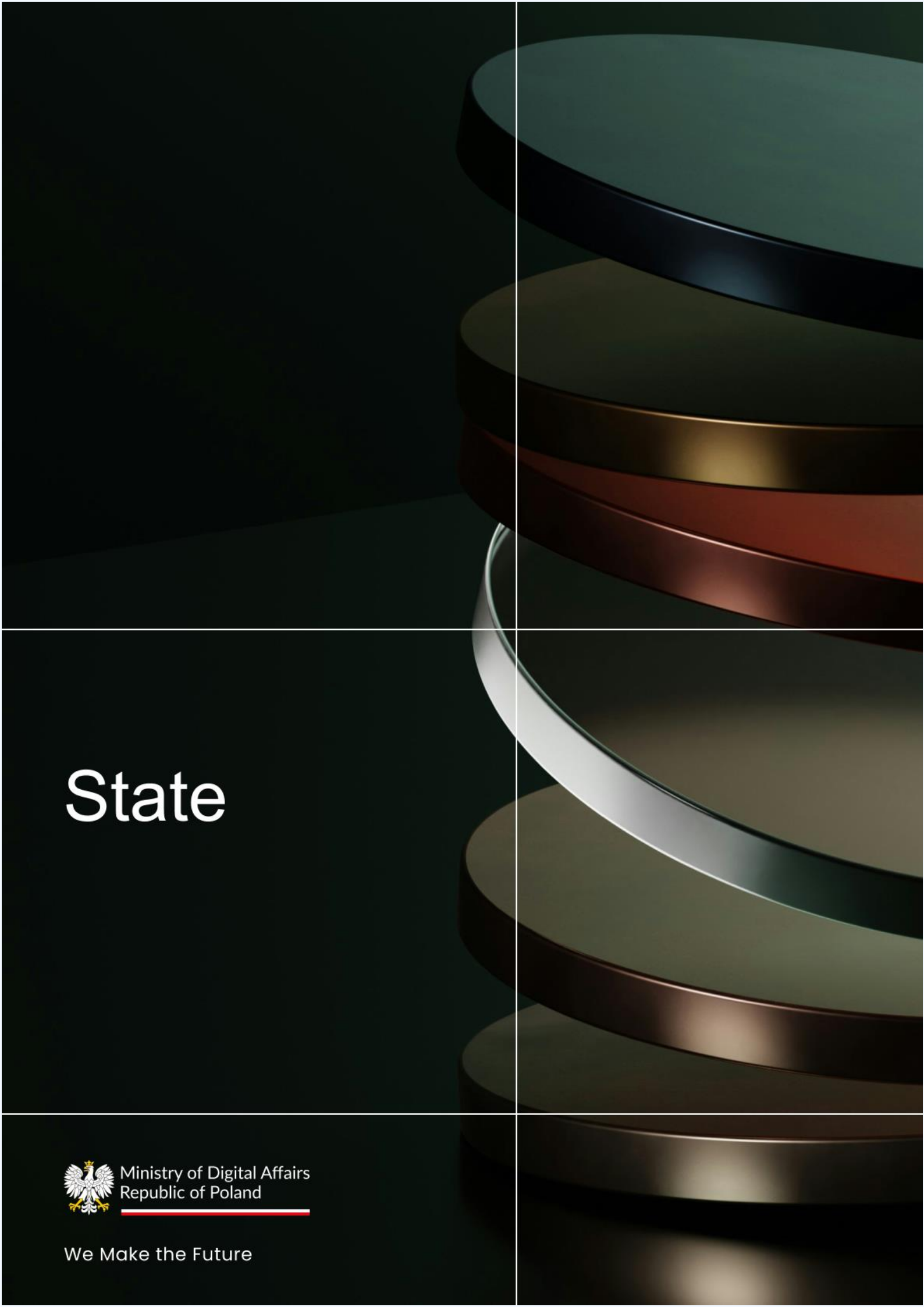
c) Appointing digital attachés, possibly digital-technological-scientific attachés, in Polish diplomatic missions and consular offices in the world’s main digital centres, taking into account that this would be an area where the competencies of several ministries overlap;

d) Regularly creating resources on digital technologies and the digital economy for Polish diplomatic missions in cooperation with the relevant ministries and supervised institutions. They are intended to improve the competencies of diplomatic staff, promote Polish technological solutions, support international cooperation with Polish institutions and businesses and facilitate the acquisition of foreign investment;

e) Ensuring that digital technologies, as perceived and acted upon by diplomatic missions, constitute a distinct field of activity, which is not a subcategory of scientific or economic cooperation while being closely correlated with these areas of cooperation.

What follows from this?

We will provide Polish diplomacy with the tools and competencies to effectively attract digital investments and promote Polish innovations.



State

Ministry of Digital Affairs
Republic of Poland

We Make the Future

State

2.1 Public e-services

Diagnosis – what is it like?

A key element in the development of e-government is electronic public services (public e-services), i.e. services for processing public tasks by means of electronic communication. The system of public e-services in Poland has noticeably developed in recent years. Government services make more than 1,700 e-services available to citizens at a minimum of maturity level 3. The main focus so far has been on providing as many public e-services as possible to citizens, entrepreneurs and the public administration with added value for the user. Current activities focus on creating and providing modern e-services at a higher level of maturity, based on existing mechanisms and relying on ICT systems, public registers and e-government platforms.

Thanks to increasing interoperability, it is easier for public entities to access data that has been collected over the years by other public entities. Therefore, legal entitlements and obligations can be handled without the need to create new electronic public services between the public entity and the service recipient. This is possible because the information necessary for their implementation is already in public ICT systems and public registers.

The default approach should be not to involve the entity (including a citizen or business) with the relevant legal obligation or entitlement in the performance of the given public task.

This saves time and results in a higher level of satisfaction among citizens and businesses. Of course, there may be legitimate exceptions to this approach.

To ensure that electronic delivery of public services does not cause difficulties for users, public e-services should be user-oriented, i.e. simple and understandable for every citizen, entrepreneur and official. Case processing is also hampered by administrative jargon and technical terminology, so the widespread use of simple and inclusive language is also necessary.

Even though many public e-services have already been made available, there are still barriers to their availability, wider dissemination and effective use. These include:

- the lack of a single point of access to public e-services for citizens, businesses and administration bodies that would provide a uniform interface and method of user authentication, as well as digital signature and electronic seal functionalities;
- implementation of a variety of tools (platforms) for the delivery of public e-services, which are based on uniform standards enabling the specific needs of e-service users to be taken into account, e.g.:
    a. tools to design electronic forms,
    b. tools to transform the defined and standardised business processes that underpin an e-service into an application to support its implementation,
    c. mechanisms for the transmission of electronic documents, and ones that do not make use of horizontal solutions to support the implementation of public e-services, such as public administration catalogues, reference registry sharing platforms, e-payment processing systems or case repositories;
- the lack of common catalogues for public administration to support organisational, semantic and technical interoperability of public administration (public administration catalogues), including catalogues of processes, cases, public e-services, document models, registers, powers of attorney and authorisations;
- a limited range of public e-services enabling matters to be handled fully online;
- non-integrated public administration registers and ICT systems, the lack of a catalogue of public registers metadata and a catalogue of public ICT systems APIs (Application Programming Interfaces), as well as the lack of platforms for making public reference registers available through APIs ensuring their interoperability, which, among other things, requires users to repeatedly input data that is already held by public administration bodies;
- insufficient data openness and use of open data exchange formats and platforms to support the delivery of public e-services;
- the lack of mechanisms to manage and monitor the implementation of public e-services to develop lines of action for improving their efficiency;
- the lack of public e-services that accept cross-border authentication methods;
- the untapped potential of new technologies in the processes of creating public e-services, including cloud computing;
- digital exclusion of part of the population, which hinders electronic communication with public administration bodies, e.g. due to inequalities in internet access, failure to

adapt e-services to people with special needs or the elderly, as well as insufficient digital skills.

Objective 1: Public e-services are available in one place and take into account the needs of all users

What will make it possible to achieve the objective:

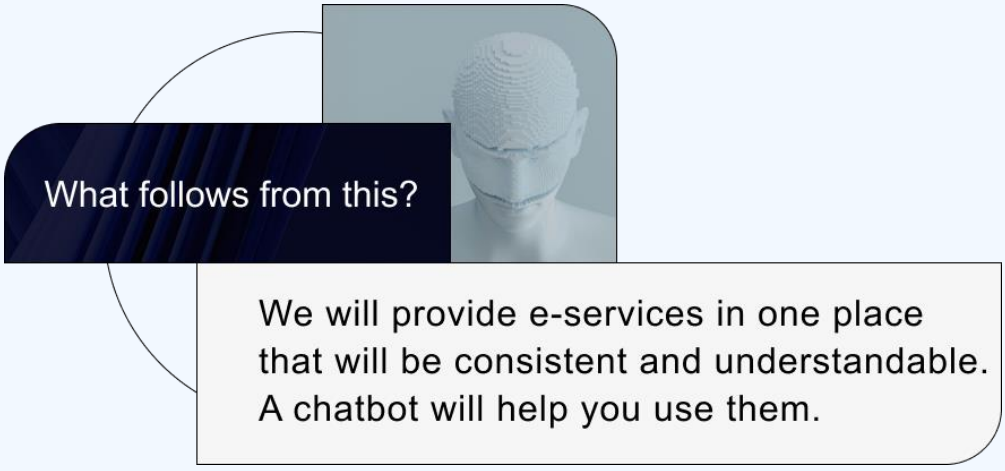
a) Implementing a single point of access to public e-services for citizens, businesses and administration bodies. This will provide a unified interface, making the available e-service communication channels more consistent;

b) Surveying the needs of citizens, businesses and public administration bodies regarding new public e-services and the modification of the existing ones. This will identify key directions for creating, developing and optimising digital solutions to support e-service delivery;

c) Aligning the required and key public e-services with the requirements of the national digital identity wallet and the EU Digital Identity Wallet, which is a certified, recognised and highly secure means of electronic identification;

d) Supporting public e-service users and identifying their reported needs using a chatbot trained on public administration data;

e) Organising systemic support for public e-service providers in harmonising their activities to ensure unified access to e-services and means of electronic identification.



Objective 2: Uniform public e-service delivery tools are implemented to facilitate interaction between e-service providers and their users

What will make it possible to achieve the objective:

a) Building, sharing and developing platforms for the implementation of public e-services provided at the national (including area-specific), regional and local levels, ensuring standardised e-service delivery, as well as the security and a high level of maturity of such services, including the mObywatel [mCitizen] System;

b) Increasing the range of public e-services provided using unified e-service delivery platforms;

c) Equipping platforms with tools to automatically transform defined and standardised business processes, which are the basis for the implementation of a public e-service, into solutions to support its implementation;

d) Equipping public e-service providers with a form generator — an intuitive tool to support the independent roll-out of public e-services based on a single, common standard, making them more usable and user-friendly;

e) Implementing functionality to support the user in processing matters quickly online without too much user involvement;

f) Implementing mechanisms for the secure transmission of electronic documents, including the e-Delivery system;

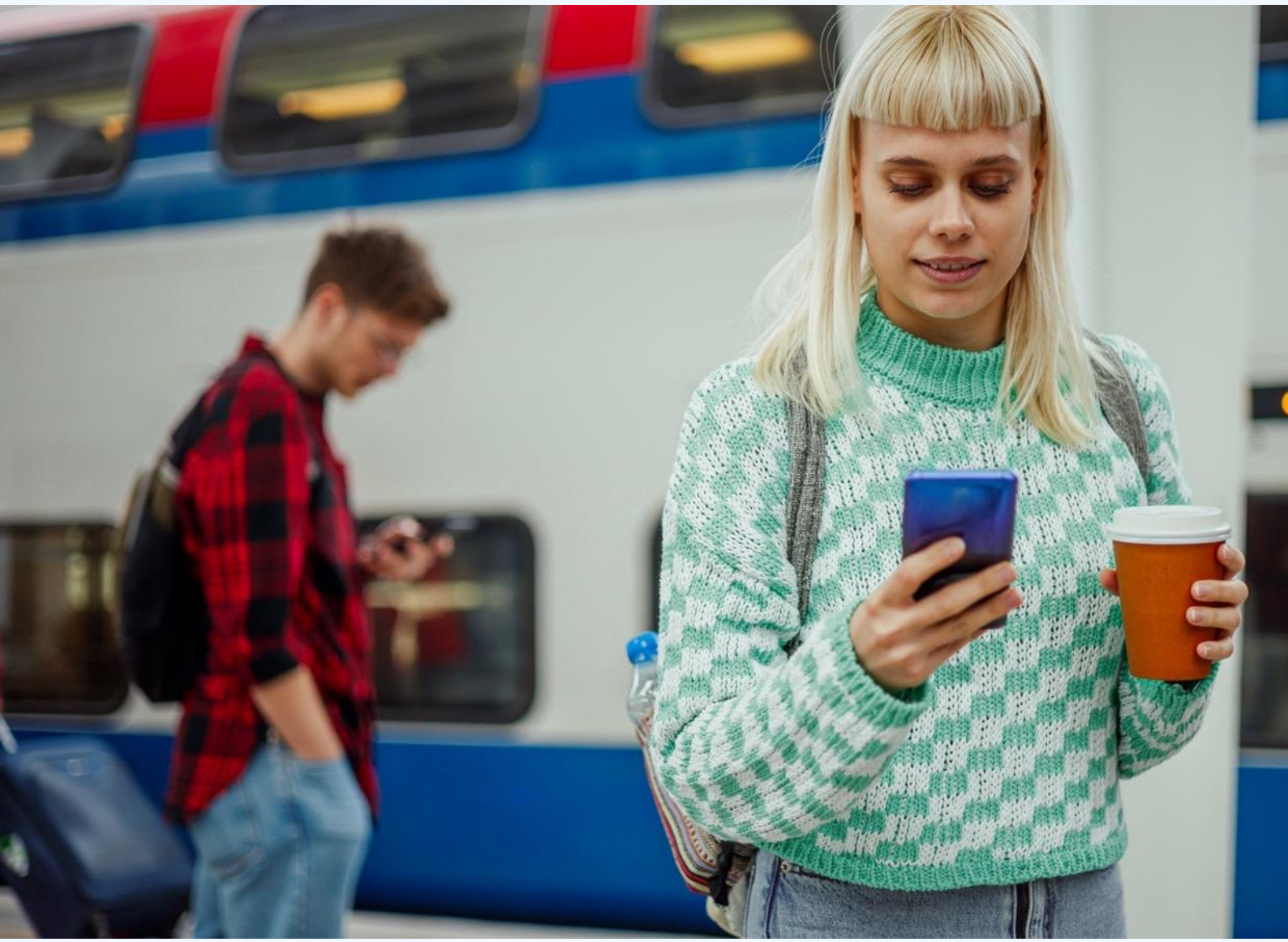
g) Implementing functionality for automated processing of cases handled as part of public e-services, including in electronic document management systems;

h) Expanding the current portfolio of document templates, enabling citizens to use electronic versions of national, regional, local and professional documents;

i) Ensuring that adequate infrastructure is in place for public e-service platforms to guarantee the high quality of e-services and the efficiency of the systems supporting their delivery.

What follows from this?

You can use the e-service quickly and safely - download a document from the document template portfolio, send the data safely thanks to the e-Doręczenia system, and your case will be handled by the office as automatically as possible.

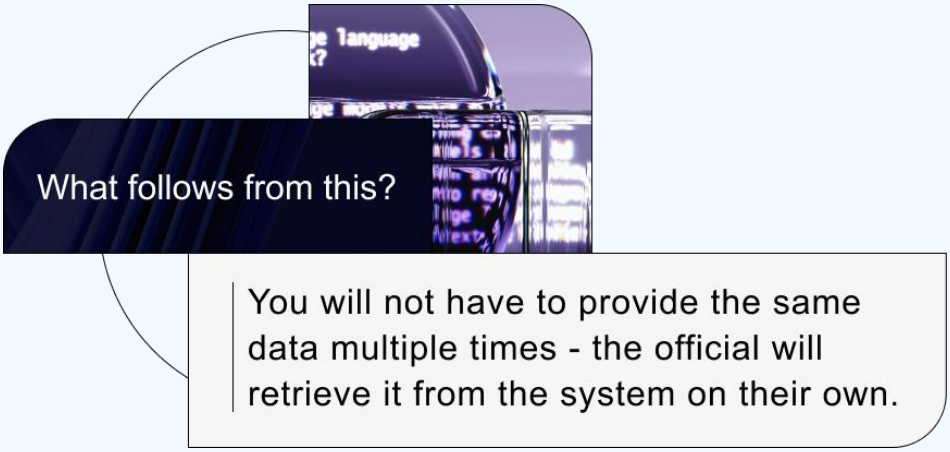


Objective 3: Horizontal solutions ensure that public e-services are optimised

What will make it possible to achieve the objective:

a) Implementing horizontal solutions supporting the implementation of public e-services, ensuring the practical security and high maturity of the e-services provided, as well as increased interoperability of public ICT systems and public registers supporting their implementation, including:

- the reference public registers of the Public Administration Catalogues, i.e. the Administrative Processes Catalogue, the Case Catalogue, the Public Services Catalogue, the Document Model Catalogue, as well as the Public Registers Catalogue and Public Entities Catalogue, making the activities undertaken by the public administration, also with regard to citizens and entrepreneurs, more coherent and effective in the provision or implementation of public e-services;
- a national data sharing platform, a catalogue of public registers metadata and a public ICT systems API to improve the use of shared data, in particular, reference data;
- an e-payment processing system to support the implementation of services e-public through the functionality of handling settlement and clearing with the citizen or business, with particular emphasis on local government administration;
- a case repository collecting information on official matters handled by citizens and businesses, including the status of these matters.



2.2 Digitalising administrative processes and judicial proceedings

Diagnosis – what is it like?

The digitalisation of the operations of public entities is an ongoing and evolving process. It depends on several factors, such as technological capabilities, the needs of society, the digital competencies of citizens and institutional staff and the legal environment. Therefore, it is necessary to constantly monitor the level of digitalisation of public institutions, analyse the phenomena that determine it and respond appropriately to barriers to the implementation of digital solutions.

The public sector now has many systems and places where data is collected and citizens' affairs are handled.

Noteworthy examples include the complete digitalisation of the passport application process, the creation of a system of state registers, as well as the development of Electronic Document Management systems used in public administration bodies as tools for the electronic circulation of documentation.

Nonetheless, their potential remains underexploited. To date, digital administration in Poland has developed in an inadequately coordinated manner. Various entities have independently developed different ICT systems, e.g. to provide public e-services, electronic document workflows or to handle entity-specific matters. This has resulted in funds being spent on building these systems and infrastructure, despite the availability of such solutions as the ePUAP platform. The result is that citizens or entrepreneurs who want to handle matters electronically are forced to use several ICT systems separately or even rely on paper documents. Moreover, citizens and businesses often do not know which e-services system they are supposed to use to resolve the given matter.

On top of this, while the digitalisation of public institutions to date has resulted in many large, complex systems and registers, some areas are still not computerised, requiring the construction and provision of central-level ICT solutions.

As many as 63 per cent of public institutions[23] still operate with a paper-based workflow, and

23 Information based on own research by NASK — National Research Institute: "Systemy klasy EZD w administracji publicznej — badanie samorządów" [EZD class systems in public administration — survey of local governments], March 2022; "Badanie potrzeb jednostek administracji rządowej w zakresie wdrożeń EZD", [Survey of the needs of government administration units regarding EDM implementations], October 2023;

many challenges are evident in the area of the digital transition of public institutions.

Some of these are systemic, making it impossible to tackle them at the level of individual institutions. This is the case, for example, with insufficient integration between public ICT systems, the lack of unified, standardised electronic tools for carrying out public tasks and the fact that some public registers are still maintained in paper form. The technology stack used by the public administration and the components of the service-oriented architecture are also not standardised. At the same time, the availability of customised, scalable infrastructure for public administration is low. Differing levels of competencies among officials and disparities in the financial potential of public institutions result in uneven levels of digitalisation. Meanwhile, with continued progress in the IT sector, it is necessary to keep adapting public ICT systems to modern solutions.

These measures will reduce the cost of process implementation and operation in public institutions, e.g. by introducing central procurement of public cloud services, which will enable user entities to acquire cloud services in a short timeframe with much less involvement from their officials.

Objective 1: Back-office processes in public administration are digitalised

What will make it possible to achieve the objective:

a) Implementing a unified way of describing and standardising processes and procedures for the administrative functioning of the back office of public administration units that support the main tasks related to the processing of cases for citizens, entrepreneurs and administration;

b) Automating and optimising the execution of administrative processes, using reference processes from the Administrative Processes Catalogue, data extracted via public ICT system APIs and artificial intelligence solutions, while maintaining supervision and the possibility of human intervention;

c) Obliging public entities to implement electronic document management using EDM systems. It will also be necessary to standardise the requirements for EDM systems and to provide public entities with support in implementing and maintaining them;

d) Amending office and archive regulations and monitoring the level of use of EMD systems in entities carrying out public tasks to reduce cases processed based on paper documents;

e) Developing and disseminating a free EDM application — EZD RP — and making the cloud-based EZD RP services available to state, central and local government administration bodies. Supporting public entities in the implementation and maintenance of as well as migration to the EZD RP system;

f) Legally empowering the EZD RP system and appointing an EZD Operator responsible for the development, free implementation and maintenance support of EZD RP provided for entities performing public tasks.

g) Adopting the “Policy for the implementation of EDM in the Republic of Poland”, setting out the planned scope of activities in the area of back-office digitalisation of public administration bodies until 2030.

What follows from this?

Communication within and between offices will be simplified and more effective, and the work of officials will be easier and faster.

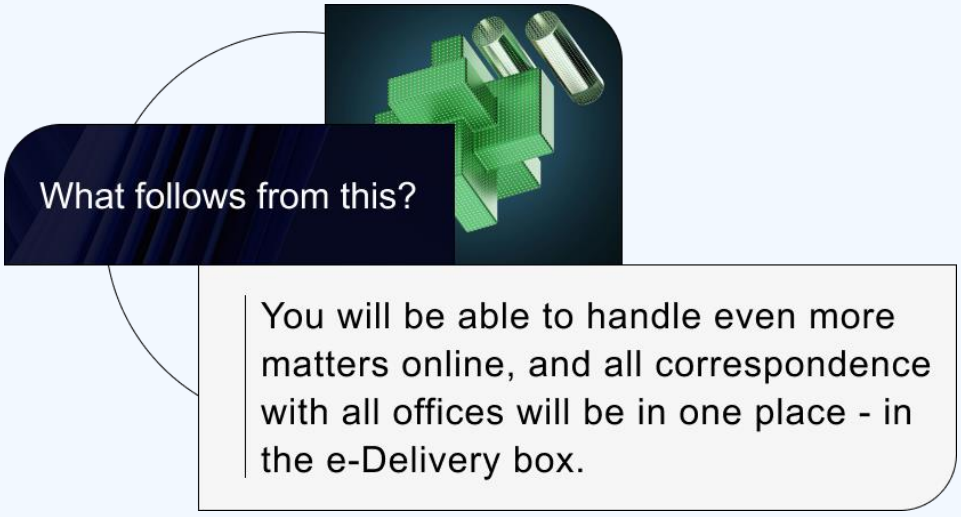
Objective 2: The legal environment favours the computerisation of public entities

What will make it possible to achieve the objective:

a) Adjusting the law to allow official matters to be handled using electronic communication, including the introduction of the digital-by-default principle in the Code of Administrative Procedure, simplification of administrative procedures and the introduction of electronic versions of documents. This will make it much easier for users to communicate with public administration bodies and other external entities;

b) Full implementation and dissemination of electronic delivery (e-Delivery) when dealing with both public and non-public entities;

c) Requiring the mandatory integration of e-services with e-Delivery, which will provide citizens with a single place with all their correspondence with the authorities, irrespective of the platform with e-services they have used.



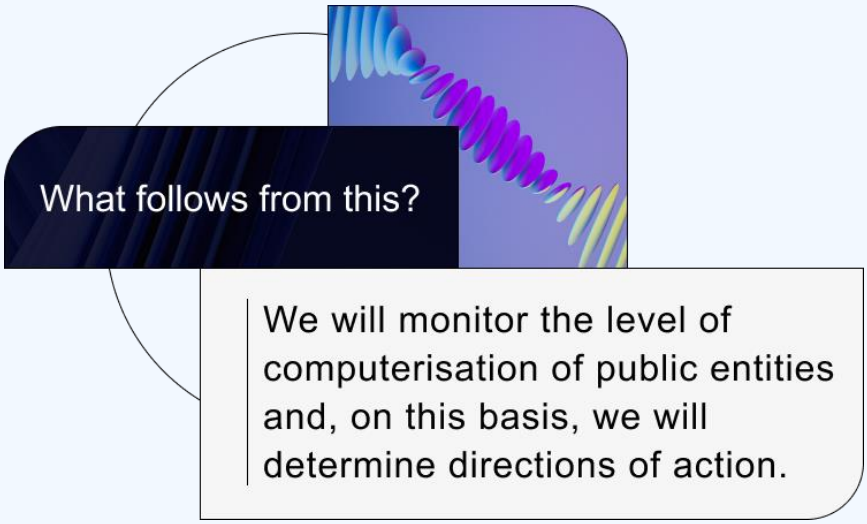
Objective 3: Monitoring the computerisation of public entities makes it possible to manage changes in this area more effectively

What will make it possible to achieve the objective:

a) Monitoring the implementation of horizontal solutions, including electronic identification means, data sharing platforms, e-payment systems and case repositories, in the ICT systems under construction or development, including those supporting the provision of public e-services;

b) Monitoring the progress and outcomes of ongoing public-use IT projects through the work of the Committee for Digitalisation;

c) Formulating conclusions from the monitoring of activities taken while computerising public entities and verifying the adopted lines of action on this basis.



Objective 4: The functioning of the justice system is improved through the use of e-services and modern technologies

What will make it possible to achieve the objective:

a) Providing advanced judiciary e-services supported by modern technologies, allowing electronic access to information and electronic handling of cases for citizens and entrepreneurs with improved transparency of proceedings;

b) Optimising procedural economics, taking into account the use of electronic documents, electronic procedural steps or conducting hearings and trials by videoconference;

c) Improving the comfort and work quality of judicial staff through automation;

d) Achieving a high level of interoperability of justice systems with national and international systems in their vicinity to improve digital judicial cooperation and data access;

e) Creating an AI tool to create transparent laws.

2.3 Systems and registers

Diagnosis – what is it like?

The systems and registers used by public administration bodies are not fully interoperable. Much of the data is unnecessarily collected multiple times, resulting in many barriers for public entities to find optimal solutions for public tasks. The numerous data inconsistencies in the various registers make it difficult to identify resources that are already available in the administration's systems and that public entities could use. Public institutions still have insufficient knowledge of the available data and reuse-ready solutions and how they can be employed when implementing new or enhancing existing IT solutions for administration. This results in an inadequate cooperation between public institutions. As such, public entities engage staff to carry out time-consuming searches and verification of data from multiple sources, with no guarantee of the quality of the data.

Data for public registers are largely provided and updated due to the obligations imposed on public entities. Maintaining high data quality is fraught with risk given the number of systems and registers in which entities have to enter data and the lack of communication and data exchange between systems and registers as regards the same data, as well as no solutions to automate these processes.

There is also an apparent shortage of data and tools for analysing the behaviour of users of systems and records used by public administration bodies, as well as the very products created for these bodies. It is essential to identify user needs and critical points in the solutions provided.

Public entities are obliged to share data from public registers with other entities under the conditions, in the manner, to the extent and within the time limit specified in the legislation based on which the given register is maintained. The lack of standards defining how procedures for accessing public registers should be carried out remains a significant challenge. There is no universally applicable and public API standard for ICT systems for handling public tasks, which would facilitate and accelerate the integration of digital solutions, contributing to increased interoperability, including the availability and quality of the state's information resources.

Objective 1: Public ICT systems and registers are interoperable

What will make it possible to achieve the objective:

a) Promoting and implementing architectural principles, standards, guidelines and recommendations, including those concerning the interoperability of ICT systems and public registers and the reusability of data and technical components, as basic principles for the creation and development of state information systems;

b) Developing and adopting a new regulation of the Council of Ministers on the National Interoperability Framework, minimum requirements for public registers, as well as minimum requirements for ICT systems used to carry out public tasks and data exchange with public entities, ensuring the widest and most convenient access to the state's information resources via Application Programming Interfaces, in machine-readable mode. Solutions that avoid over-involving their users and meet organisational, semantic and technological interoperability requirements should be built;

c) Ensuring that public ICT systems and registries comply with the National Interoperability Framework and the minimum requirements for ICT systems and public registries, and regularly reviewing standards and specifications to assess their ability to deliver interoperability;

d) Making the implementation and funding of public-use IT projects conditional on a positive assessment by the Committee for Digitalisation, also with regard to compliance with the digitalisation strategy and cybersecurity strategy, EU and national interoperability provisions, as well as minimum requirements for public ICT systems, public registers and data exchange with public entities;

e) Verifying the compliance of draft legislation with the digitalisation strategy and cybersecurity strategy, EU and national interoperability provisions, as well as minimum requirements for public ICT systems, public registers and data exchange with public entities, as part of the work of the Committee for Digitalisation;

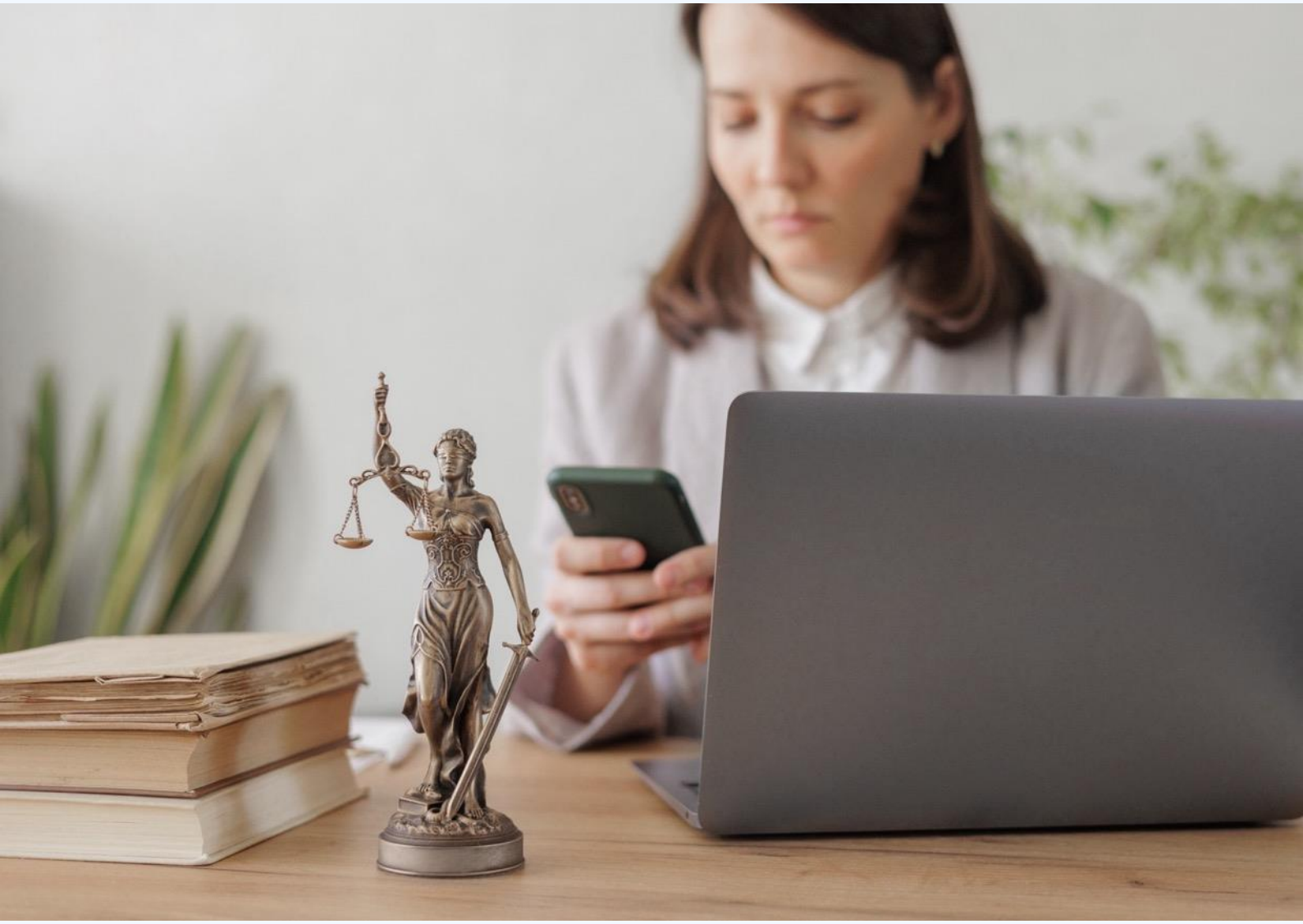
f) Conducting national interoperability assessments and cross-border interoperability assessments, including analysis of the impact of changes to public ICT systems and public registries on national and EU public entities;

g) Providing unique identifiers for state information resources within the interoperability layers (relating to such things as general laws, policy documents, public registers, public ICT systems) to ensure that such resources are unambiguously referenced in the documentation and that the links between them are unambiguously identified (including for the results of national and cross-border interoperability assessments);

h) Enhancing cross-border interoperability in line with the principles of the European Interoperability Framework:

- digital-by-default (i.e. providing services and data via digital channels by default),

- cross-border-by-default (i.e. accessible to all EU citizens),
- open-by-default (i.e. enabling re-use, participation/access and transparency).



Objective 2: High-quality data from public registers and ICT systems are made available in a secure and automated manner

What will make it possible to achieve the objective:

a) Strengthening in legislation the concept of reference public registries, i.e. public registries formally designated as trusted benchmarks for other public registries and ICT systems in a certain range of data;

b) Preparing, sharing and updating the reference public registers — “Public Administration Catalogues”, i.e. the Administrative Process Catalogue, the Case Catalogue, the Public Services Catalogue, the Document Model Catalogue (taking into account the functioning of the Central Repository of Electronic Document Templates) and the Public Registers Catalogue (taking into account the prepared interoperability repository);

c) Legally empowering public administration catalogues to automatically feed and exchange data and reduce the administrative burden on citizens, businesses and public administration bodies to provide and update this data, including the Catalogue of Public Entities (KPP) in terms of mandatory integration of the KPP with public administration systems that require data on public and non-public entities entrusted with or commissioned to carry out public tasks;

d) Imposing a legal obligation to maintain public registers solely using ICT systems and to apply uniform mechanisms to facilitate the validation and monitoring of the quality of the data contained in them;

e) Imposing a requirement to make data from public ICT systems and registers available via APIs;

f) Making available to the public a catalogue of public ICT system APIs, as well as information on the structure and meaning of data stored in all public registers, expanded to include information on dictionaries, classification schemes, taxonomies and code lists in public registers;

g) Creating a national data sharing platform as an organisational and technical solution, providing standardised mechanisms for accessing data processed in public registers.

What follows from this?

Dealing with matters in offices will be much faster and easier - while maintaining human supervision over the decision-making processes.

2.4 Digital identity

Diagnosis – what is it like?

For many years, Poland has had a successful federated digital identity model, in which it is up to the users to decide which means of identification they want to use in a public e-service. Today, users of the public eID system can take advantage of such tools as the trusted profile, the personal profile (the so-called eID) and the mObywatel [mCitizen] profile. The personal profile and mObywatel [mCitizen] profile can also be used by commercial providers of public e-services to authenticate users. Moreover, Polish citizens and residents can also make use of the so-called bank identification means available as part of the mojeID [myID] system.

Electronic signature services are also being developed in tandem with electronic identification. Free public solutions are currently available on the market: trusted signatures and personal signatures, as well as qualified electronic signatures provided on commercial terms by trust service providers.

However, the above models are subject to limitations that limit the widespread use of electronic identification means, electronic signatures and public e-services in general.

Electronic identification means can now only be used by natural persons, without distinguishing between the roles or contexts in which they authenticate online. There are no solutions that enable direct authentication of companies, institutions or other collective entities (legal persons), as well as natural persons acting as agents or representatives of legal persons (including public officials). Currently, additional confirmation and verification of the representation authorisation is required for these entities to be authenticated, leading to difficulties in the handling of administrative cases and increased waiting times.

As things stand at present, a natural person who acts in the name and on behalf of a legal person via a public e-service must, after authenticating, provide additional information and often an appropriate document confirming their representation authorisation, and this must be manually verified by the given authority. In cases where the public e-service in question is aimed directly at legal persons (e.g. commercial companies), the provider often has to either rely on unconventional methods to confirm the identity of legal persons or face the need to dedicate additional human resources to verify their representation authorisations.

The lack of adaptation of public e-services to serve legal entities is also noticeable with regard to the support of electronic signatures in situations where a letter must be signed by multiple attorneys, as required by the joint representation of the company. This is because there is no free, ready-made and easy-to-integrate tool that would enable multiple signatures to be placed easily within a public e-service.

Public administration also faces the problem of reliable verification of affixed electronic signatures from within the individual public e-services. Indeed, it is necessary to enable the

correct submission and verification of documents bearing not only a trusted signature but also a personal signature and a qualified electronic signature and to rectify errors that have arisen over the years of development of the electronic signature market.

Additionally, there are noticeable restrictions on the cross-border use of public e-services and this is despite the existing EU principle of mutual recognition of notified electronic identification means by Member States.

Poland has two notified electronic identification means: the trusted profile and the personal profile, but their practical use in other Member States' online services is negligible.

At the same time, it is worth noting that a PESEL number is required for the vast majority of Polish online services, which means that, in practice, the acceptability in Poland of notified identification means from other Member States is also at a very low level. Recognising these systemic practical problems in the mutual recognition of electronic identification means, the European Commission has proposed several solutions aimed at enhancing the security and freedom of electronic transactions within the digital single market, with the eIDAS 2.0 Regulation as the legal basis. It provides for the introduction of EU digital identity wallets by the end of 2026, allowing citizens to freely use public and commercial services online and to selectively and securely share information about themselves. The regulation pays particular attention to the voluntary nature of its use, as well as its accessibility and the protection of personal data and the privacy of wallet users. Qualified electronic signatures are to be available in the digital wallets for free for non-professional use, and the wallets themselves are to become highly secure electronic identification means.

To promote and accelerate the development of electronic identification systems while ensuring the security of their many users, it is necessary to continuously improve the cybersecurity of the identification means. Moreover, continued public education is needed regarding the possibility of handling official matters online, as well as the proper use of electronic identification means to prevent identity theft, personal data breaches, cyber attacks and other online dangers.

Objective 1: Legal entities can easily and quickly process official matters online

What will make it possible to achieve the objective:

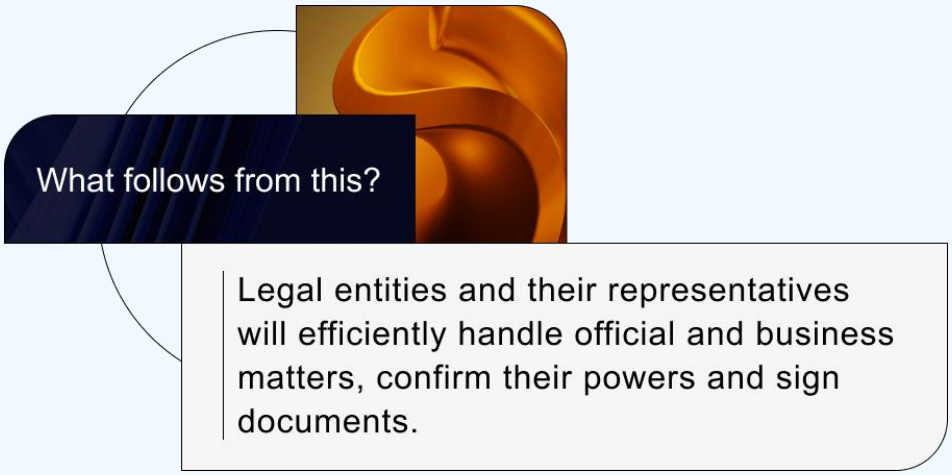
a) Establishing electronic identification means for legal persons and natural persons representing legal persons within the public electronic identification system;

b) Effective legal empowerment of electronic identification means for legal persons and natural persons representing legal persons so that they can be used for automated authentication in online public services, without the need for an official to manually verify each time that the power of attorney or representation authorisation submitted is correct and up-to-date;

c) Creating new or modifying existing public services so that they accept the issued electronic identification means for legal persons and natural persons representing legal persons;

d) Creating a tool to ensure that electronic signatures can be created easily and conveniently, regardless of document type and format, in the case of multi-person representation of a legal entity (“multi-signature”);

e) Making the EU Digital Identity Wallet available for use by legal entities.

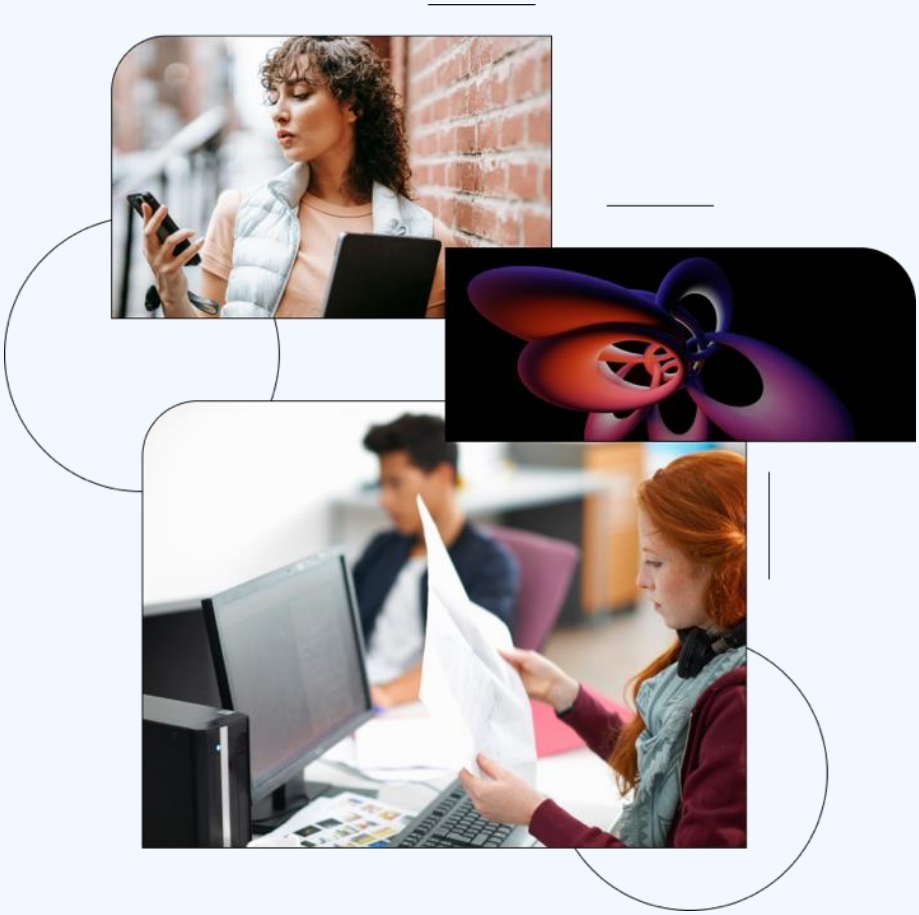


Objective 2: Electronic signatures are available and widely used, and their verification is simple and reliable regardless of document format and signature type

What will make it possible to achieve the objective:

a) Developing tools for signing and verifying documents with trusted signatures, personal signatures and qualified electronic signatures;

b) Disseminating information about the benefits of enabling electronic signatures to be created and verified in the systems of public offices, including those supporting the delivery of public e-services, through integration with the signature node component.



Objective 3: The electronic identification means are secure and convenient to use

What will make it possible to achieve the objective:

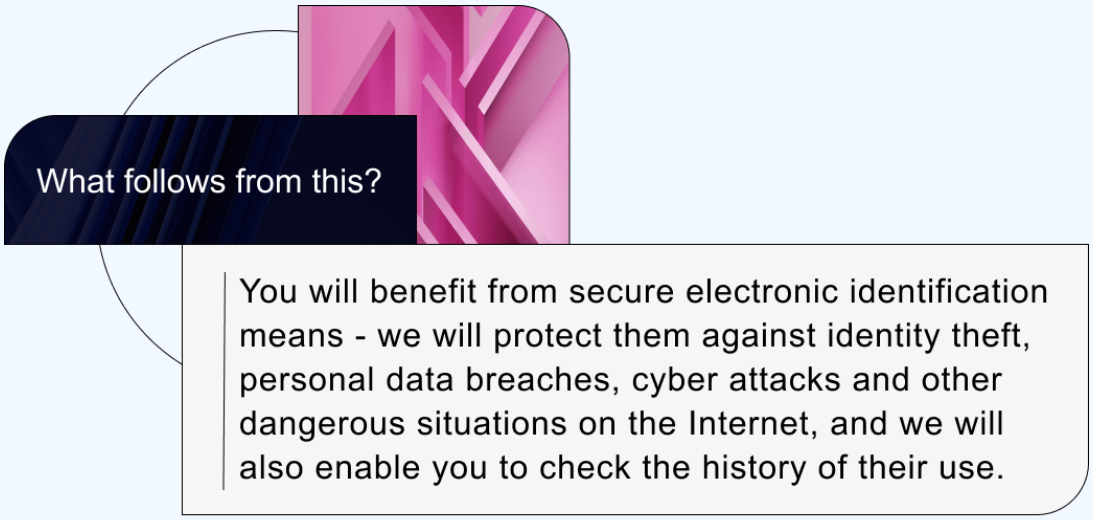
a) Developing and implementing a model for the widespread use of the personal ID card’s electronic layer and profession-related electronic certificates in ICT systems;

b) Adding a high-security means of identification — the EU Digital Identity Wallet — to the national node;

c) Adding a history of the use of electronic identification means to the national node;

d) Verifying whether the device from which the user logs in to ICT systems connected to the national node is on their list of trusted devices;

e) Implementing educational activities to enable the safe use of electronic identification means by the users.



Objective 4: Citizens and businesses use cross-border commercial and public services freely and safely

What will make it possible to achieve the objective:

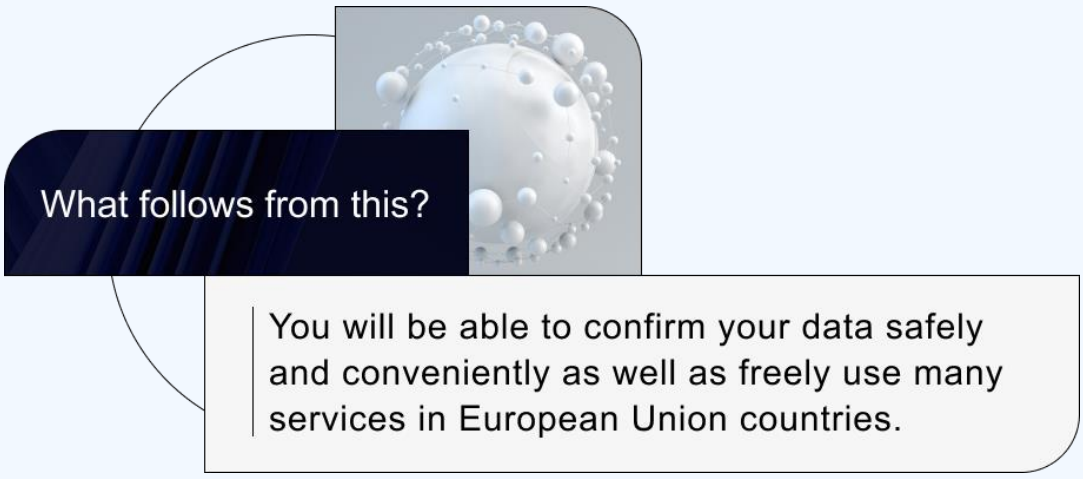
a) Establishing a mandatory register of entities wishing to provide their services based on the European Digital Identity Wallet;

b) Creating and making available the means of verification of certain user data in state registers to enable the issuing of electronic data certificates that are legally equivalent to traditional certificates and recognised abroad;

c) Making qualified electronic signatures available free of charge in the EU Digital Identity Wallet for individuals, at least for non-professional use;

d) Introducing procedures for unambiguous cross-border identity matching, in which a person's identifying data is mapped to an existing account belonging to the same person within a given public service;

e) Modifying national ICT systems, including those supporting the delivery of public e-services, to expand the range of the cross-border electronic identification means they recognise, including EU Digital Identity Wallets issued by other Member States, and facilitate the use of public e-services for users from other Member States (with service and support available in languages other than Polish).



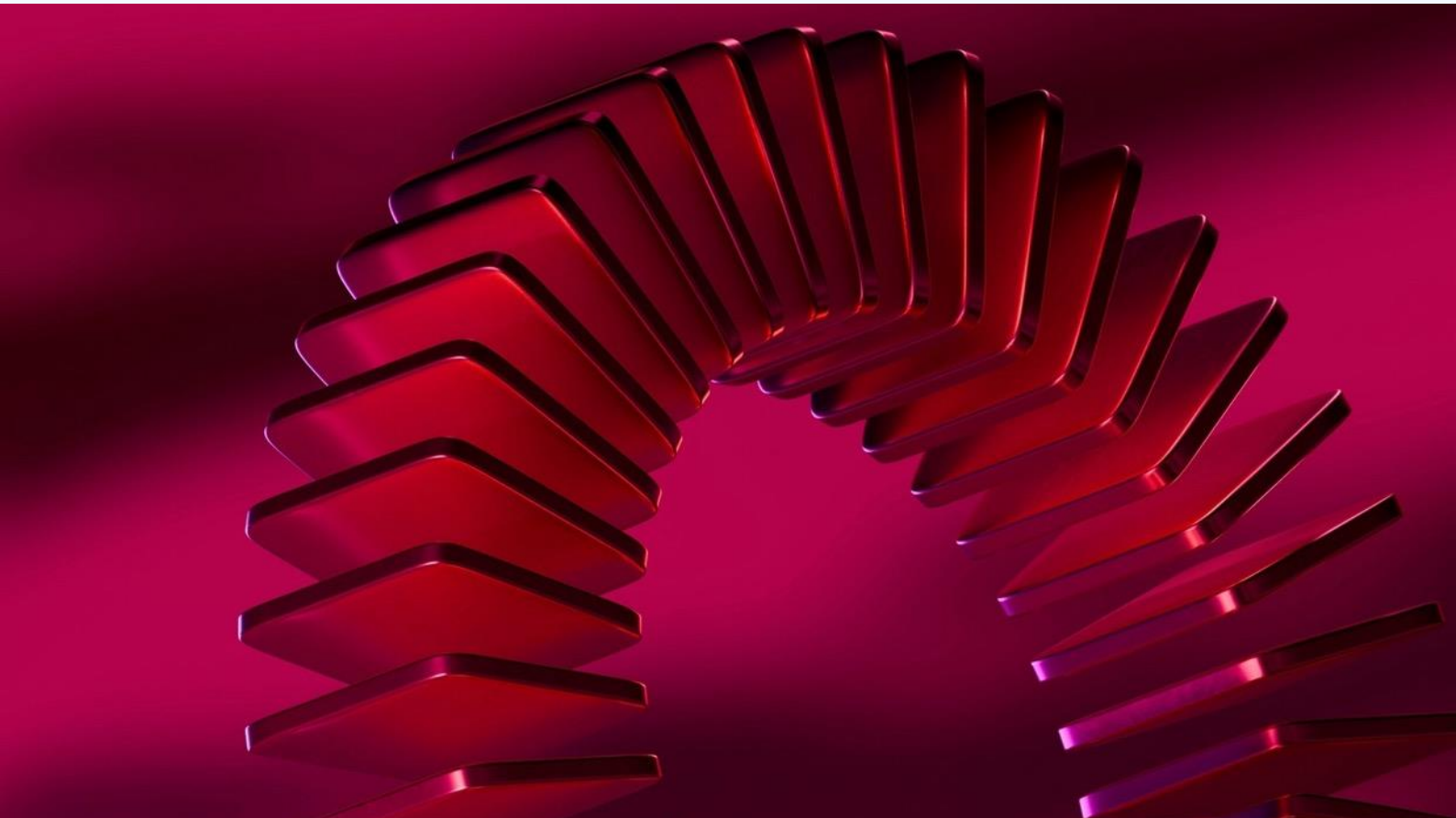
2.5 Cloud computing

Diagnosis – what is it like?

The cost of implementing processes and handling them in public institutions is high and the implementation of new public e-services and ICT systems is too slow. This, in turn, hampers the development of more mature and complex e-services. At the same time, attention must be paid to the risk of disruption of service continuity of public e-services and ICT systems, as well as data loss in the case of key public administration systems.

We recognise that the efficient and secure collection and processing of data on citizens, businesses and state operations is impossible in the long term without the use of cloud computing, primarily due to the scale (volume of this data).

However, it is necessary to adapt to the circumstances where the dominance of the commercial cloud services market by the digital giants results in a significant imbalance to the disadvantage of public sector institutions, which deal with large providers on their own. Further, the use of cloud technologies must take into account the issues of data sovereignty and its security from foreign intelligence services.



Objective 1: Government cloud infrastructure and data-driven services are developed

What will make it possible to achieve the objective:

a) Generating innovative cloud services dedicated to public administration as part of the Government Cloud Computing and the Local Government Cloud Computing programmes. These services will be delivered in Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS) models and, depending on the characteristics, will support the operation of IT systems, be used as building blocks for the creation of modern IT systems supporting the design and roll-out of cloud-based software, or be applied independently for the implementation of public services and processes operating across the relevant units;

b) Ensuring that any implemented services meet the highest security standards, comply with Polish and EU legal regulations and are based on the best global standards in accordance with the principles of the State Information Architecture;

c) Increasing the availability of scalable infrastructure services delivered in a cloud model, tailored to the evolving needs of administration bodies;

d) Simplifying the technology stack, service-oriented architecture components and the provision of architectural standards and predefined software modules to simplify and accelerate the implementation of new public e-services and IT systems;

e) Creating data embassies — out-of-country units for storing key data and information from state registers and systems and for ensuring the continuous operation of these registers and systems in the event of emergencies in the Republic of Poland.

Objective 2: The data processing infrastructure is modern and extensive

What will make it possible to achieve the objective:

a) Building and developing the National Data Processing Centre, including three modern, scalable and highly efficient processing centres to ensure service continuity for systems and security of public administration resources. The centres will be connected by fibre optics and will use green energy;

b) Ensuring service continuity for public e-services and ICT systems by securing public administration systems processing reference data against data loss, defining a guaranteed data recovery time in the event of a major breakdown, as well as providing standardised services to support business continuity plans, archives and backups, including for long-term data storage, data restoration and supporting the recovery of standard ICT system components;

c) Developing state-owned infrastructure for the provision of public e-services to enable efficient data processing, including the optimisation of the network of computing centres ensuring service continuity for e-services and the flow of data for their supporting ICT systems, e.g. for the healthcare and finance sectors, as well as courts.

Objective 3: Public entities are supported in the acquisition, implementation and use of IT systems and cloud-based solutions

What will make it possible to achieve the objective:

a) Conducting regular demand surveys for government and public cloud computing services in public administration;

b) Having a designated entity coordinate and run centralised procurement of public cloud services for the services most commonly used by public administration bodies, including entering into framework agreements to expand the range of cloud services available to public administration bodies after simplified implementation proceedings;

c) Supporting the secure procurement of cloud services as part of procurement proceedings thanks to the Cloud Services Provision System (ZUCH). The system will provide support for the full Public Procurement Law purchasing process through integration with e-Zamówienia [e-Procurement], with implementation proceedings and the signing of contracts and agreements handled directly in the ZUCH system;

d) Supporting competitiveness in the sourcing and discovery of cloud services by directly integrating the ZUCH system with cloud service management portals for public and private clouds to support service comparison, commissioning, reporting and billing processes, thereby ensuring independence from specific service providers;

e) Providing the Business Cloud Service Management Platform in the ZUCH system for simple management of services from different cloud service providers;

f) Providing in the ZUCH system, for new innovative cloud services within government cloud computing resources, the options for configuring, managing and billing these cloud services;

g) Establishing a Cloud Academy where administrative units can gain knowledge about secure solutions and good practices in setting up and maintaining cloud-based infrastructure solutions.

What follows from this?

All cloud services for public administration will be ordered centrally, which will increase the security and transparency of this process, as well as reduce administration costs.

2.6 Open data and data sharing

Diagnosis – what is it like?

Data is of high importance in the economy and society. Generated by computers, smartphones and appliances equipped with numerous sensors, they drive economic development, competitiveness, innovation and social progress. According to the European Commission, the direct economic value of public sector information was calculated in the impact assessment to be EUR 52 billion as of 2018 and is estimated to increase to EUR 149 billion[24] by 2030. Conclusions from the monitoring system of the Data Opening Programme for 2021–2027[25] indicate such things as the need to increase the amount of data at dane.gov.pl and objects at kronika.gov.pl, to take care of data quality and increase the scope of data, to undertake a cyclical and long-term effort to improve the knowledge and skills of administrative staff in opening and managing data, as well as to implement actions promoting the policy of open access to data and actions informing about the possibility of making data available at dane.gov.pl and the benefits of doing so.

Moreover, given the dynamic development of artificial intelligence, which is based on good-quality data, measures are needed to improve the quality of the resources published at dane.gov.pl, including those for machine learning.

The evaluation of the Act on open data and the re-use of public sector information[26] has identified areas requiring intensified non-legislative action. These include the need to strengthen the network of open data officers, further development of the dane.gov.pl portal and undertaking awareness, educational and promotional activities aimed at increasing knowledge about the process of opening up and re-using public data.

At the EU level, the European Commission is taking action to increase the exchange and sharing of data between different actors, i.e. consumers, businesses and public sector entities. A consequence of the adoption of EU legislation is the need for Poland, as a Member State, to ensure the proper application or implementation of EU data instruments. Constant monitoring of national and EU regulations is crucial to adapt to the changing needs of data users.

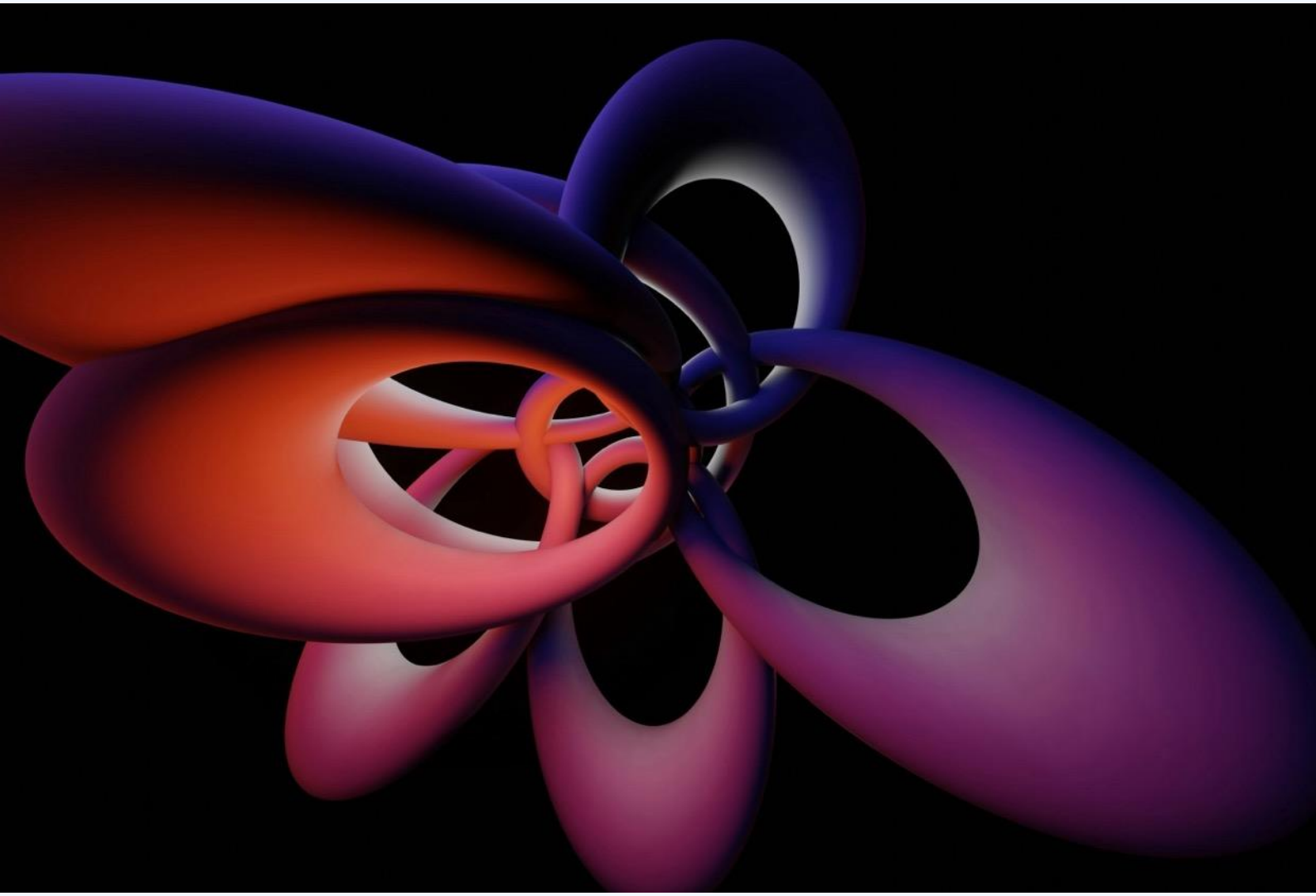
---

24 Open data maturity report 2023, https://data.europa.eu/en/publications/open-data-maturity/2023, za https://digital-strategy.ec.europa.eu/en/library/impact-assessment-review-directive-200398ec-reuse-public-sector-information.

25Resolution No. 28 of the Council of Ministers of 18 February 2021 on the Open Data Programme for 2021–2027 (M.P., item 290).

26Act of 11 August 2021 on open data and re-use of public sector information (Dz.U. /Journal of Laws/ of 2023, items 1524).

We have identified the need to stimulate Poland’s emerging data market, which is to be subject to the newly adopted European regulatory framework (in particular, the data intermediary sector and data altruism organisations). The measures we are taking will be aimed at supporting the exchange of data between participants in a market that is not yet fully developed and which needs to adapt quickly to the regulations imposed on it. In particular, it is vital to include Polish actors from the public sector and beyond in the emerging Common European Data Spaces. Simultaneously, it is necessary to create conditions for the emergence — based on the possibilities offered by the new EU regulations we are implementing — of smaller equivalents of European Data Spaces, which could benefit from the potential of the data intermediaries and data altruism organisations that are gradually being set up.



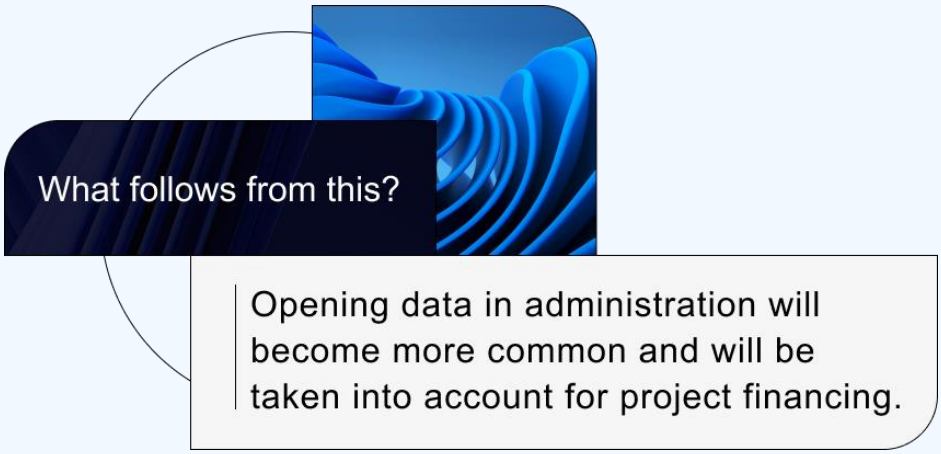
Objective 1: Public administration deliberately works towards data openness

What will make it possible to achieve the objective:

a) Making the implementation and funding of IT projects conditional on a positive assessment by the Committee for Digitalisation in terms of aspects like compliance with data creation rules, etc.;

b) Promoting the principles of data by design and openness by default in processes and projects implemented by public administration bodies, including IT-related ones, as well as including data sharing through APIs;

c) Expanding the network of open data officers at multiple institutional levels.



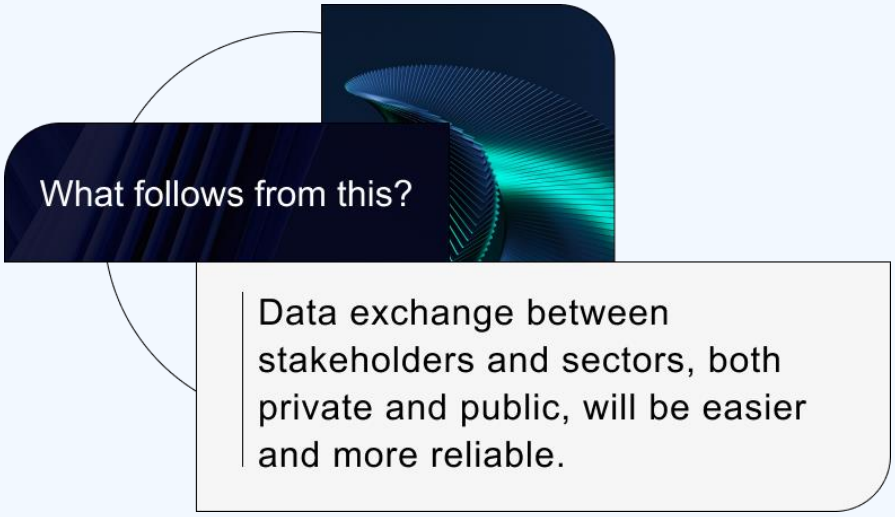
Objective 2: The legal environment in the area of data management fosters the development of a data-sharing ecosystem

What will make it possible to achieve the objective:

a) Establishing a legislative environment that is conducive to altruistic data sharing and data exchange in B2B and B2G relationships, (including the adoption of national legislation to apply the Data Governance Act and the Data Act);

b) Participating in the development of further legislation making the EU common data market a reality and in the revision of EU legislation according to the needs and course of development of the national data market;

c) Optimising the provisions of the Open Data Act towards facilitating and expanding the re-use of public data.



Objective 3: Access to high-quality data for reuse and machine learning is widespread

What will make it possible to achieve the objective:

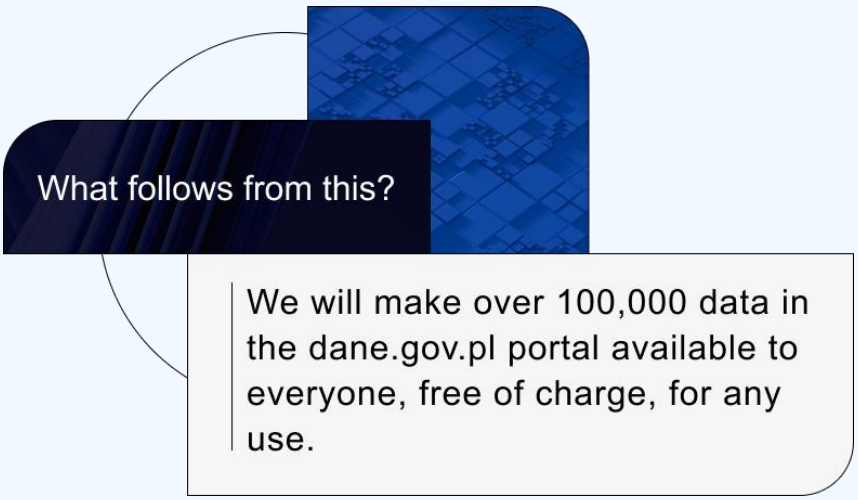
a) Research to determine the level of supply and demand in relation to data;

b) Working with data holders to increase the volume of data[27] at dane.gov.pl, including linked and dynamic data and particularly data accessible via APIs, concerning such areas as housing, environmental pollution, energy sector;

c) Developing the trusted dane.gov.pl portal through the portal's user communication, data quality and usability and statistics modules;

d) Mechanisms to improve data quality at data.gov.pl;

e) Identifying high-value data and, through public partnerships, building APIs to share it.



27In the context of the dane.gov.pl portal, data is construed as any content or part thereof, irrespective of its form, particularly in paper, electronic, audio, visual or audiovisual form, which is held by an obliged entity in accordance with the Act on open data and the re-use of public sector information or held and produced by an entity other than the obliged entity. A dataset is construed to be a set of data on a specific topic.

Objective 4: Access to science and culture resources through the kronika.gov.pl portal is easier

What will make it possible to achieve the objective:

a) Researching the level of supply and demand for science and culture resources;

b) Working with data stakeholders to increase the volume of resources on kronika.gov.pl for reuse and preservation in the back-up repository;

c) Developing the trusted kronika.gov.pl portal as a digital resource space for Polish science and culture;

d) Building an API linking the kronika.gov.pl portal and institutions publishing science and culture data to facilitate the integration of resources published on non-linked websites within an information hub such as kronika.gov.pl;

e) Running awareness and promotional activities on the re-use of science and culture data;

f) Working with the academic community to link the relevant digital cultural objects with published scientific research and creating a catalogue of scientific papers based on the resources published at kronika.gov.pl.

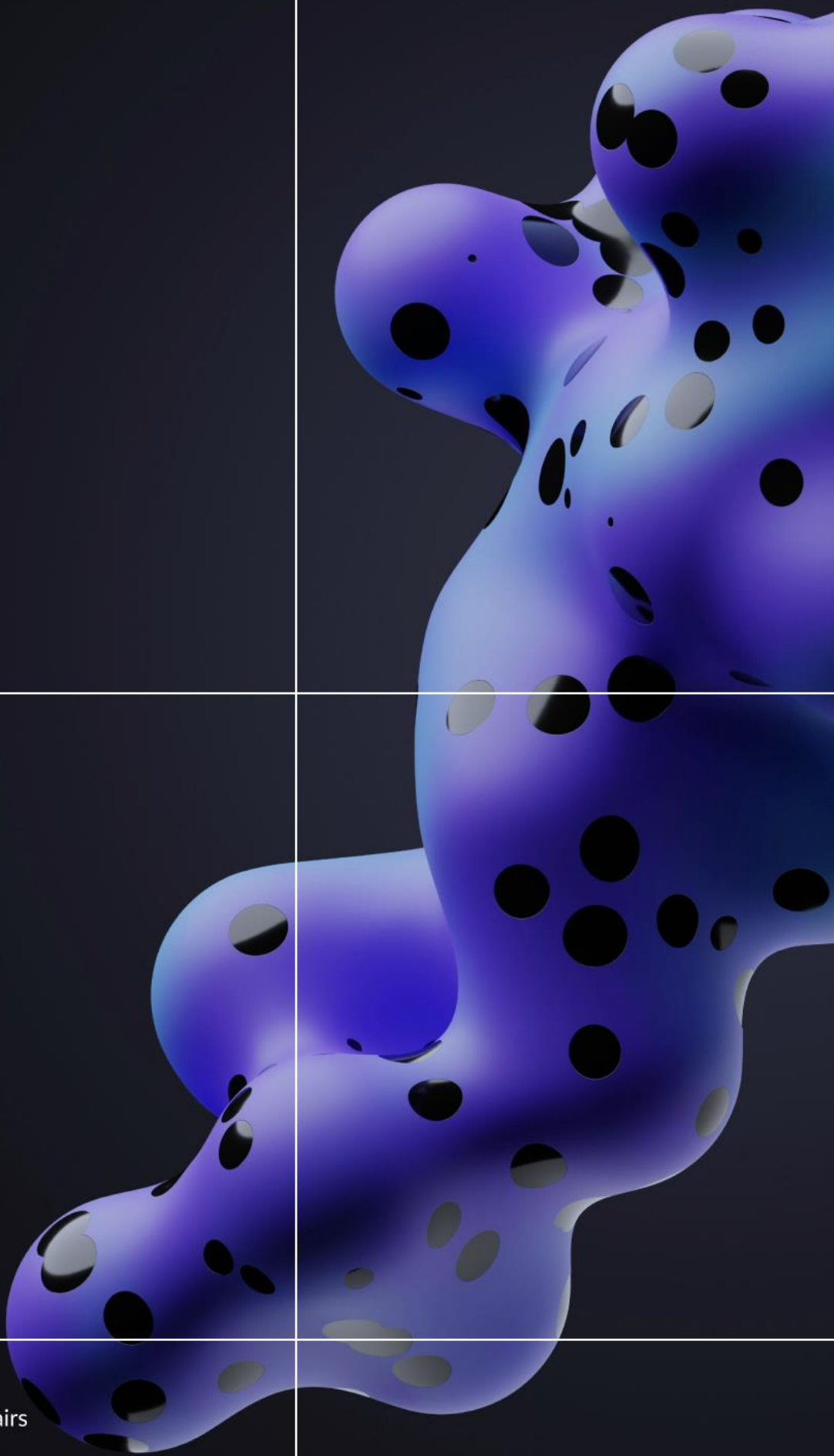
Objective 5: Poland’s data exchange market is mature

What will make it possible to achieve the objective:

a) Recommending systemic funding for projects that support the development of data brokering and data altruism services within the new EU financial perspective;

b) Stimulating data exchange with and between stakeholders outside the administration.

People



Ministry of Digital Affairs
Republic of Poland

We Make the Future

People

3.1 Secure digital space

Diagnosis – what is it like?

The main factors influencing the public's attitude towards e-governance include tool usability, social aspects (the conduct of others), potential risks and equipment and skills already available to the citizens. Yet, trust is a particularly important factor affecting the use of public e-services, among other things.

For this reason, the state is obliged to strive to build security for the digital sphere in the broadest sense — to take care of user security, to respect the principles of the democratic rule of law and citizens' rights and to protect the online information space.

Protecting the security of citizens and their data, market competition and building technological sovereignty should be considered crucial. It is therefore essential to follow the regulations and digital standards protecting citizens' rights, which are established in the European Union. Particularly relevant is the national implementation of the EU's 2022 Declaration on Digital Rights and Principles in the Digital Decade. It aims to support the digital transition in the EU, including by making it human-centred, as well as considering solidarity and inclusion, freedom of choice and safety and security. The assumption that the protection of citizens is a priority must be reflected by, among other things, the provision of adequate institutional resources for the implementation and application of national and EU legislative acts in this area.

Digital civil rights are exercised through the individual's relationship with institutions of power and the users' relationship with digital service providers. Threats in the context of the latter include unwarranted moderation of content by platforms, ambiguities in the rules and standards of digital communities, the so-called deceptive interface patterns, lack of transparency of algorithms and no accountability for the platforms' actions. These problems are linked to a business model based on the competition for user engagement, creating risks for privacy and the use of personal data. Failure to respond to these phenomena results in long-term and growing social polarisation, which undermines both the democratic order and the information order of the state.

Fundamental rights in the digital sphere should also be examined from the perspective of the impact of the digital sphere on employees.

The new trends of process automation and digitalisation in companies affect both blue- and white-collar workers. Digital tools enable extensive surveillance of employees, which can involve violations of their privacy and well-being. The rise in popularity of remote working has enabled flexible time arrangements and has benefited many employees and employers. At the same time, however, it generates risks related to the expectation of continuous availability of employees and makes it difficult to separate work and private life. We are also seeing the continued intensive development of unconventional business models, spearheaded by the sharing economy. On the one hand, it has opened up new opportunities for consumers, entrepreneurs and workers, but on the other, it has destabilised working conditions and deprived those working via apps of their basic rights. Thus, shifting responsibility and operating costs to platform workers — expected to reach 43 million[28] in the EU — leads to increased job insecurity and the spread of the precariat phenomenon.

Finally, ensuring comprehensive security of the digital sphere requires an effective fight against disinformation. It is construed as untrue or misleading (manipulated) information, created, presented and disseminated to obtain economic benefits or mislead the public, which may cause public harm. It is vital to distinguish between two types of disinformation — external and internal (used by specific actors/groups against citizens of the same state). Disinformation as an organised activity is strategic and long-term in nature.

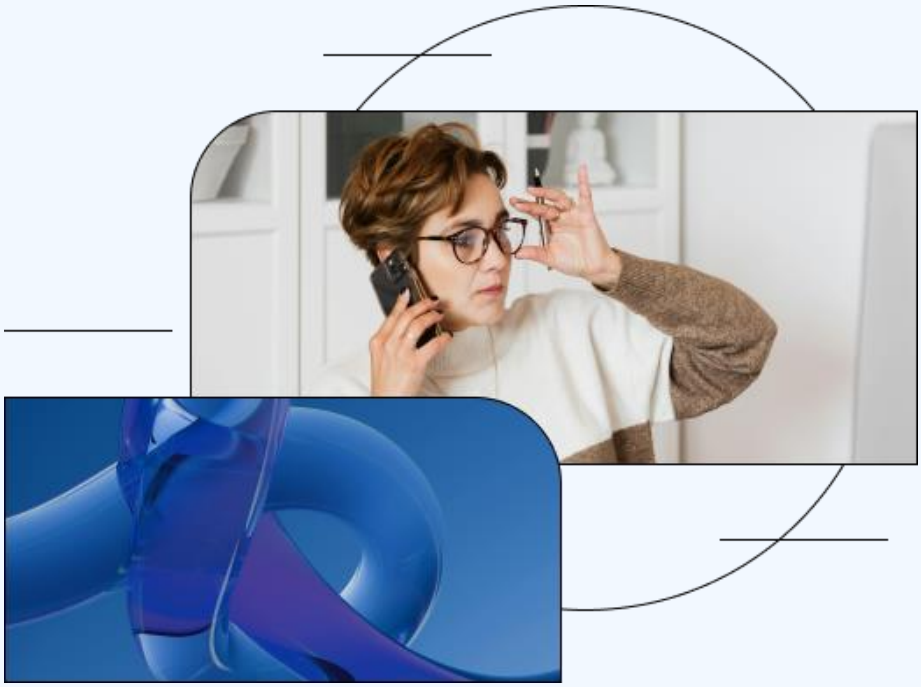
Internal disinformation is carried out to build social, political or financial capital. On the other hand, external actors use disinformation for such purposes as destabilising a country's social and political situation and stimulating social polarisation. Poland's most active adversaries are state actors waging an information war against it, including Russia and Belarus. Their activities include complex disinformation efforts, advanced influence operations, intelligence and subversion actions, as well as physical attacks. The disinformation messages promoted by antagonistic states serve their internal goals (including increasing the support for leaders) on the one hand, and external goals (such as stimulating anti-NATO, anti-EU, anti-American and anti-Ukrainian sentiment) on the other.

In Poland, anti-disinformation efforts are handled by several institutions, including NASK — National Research Institute, the Ministry of Foreign Affairs, the National Broadcasting Council (media education), the Government Centre for Security (threat analysis, including disinformation), the relevant services (including the Military Counterintelligence Service and the Internal Security Agency) and the commission for investigating Russian and Belarusian influence. In line with the EU Digital Services Act, the President of the Office of Electronic Communications will also be involved — as the digital services coordinator. The multitude of institutions involved in handling disinformation translates into one of the main challenges in this area — inadequate coordination and communication, as well as inconsistent operating methods.

28 https://www.consilium.europa.eu/pl/policies/platform-work-eu/

Other challenges include:

- Development of new technologies (including AI) to enable faster and more effective creation of disinformation content;
- Ineffective cooperation with social media platforms in the process of identifying and taking down disinformation content as well as the accounts spreading it (including bots);
- The need for increased efforts to comprehensively analyse disinformation campaigns;
- Low public awareness and the need for competence development in media education, critical thinking and information security;
- Scattered and insufficient funding for NGOs working against disinformation;
- Lack of established strategies at the central and local government levels for responding to disinformation and for crisis communication.



Objective 1: The institutional and regulatory environment in the digital sphere supports the protection of fundamental rights

What will make it possible to achieve the objective:

a) Fostering a strong institutional environment based on regulations designed to ensure respect for the recognised values and rights of individual Internet users by providing those responsible for enforcing them with technical, personnel and financial resources;

b) Promoting a fundamental rights-compatible design, development, implementation and use of technological solutions by applying the principle of “ethics by design”.

c) Conducting a Fundamental Rights Impact Assessment (FRIA) for citizens' rights in terms of the use of automated decision-making and AI systems in state administration

d) Creating a model form for assessing the ethical aspects of AIs used by the state;

e) Developing national solutions on the presumption of an employment relationship in the sharing economy and promptly transposing the Platform Work Directive into Polish law;

f) Ongoing analysis of the impact of digital technologies, especially AI, on the labour market;

g) Ensuring effective compliance with labour law and the timeliness of public policies in relation to a dynamically changing labour market influenced by digitalisation and the trends it has triggered. This includes protecting employees from the risk related to constant availability (adopting the right to disconnect), non-transparent “scoring” and prejudice-based employee assessments (implementing regulations related to the use of AI at work) and digital surveillance (enforcing privacy laws);

h) Actively advocating at home and in the EU for the implementation of solutions, particularly legislative ones, for the protection of the right to privacy, the protection of personal data and the right to disconnect.

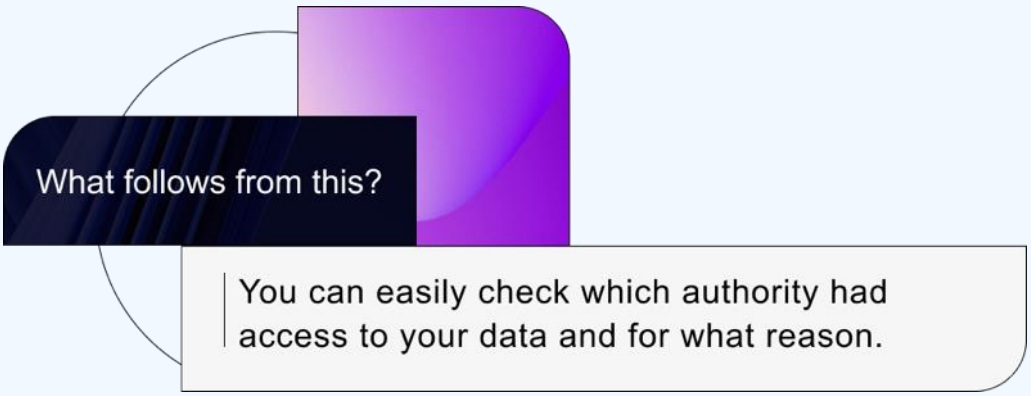
Objective 2: The public digital space is user-friendly and inspires confidence in citizens

What will make it possible to achieve the objective:

a) Implementing in practice the European Declaration of Digital Rights and Principles in the Digital Decade in all state/citizen interactions in the digital sphere;

b) Building trust in the e-state by increasingly involving citizens in the creation of digital law (including using digital tools) and digital public services, as well as closing the gap in the digitalisation of documents relevant to the public (publishing documents, e.g. MPs' property statements, in a digitally accessible, machine-readable format) and aiming for greater transparency in the processing of citizen cases and data;

c) Designing solutions to enable citizens to access information on which authority accessed their data and for what purpose — using "privacy by design" and "security by design" mechanisms, taking into account the GDPR rules, as well as introducing the principle of automatic detection of data operations to enable citizens to monitor their data and report breaches, and using data request history analysis to catch risks.



Objective 3: The activities of the anti-disinformation units are coordinated

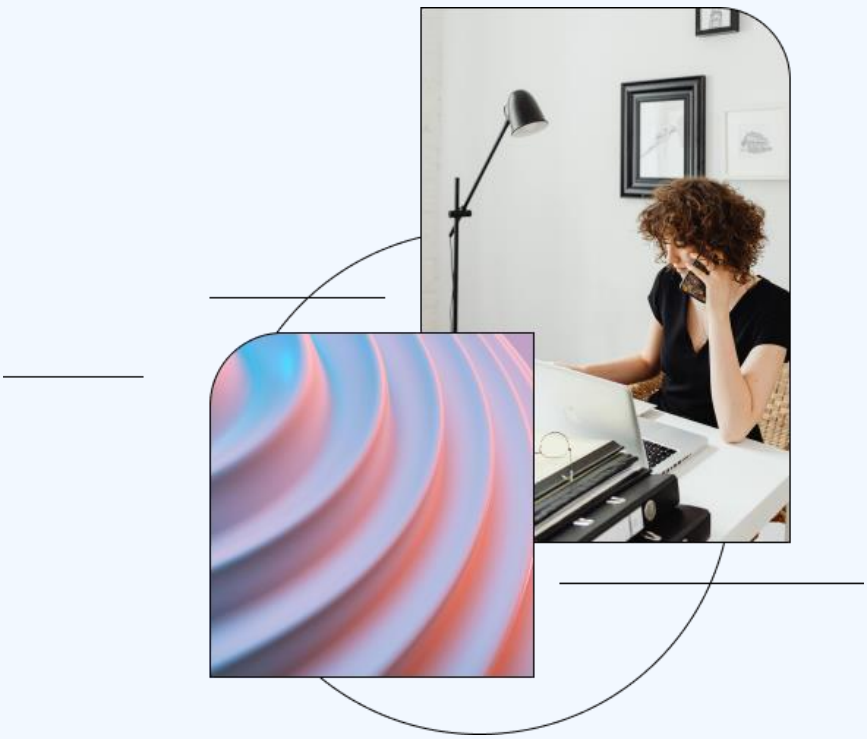
What will make it possible to achieve the objective:

a) Establishing a body responsible for overseeing and integrating the activities of the various actors involved in countering disinformation;

b) Ensuring a clear communication structure and information flow between all units involved through regular meetings and data exchange platforms;

c) Developing uniform or similar operational procedures and standards for use by all units involved in countering disinformation;

d) Providing advanced technology tools and training for unit staff.



Objective 4: The level of public awareness of disinformation is steadily increasing

What will make it possible to achieve the objective:

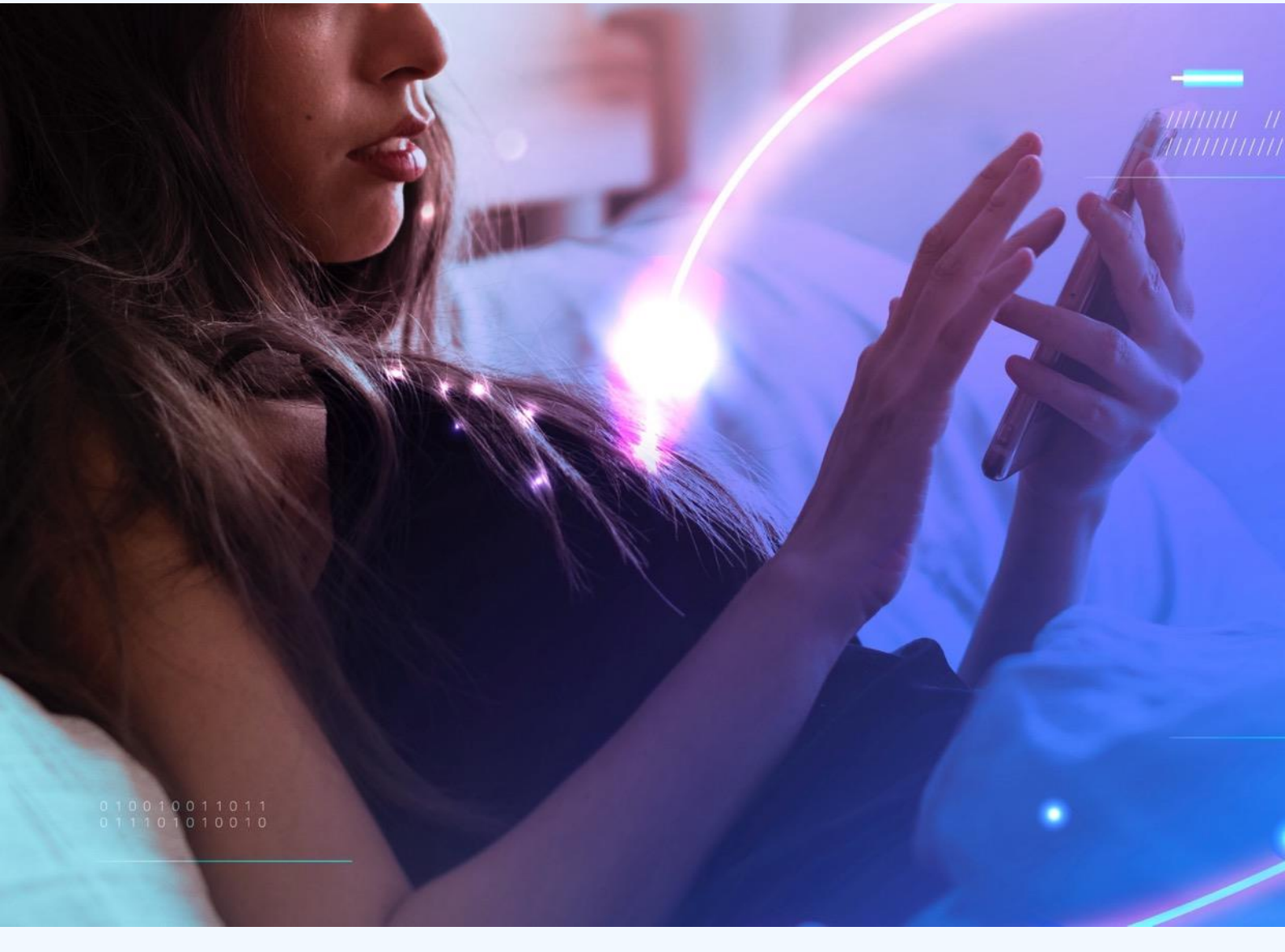
a) Implementing awareness and social campaigns on disinformation and responsible media use;

b) Conducting educational activities for selected community groups;

c) Running dedicated information campaigns in connection with key events, e.g. elections;

d) Developing interactive e-learning platforms and multimedia teaching resources;

e) Organising discussions, debates and workshops on ethical aspects of media activities, such as privacy, data protection, copyright and responsibility for published content.



Objective 5: Social media platforms promptly remove harmful content

What will make it possible to achieve the objective:

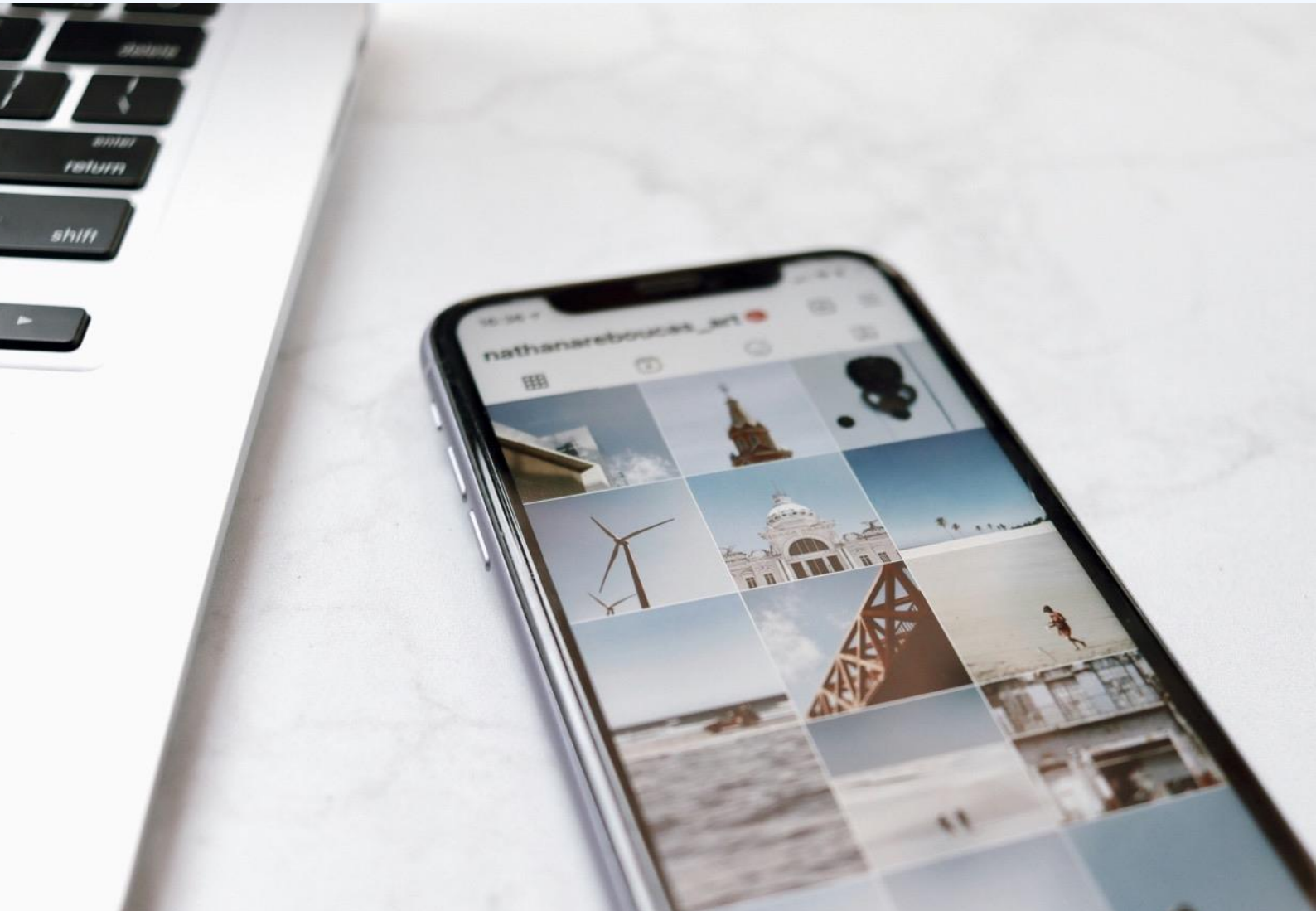
a) Constantly monitoring the content on social media platforms;

b) Establishing appropriate information exchange pathways for trusted whistleblowers (under the Digital Services Act);

c) Establishing clear and transparent criteria leading to trusted whistleblower status. Trusted whistleblowers should have specific expertise and competencies in detecting, identifying and reporting illegal content and be independent of online platforms;

d) Implementing effective mechanisms to sanction social media platforms and IT service providers for failing to take targeted action against disinformation;

e) Establishing a framework for collaboration with the private sector, particularly with social media platforms.



3.2 Digital health

Diagnosis – what is it like?

A comprehensive diagnosis of the relationship between technology and health requires seeing two, often contradictory, dimensions of this relationship. The first dimension is the

negative impact of some aspects of digital technology use on citizens' mental health.

This is due to such factors as the addictive mechanism of social media platforms and the harmful nature of some of the content that appears there, which is characterised by sensationalism, unrealistic beauty standards and a glorification of violence. A particularly clear problem, not least in view of the inadequacy of age verification mechanisms, is the widespread access by children to content that is harmful to their development and promotes inappropriate role models. Online abuse of minors is also a significant problem. The state is obliged to address these challenges, including through international cooperation, which the nature of these challenges often requires.

The second aspect of the relationship between technology and health is more positive.

It concerns the enormous opportunities that the digitalisation of this sphere offers in terms of increasing the effectiveness of treatment and prevention.

An analysis of the situation surrounding the digitalisation of Poland's healthcare sector reveals an advanced but still maturing e-health infrastructure. According to the EU report on the state of digital health in the last decade, Poland ranks 6th and 5th, respectively, in terms of access to Electronic Health Records (EHR) and access to technology among the 27 EU29 countries, ranking below the EU average only in terms of the categories of data available to the patient.

The cornerstone elements of Poland's digital health are the e-Health Platform (P1) and various registers, domain systems and regional platforms. The P1 platform serves as a hub for digital health services, offering e-prescriptions, electronic referrals and EHR access, among other things. The development of this platform has increased the use of the Internet Patient Account (IKP), which is now used by more than 18 million Poles. It is also vital to highlight the successful roll-out of the e-prescription system, which allowed 2 billion e-prescriptions to be issued by April 2024.30 However, the e-health services that have been

29 https://op.europa.eu/en/publication-detail/-/publication/78938111-461e-11ee-92e3-01aa75ed71a1/language-en

30 https://pacjent.gov.pl/aktualnosc/48-proc-polakow-uzywa-ikp

introduced are predominantly a digital reflection of traditional processes and do not exploit the full potential of digitalisation.

At the local level, as per the e-Health Centre's survey of the extent of computerisation of healthcare entities, more than 84% of hospitals operated a basic EHR system, 78% implemented EHR indexing in P1 and more than a third were exchanging EHR data with other entities by late 2023.[31] The percentage is significantly lower for non-hospital healthcare entities.

A prerequisite for the development of digital services in healthcare is to ensure data security.

Despite the measures taken by the e-Health Centre and the Ministry of Health, cybersecurity at the local level remains unsatisfactory. According to the e-Health Centre's survey data, as of April 2022, 81% of healthcare entities did not have a vulnerability management plan, 68% lacked offsite backups and 86% of entity managers had not received cybersecurity training[32].

The siloed nature of data, which does not provide a complete picture of a patient's health, and the lack of democratic rules for accessing data for research and development (R&D) purposes are also significant problems for e-health development. Unclear rules for access to data already collected, including doubts about the legal basis for processing health data for R&D purposes and uncertainty about the adequacy of the data collected in central registers,[33] are slowing down medical development.

The proportion of healthcare entities using new technologies such as artificial intelligence is increasing and now stands at almost 7% for hospitals.[34] There is also growing interest in and awareness of the benefits of using AI in medicine.

31 https://cez.gov.pl/sites/default/files/paragraph.attachments.field_attachments/2023-12/vii_edycja_raport_2023.pdf

32 e-Health Centre data

33 https://www.mdpi.com/1660-4601/19/19/11964

34 https://cez.gov.pl/sites/default/files/paragraph.attachments.field_attachments/2023-12/vii_edycja_raport_2023.pdf

Objective 1: The state works to minimise the negative impact of digital technologies on mental wellbeing

What will make it possible to achieve the objective:

a) Launching a programme to fund research into the impact of digital technologies on the mental health and psychosocial development of citizens, particularly children and young people.

b) Implementing social and awareness campaigns on digital hygiene and the rights of citizens (especially children) in the digital space.

c) Implementing measures to prevent online sexual exploitation of minors;

d) Introducing standards for the protection of minors in digital products and services. These should:

- Rely on an established catalogue of harmful content;
- Require digital product and service providers to prevent content listed in the catalogue from appearing in their products and services, or at least intervene when it does;
- Assume the use of tools to effectively verify the users' age while maintaining anonymity and protecting their personal data;
- Exclude solutions that lead to loss of control over screen time;
- Introduce solutions to protect the image of children and young people online.

Objective 2: Electronic Health Records are universal, complete and maintained in a manner that enables the exchange of records between healthcare providers

What will make it possible to achieve the objective:

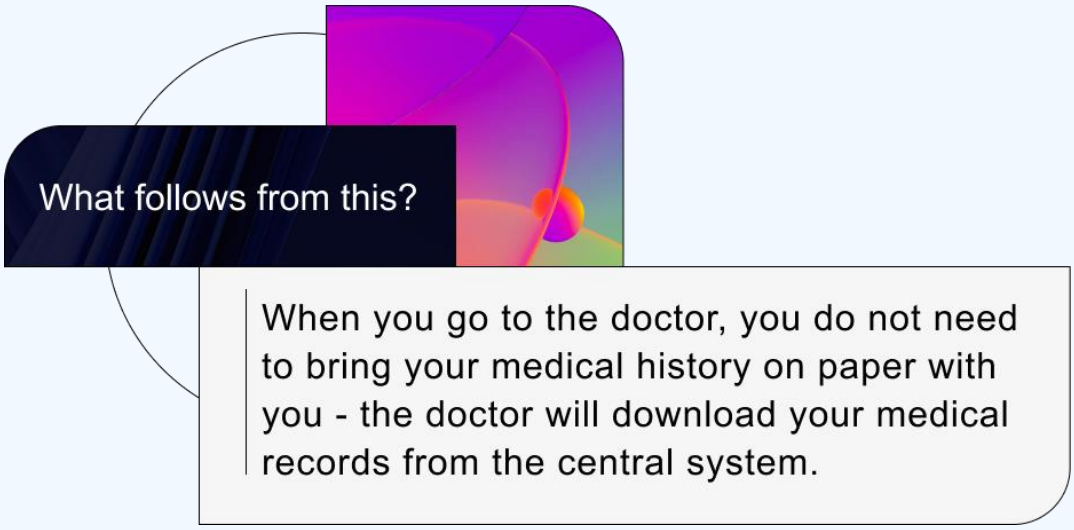
a) Continuing to develop e-health systems in the P1 system;

b) Implementing a financial incentive system for entities that maintain an EHR system with indexing in P1 and the possibility to exchange records with another entity;

c) Enabling data collected in the P1 system to be enriched with data recorded by wearable and implantable devices;

d) Streamlining the way medical records are kept, especially in areas where data are not validated;

e) Promoting interoperability between healthcare IT systems and the quality of data collected.



Objective 3: A large reservoir of reliable health data is available, with the rules for accessing it for R&D purposes being transparent, democratic and efficient

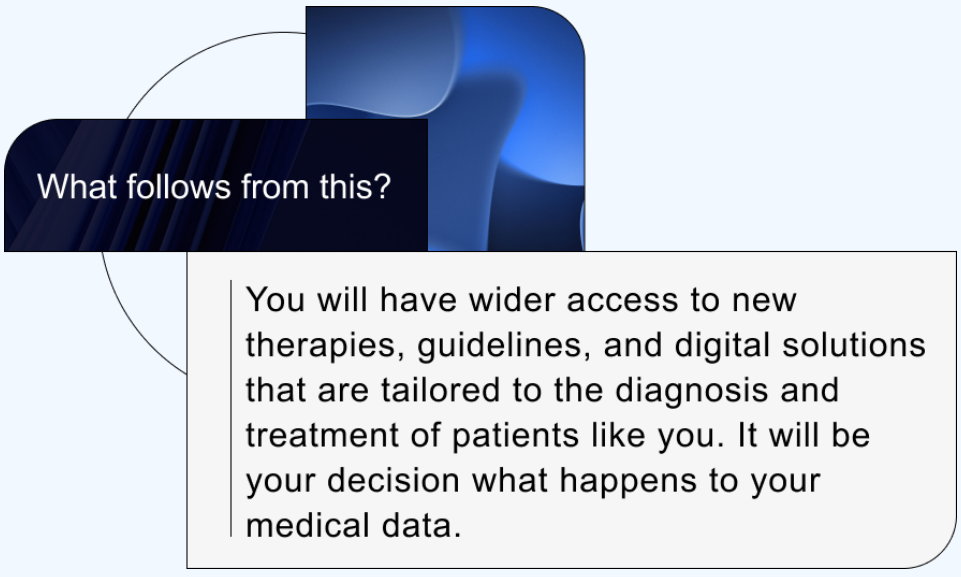
What will make it possible to achieve the objective:

a) Implementing operational activities in connection with the entry into force of the European Health Data Space and the Data Governance Act;

b) Promoting medical data donation (altruism) among patients;

c) Regulating the rules of access to microdata and statistical data for R&D purposes, including standardising the rules of access to data in public registers and medical records held by healthcare entities;

d) Establishing a standard for anonymisation and pseudonymisation of medical data.



Objective 4: Artificial intelligence and other new digital technologies are being used safely and effectively to improve the quality of patient care.

What will make it possible to achieve the objective:

a) Funding the use of new digital technologies in healthcare, including AI and health apps, from public funds as part of guaranteed healthcare services, through such means as:

b) Including these solutions in the description of the standard of the existing guaranteed healthcare services,

c) Introducing a reimbursement mechanism for these solutions,

d) Allocating the necessary funding to finance these solutions,

e) Making the necessary changes in public administration, with new regulations, procedures and strengthened competencies in financing and monitoring of digital solutions, including by creating a standard for assessing the cost-effectiveness of AI-based technologies by the Agency for Health Technology Assessment and Tariff System.

f) Introducing new e-health services to analyse medical data in central registers for health profiling, predictive analytics and result-based interventions e.g. patient contact and educational advice, taking into account the highest privacy standards and allowing the patient to opt in or out of such a programme;

g) Expanding the e-prescription module to include two-way communication, allowing alerts to be displayed to optimise the medicinal treatment;

h) Honest communication and education, aimed at both patients and medical professionals, on the opportunities and limitations of using AI in healthcare;

i) Adjusting ministerial guidelines for medical faculties to educate students on new digital technologies, including AI;

j) Facilitating patient access to information on healthcare arrangements and medical knowledge using artificial intelligence.

What follows from this?

You will receive treatment using the most state-of-the-art, proven technology. You will receive information about the risk of illness before a health incident occurs, which will enable you to take preventive measures.

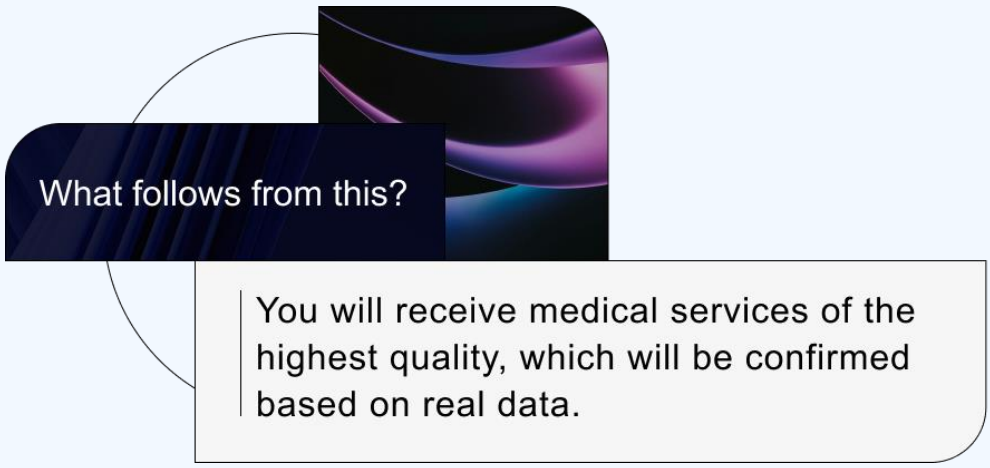
Objective 5: The quality of health interventions is being monitored comprehensively and transparently based on real-world data

What will make it possible to achieve the objective:

a) Enabling ongoing monitoring of the diagnostic and treatment pathways of patients with a specific profile, based on real-world data;

b) Introducing a publicly accessible system for monitoring the quality of services provided by healthcare entities;

c) Providing access to real-world data for the implementation of risk-sharing instruments for drug technologies and selected non-drug technologies, based on a measurable health effect for patients, with this data being available to the public in statistical form.



Objective 6: Healthcare entities and central data repositories have a high level of cybersecurity

What will make it possible to achieve the objective:

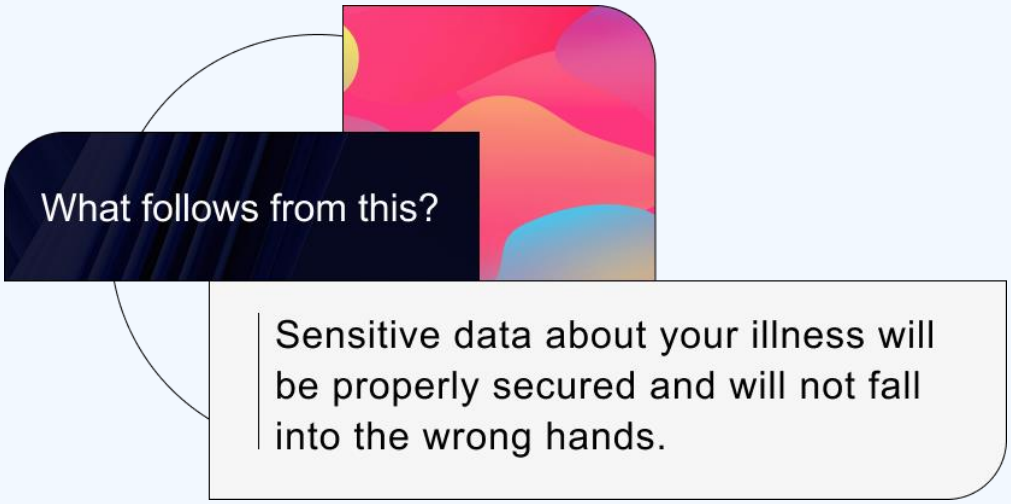
a) Continuing funding programmes for hospitals to improve IT infrastructure and bolster cybersecurity, including by employing the services of specialised third parties;

b) Transforming the Sectoral Cybersecurity Team at the e-Health Centre into a sectoral CSIRT and strengthening it to proactively support healthcare entities in maintaining an adequate level of cybersecurity;

c) Regular training for healthcare managers and medical staff in basic cybersecurity;

d) Increasing the budget allocated to cybersecurity for central systems;

e) Adjusting ministerial guidelines for medical faculties to educate students on basic cybersecurity;



3.3 Creative industries

Diagnosis – what is it like?

Based on the creative, innovative and talent-driven activities of creators of broadly-defined art, media and design, the creative industries are a relatively new sector of the global economy. Characteristic of the sector is the high level of added value that comes with the goods it produces, which is based on the advanced and multidisciplinary knowledge of the creators. The economic importance of the sector is growing both in terms of the value generated and the market. In 2021, Poland's cultural and creative sectors directly generated PLN 31.2 billion in added value. Including indirect effects, this was over PLN 82 billion (3.58 per cent of GDP). As regards the share of value added created in these sectors in GDP, Poland is below the EU average; however, when the indirect impact is also considered, it ranks third in Europe behind only Cyprus and Sweden (out of the 15 countries surveyed).

Yet, the impact of this sector on the state's development cannot be measured by economic indicators alone.

This is because it is located at the intersection of economy, culture, technology and business — it is of considerable cultural and educational importance while fostering innovation at the same time. Indeed, its development is hardly dependent on the use of natural resources or industrial infrastructure. Social changes, which are important for building demand for products and services, highlight good prospects for the creative industries. Nevertheless, a number of important risks cannot be overlooked. These include insufficient funding, unfavourable and complicated regulations, increased international competition and a shortage of skilled workers.

Among the diverse creative industries — which include the film and music industries, the media and the publishing market — the video games sector and its related e-sports scene are of particular importance from the perspective of the digitalisation strategy. Nearly 500 companies are operating in the video games industry in Poland, with revenues of EUR 128 million as of 2022.[35] Poland specialises in premium games for large hardware platforms — PCs and consoles. In terms of the number of people employed in the industry (15,000 people), Poland is only surpassed in Europe by the UK and France. The export-oriented nature of the sector (domestic sales are less than a few per cent) means that it has to confront increased competition, including from the world's largest players. Meanwhile, both Polish and global gamedev is facing a crisis, resulting from the reversal of inorganic growth trends during the pandemic, among other things.

35 https://en.parp.gov.pl/storage/publications/pdf/The_Game_Industry_Poland_2023_12_07.pdf

In the context of its development, the industry's cultural and culture-making aspects should also be considered.

It is not only children, teenagers and middle-aged people who play games but also the elderly; as the Polish population ages, the so-called *silver gaming* is bound to become increasingly widespread. This trend is important when considering the accessibility of games for a wide range of audiences, including people with disabilities. We recognise that games should be treated as a cultural text just like films or literature, which means, among other things, support for their translation into Polish and archiving. However, continued attention to digital hygiene and anti-addiction issues is necessary.

State action should also extend to the area of e-sports, i.e. professional gaming. The global e-sports market was worth USD 3.8 billion in 2023; it is projected to grow at an annual rate of 14.8 per cent until 2028. Poland ranks 20th internationally, with an e-sports sector worth USD 596 million.[36] Indeed, domestic players have some notable achievements, and Poland is also home to one of the world's largest industry events. The e-sports market continues to grow, which is largely linked to the permeation of gaming culture into popular culture. The increasing presence of gaming and e-sports in popular culture is attracting more viewers as well as sponsors. Further popularisation of the area, including among Polish children and young people, is therefore to be expected. Meanwhile, however, the e-sports scene is not free of negative patterns (which are propagated on popular channels), including toxic behaviour of players towards each other, adverse effects of long-term gaming on physical and mental health, gender discrimination, etc. It is therefore necessary, on the one hand, to support the development of the scene and Polish success stories and, on the other, to combat the negative trends still emerging in the sector.

36 https://markethub.pl/rynek-e-sportu/

Objective 1: The development of the gaming industry is rapid

What will make it possible to achieve the objective:

a) Expanding existing support for game developers by increasing the subsidies they can apply for and extending support programmes over several years;

b) Supporting the promotion and marketing of games in target markets, especially those that are difficult due to geographical distance and cost, such as the USA, and building a positive atmosphere through the use of cultural and economic diplomacy tools where relevant to the industry;

c) Supporting the seizing of opportunities presented by the AI revolution for the development of the games industry;

d) Establishing or adapting the tasks of a government institution with the competencies and tools to provide real and tangible support, including mentoring, solely to the video games industry;

e) Systemic support for apprenticeship and scholarship programmes to facilitate the entry of young, talented people into the industry, and tax credits for studios employing first-timers;

f) Facilitation for studios employing high-level experts and managers from outside Poland in areas where there is a shortage of qualified Polish workers;

g) Supporting the processes of setting up branches of foreign companies in Poland and of Polish companies abroad;

h) Working with the academic sector to support education in the competencies required by game development studios: game programming, graphic design, sound production, scriptwriting, business management, etc.;

i) Support by public institutions for local industry events with international reach;

j) Tackling toxicity in the game dev environment, working towards a more inclusive industry (especially for women), combating working environment dysfunctions (e.g. overtime, mobbing, etc.) and promoting proper relations between employees and employers;

k) Promoting video games as cultural works — with a particular focus on Polish language versions (for games by both Polish and foreign developers);

l) Developing an archiving mechanism for Polish video games;

m) Promoting the implementation of accessibility technologies in video games.

Objective 2: Legal barriers to the development of the e-sports industry in Poland are being removed and e-sports popularised

What will make it possible to achieve the objective:

a) Applying the legal aspects of e-sports, including such things as the copyright status of video games, as well as of images and broadcasts of e-sports events;

b) Popularising e-sports by supporting the organisation of amateur competitions at the school level;

c) Promoting physical and mental health prevention, as well as positive and inclusive social conduct, among players;

d) Introducing specialised curricula in schools and universities to train future e-sports professionals, whether as players, managers or analysts;

e) Creating legislation to regulate e-sports, such as player contracts, broadcasting rights or youth protection;

f) Representing Polish e-sports at international conferences and industry fairs;

g) Funding and organisational support for local e-sports clubs that promote healthy competition and talent development.

Objective 3: Creative industries are supported in their development process

What will make it possible to achieve the objective:

a) Grants and development grants for creative projects, enabling artists and companies to develop new projects and technologies;

b) Supporting the development of curricula and training programmes that educate students in creativity, new technologies and creative project management, as well as working with universities and colleges to develop curricula tailored to the needs of the creative industries;

c) Considering the creative industries and their specificities in culture-oriented scholarships and mentoring programmes for young talent;

d) Establishing clusters and incubators that provide working space, technical support and the opportunity to collaborate with others in the industry;

e) Activities that facilitate access for creators to modern technologies and tools that support creativity and innovation;

f) Organising campaigns to promote the Polish creative industries internationally, including participation in fairs and exhibitions;

g) Strengthening intellectual property protection legislation to better protect the creators' work and encourage innovation;

h) Supporting the organisation of conferences, workshops and networking events to share experiences and make contacts;

i) Partnering with the private sector to implement joint projects and initiatives to support the development of the creative industries;

j) Introducing startup support programmes that offer mentoring, access to funding and industry networks;

k) Fostering cross-industry and cross-sector cooperation.

3.4 Digital academia

Diagnosis – what is it like?

The development of the digital state and economy requires cooperation with academia and the scientific sector but also recognition of the need for long-term support for this area's advancement.

If not supported by strong national scientific resources, the Polish digital sphere will not develop harmoniously.

Meanwhile, Polish science is struggling with structural problems due to such factors as the low attractiveness of scientific careers, particularly among early-career scientists. The exodus of the workforce and the relatively low proportion of STEM graduates are serious obstacles to the development of a sustainable higher education and science system, and the limited flow of experienced researchers between science and industry hampers the innovation capacity of the economy. These structural problems are further reinforced in the case of ICT faculties, which have dominated the salary ranking in the Polish Graduate Tracking System for years.[37] Due to strong pressure from industry, some students do not complete their studies, focusing on career development. Very few people choose to pursue an academic career, leading to an increasingly pronounced generation gap in many academic centres.[38] The shortage of IT specialists is also indicated in a report by the Polish Economic Institute, prepared in cooperation with the Software Development Association Poland (SoDA).[39] In turn, Stanford University's "2024 AI Index Report" suggests that these gaps have already led to a decline in the number of ICT specialists being educated in Poland.[40]

Negative trends in IT talent development are a major concern, especially due to the rapid development of AI. The increasing strategic importance of this technology makes it necessary to develop it at the national level. The Polish academic system needs to be strengthened with regard to the training of AI specialists and the possibility of using AI horizontally in interdisciplinary research. Notably, due to two unique conditions developed over the years, Polish science is in a good starting position in the race for leadership in the coming changes. First, despite the lack of growth in the number of students, Poland's IT education is at a very high level and its algorithmics and programming scene has allowed Polish IT specialists to achieve major success in numerous competitions, contests and olympiads. Second, Poland is one of the leaders in the computerisation of higher education

37 https://ela.nauka.gov.pl/

38 https://www.zycieuczelni.p.lodz.pl/luka-pokoleniowa-problem-dla-uczelni-i-biznesu/

39 https://pie.net.pl/wp-content/uploads/2022/11/PIE_Raport_Ilu-specjalistow-IT-brakuje-w-Polsce.pdf

40 https://aiindex.stanford.edu/report/

and science in Europe, primarily thanks to the Integrated Information System for Higher Education and Science — the POL-on network — and the public e-services built on it.

Cel 1. Academics who are key to developing the workforce for the digital state are effectively supported in their research and teaching work.

What will make it possible to achieve the objective:

a) Ensuring the stability and security of university jobs. Establishing mechanisms to recognise the importance of cross-sectoral scientific mobility (including mutual recognition of experience between sectors) and to change the publication evaluation system to focus on the quality and relevance of research results. In the case of digital technologies, numerous researchers often transition between academia and industry, so it is vital to promote the importance of such industrial experience in academia, and academic experience in industry. Facilitating the flow of people in this way will enhance and strengthen cooperation between science and business;

b) Increasing financial support for young researchers in the field of ICT. We recognise that it is much more difficult to do well academically without securing a decent standard of living. We also plan to seek other models of financial support, rewards and bonuses for IT, AI and STEM research and publications across all disciplines;

c) Promoting STEM research in the area of new technologies as a career that offers great opportunities for growth — from working in academic research units and centres to establishing startups. Promoting cooperation between different types of research units;

d) Structuring for non-traditional career paths, including the creation of research engineer positions at universities, and other mechanisms to ensure better mobility between the public and private sectors. Increasing the importance of industry experience in academic careers.

Objective 2: Polish science is supported by an advanced IT infrastructure.

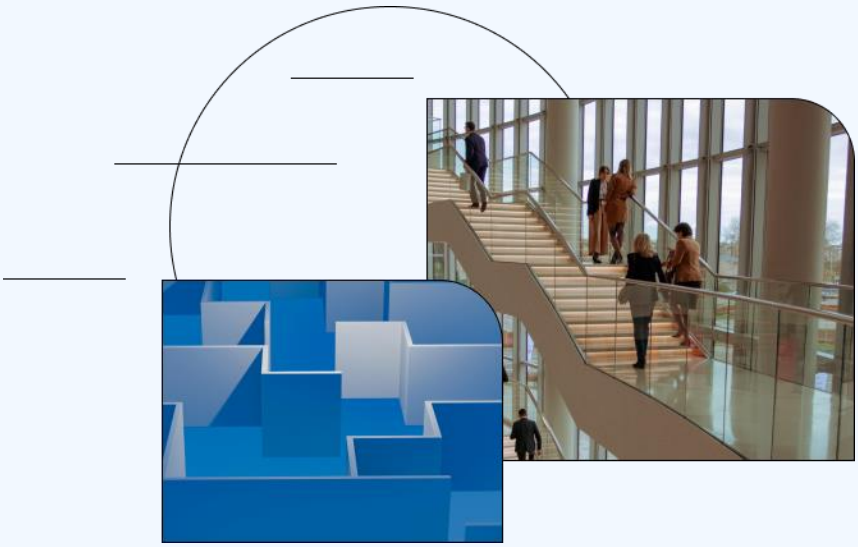
What will make it possible to achieve the objective:

a) Investing in computing capacity for research, which is particularly needed for the use of AI in interdisciplinary scientific fields. The increase in computing capacity must be accompanied by the establishment of, as part of HPC (High-Performance Computing)/plGRID, load reporting systems as well as the relevant number of projects/grants and supported startups;

b) Continuing to develop the POL-on (Integrated Information System for Higher Education and Science), ELA (Polish Graduate Tracking System) and OSF (Funding Stream Support System) systems to enable them to become reference data sources for public e-services to more effectively measure and analyse the effectiveness of ongoing scientific projects and commercialise research results;

c) Developing digital e-services addressed to university candidates, students, doctoral students and graduates, including a system to help university candidates choose a university and field of study, e-Diplomas, a set of tools to support the proper choice of fields of study, Student mIDs;

d) Creating a portal that would semi-automatically, with the support of AI, create a database of technologies, services and infrastructure, and collect in one place the research, commercialisation and implementation potential of all scientific units in Poland. On the one hand, it would be available to scientific institutions and, on the other, to entrepreneurs, enabling them to establish cooperation, e.g. to carry out joint projects in scientific-industrial consortia.



Objective 3: Polish ICT science is internationally prominent

What will make it possible to achieve the objective:

a) Promoting and internationalising Polish science, e.g. by collaborating with the best universities in Europe and worldwide and highlighting the achievements of Polish computer scientists;

b) Developing science diplomacy in terms of increasing the level of foreign public funding (including European funding) for research.

c) Adapting and improving the system of parametric evaluation of scientific and research units so that it is more supportive of the commercialisation of research results and the development of new paths for research commercialisation, taking into account modern, international models for conducting research;

d) Supporting the participation of Polish institutions and researchers in international technology networks and organisations that aim to promote ICT sector development;

e) Strengthening leading IT universities and research centres and creating research institutions in Poland that have the potential to become internationally renowned. We recognise that having internationally renowned research institutions at home is one of the most effective measures against brain drain. Leveraging the IDEAS Institute, which will also promote the use of AI in diverse fields through interdisciplinary research.

Business and technology

Ministry of Digital Affairs
Republic of Poland

We Make the Future

Business and technology

4.1 Digital transition of businesses

Diagnosis – what is it like?

In 2023, more than three-quarters of Polish companies were classified as having very low or low digital intensity, with only 21% of companies having a high or very high level of digital intensity. In Poland, the SME sector accounts for 99.8% of the total number of enterprises, generating 43.6% of GDP (2020 data). Small and medium-sized enterprises play a key role in the development of the Polish economy, and their digital transition is a condition for maintaining and improving Poland's competitive position in the international market.

In 2023, the percentage of businesses with broadband access reached almost 99%. Enterprise Resource Planning (ERP) software was used by 36% of companies, and sales through computer networks were conducted by 18%. In 2022, almost 73% of businesses were issuing and sending electronic invoices, with 67% of those being unsuitable and 14.8% suitable for automated processing[41]. As of 2023, intermediate and advanced cloud technologies were used by 47%, data analytics by 19% and artificial intelligence by 4% of companies[42]. A total of 32% of SMEs did not use any digital tools (39% among micro businesses), while those that did, most often utilised basic digital tools such as social media and online payment platforms (38%). Only 14% used the cloud and 13% used IT tools for process management.

The level of digitalisation of companies is correlated with their size: on average, the larger they are, the more they spend on R&D and the implementation of new technologies.

A similar relationship exists in the case of enterprise innovation: the highest proportion of innovation-active entities is found among large enterprises. Business process innovation is more common than product innovation.

Another aspect of digital transition is the implementation of advanced Industry 4.0 technologies. The diagnosis of the implementation of Industry 4.0 in Poland for 2022–2024 indicates that progress in the adaptation of modern technologies in various sectors of the economy is gradual, although uneven, and depends on the size of the enterprise (most often, these technologies are implemented by large companies with revenues exceeding PLN 500

41 Information society in Poland in 2023, Statistics Poland

42Data for: Eurostat 2023

million). Poland is in the early stages of implementing Industry 4.0 but with great potential for growth, especially among large enterprises. However, the low rate of adoption of disruptive technologies and the lack of long-term plans for Industry 4.0 technologies puts Polish industry at a disadvantage compared to other EU countries, where investments in digitalisation are at a higher level.

The technological sophistication of Polish companies must be raised to increase their productivity; this is especially the case for small and medium-sized enterprises.

This in turn is a prerequisite for further dynamic development of the Polish economy. Research on the productivity of Polish enterprises shows that there is great potential to increase its level by using improvements in the form of modern digital tools.

Poland is dominated by high-mix low-volume production, so traditional approaches to digitalisation, automation and robotisation can hardly have the expected economic effect. Various types of advanced equipment, machines, machine tools and robots require skilled human operators. The demographic decline could further aggravate the current situation. Production preparation costs and the acquisition of new orders account for a larger share of overall production costs. This area is not covered by automation at all.

Apart from designing appropriate financial support instruments for companies, it is also necessary to raise awareness among businesses of the benefits brought by the use of new technologies, the development of competencies and skills of employees and company managers in the application of modern digital solutions, as well as the development of a business environment system favourable to innovation.

The main barriers in the area of digital transition include[43]:

- doubting the benefits — the type of return on investment in digitalisation;
- a shortage of specialists on the market and a lack of competencies, particularly in software development, complex data and mathematical analysis, project management skills using IT tools, as well as digital strategy development and leadership skills;
- the high cost of implementing digital tools and the lack of adequate funding opportunities;
- a lack of time to implement digital solutions;
- IT security issues.

43eSkills for Jobs Index, “Dojrzałość technologiczna polskich firm” [Technological Maturity of Polish Companies] Report and BGK’s 2024 report “Cyfryzacja w sektorze MŚP — szanse i ograniczenia” [Digitalisation in the SME sector — opportunities and constraints]

Objective 1: An efficient system is in place for managing activities in the area of supporting the digital transition of enterprises

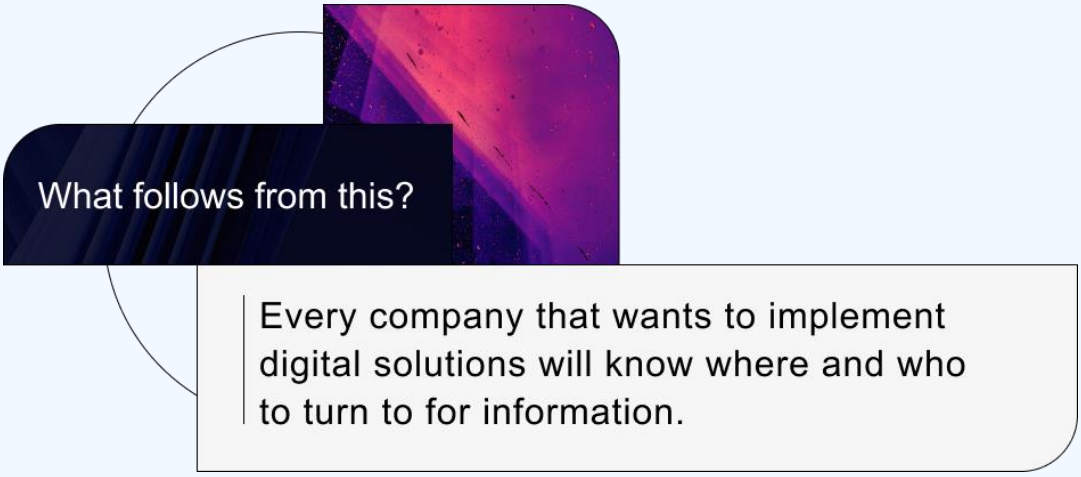
What will make it possible to achieve the objective:

a) Establishing an entity to coordinate the digital transition of businesses, especially SMEs, to define objectives and actions, monitor progress, assess the extent to which objectives are being met, as well as identify technology needs and the expectations and opportunities of SMEs;

b) Developing a common and nationally consistent vision for the digitalisation of businesses, particularly including the SME sector, taking into account the impact of large companies on the digitalisation of SMEs in their supply chain, and defining strategies and standards that will support the integration of SMEs into the digital solutions implemented by large companies;

c) Ensuring that programmes supporting the digitalisation of businesses are comprehensible and informative;

d) Providing one-stop access to comprehensive information on available support programmes and materials and training for entrepreneurs.



Objective 2: Entrepreneurs see the digital transition as a process to make business easier and more efficient

What will make it possible to achieve the objective:

a) Conducting educational activities that build awareness of the benefits of the digitalisation process and the development of digital competencies of employees and managers;

b) Evaluating existing solutions to support the digitalisation of businesses and designing, based on the diagnosis made, as well as implementing new instruments to support the digital transition of businesses, which will be tailored to the needs of specific categories of entrepreneurs;

c) Identifying key industries that guarantee technology transfer and the creation of an internal supply chain based on domestic companies in which Poland has the potential for competitive advantage and targeting these areas. The key industries will be those that have a significant impact on Polish GDP, a large share of exports and significant potential for productivity growth as a result of the digital transition and the implementation of Industry 4.0 technologies;

d) Introducing the “Cyfrowy start dla biznesu” [Business Digital Startup] facility to support newly established companies in their digital development. This package would propose solutions, digitalising business processes right from the start and making it easier to run the company — e.g. office, accounting and financial software, customer relations and document management, communication and collaboration software, cybersecurity software and, possibly, Enterprise Resource Planning systems;

e) Providing services for entrepreneurs, in particular, advice, training, skills development, opportunities to test and experiment with solutions in pilots and support in finding sources of funding for the digital transition (as exemplified by the EDIH (European Digital Innovation Hubs) network).

What follows from this?

We will help companies understand the benefits of digitalisation and guide them through digital transformation by offering the best tools for the company.

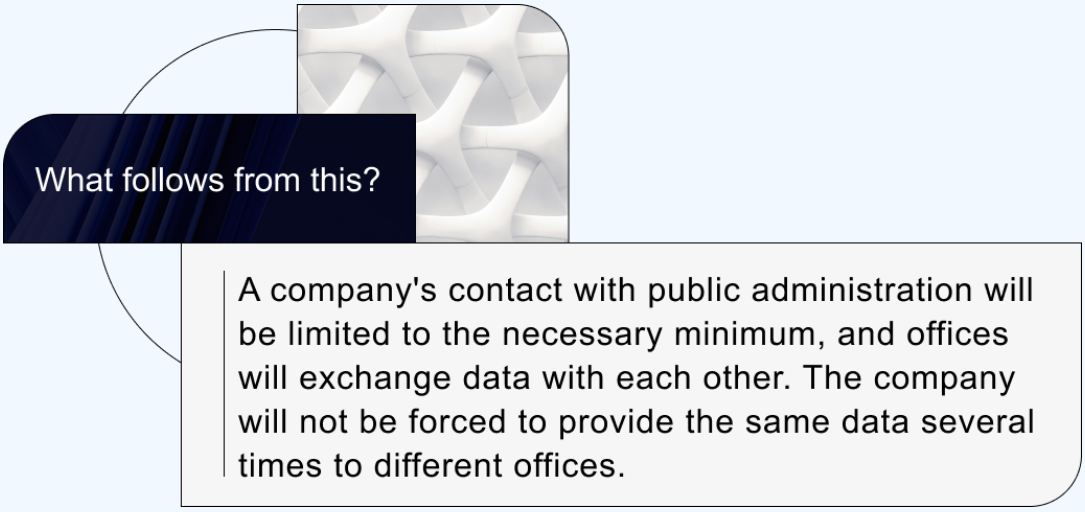
Objective 3: Digital public services for entrepreneurs are proactive and mature, and systems interoperability makes it possible to reduce administrative workloads

What will make it possible to achieve the objective:

a) Developing public services to an ever-increasing level of maturity, based on user needs, which propose to users to perform actions or accept actions performed by the system;

b) Fully digitalising the contacts between entrepreneurs and the state (including, for example, through the digitalisation of public procurement or construction permit processes);

c) Introducing the “one time only” principle, meaning that citizens and businesses provide their data to the public administration only once, and the public administration then shares this data internally between institutions to avoid burdening citizens and businesses.



Objective 4: Entrepreneurs are aware of cyber threats and are taking up preventive instruments.

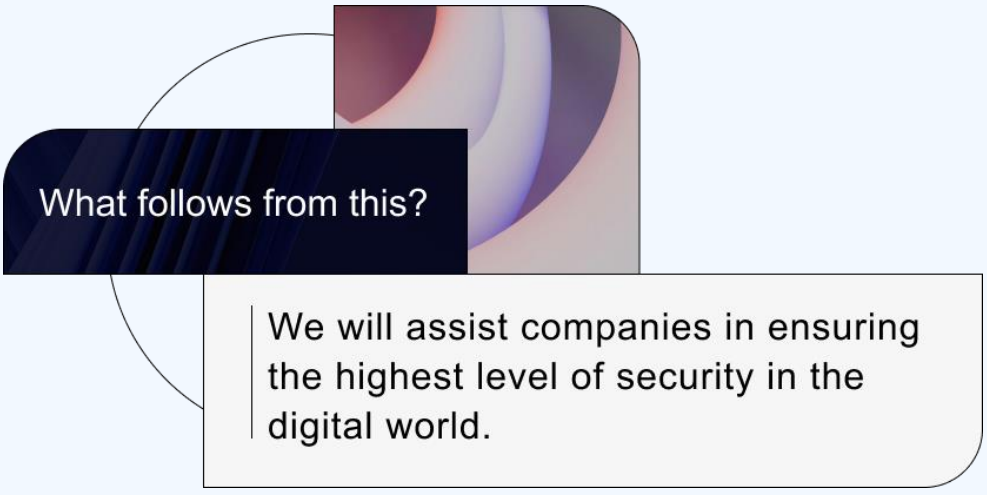
What will make it possible to achieve the objective:

a) Promoting basic cybersecurity knowledge;

b) Providing training and courses covering topics such as cyber threats and disinformation (including as part of the “Cyfrowy Start dla Biznesu” [Business Digital Startup] programme);

c) Introducing a voluntary cybersecurity certification scheme for companies;

d) Linking the cybersecurity certification scheme to insurance for cybersecurity risks as well as linking the premium to the insurance held.



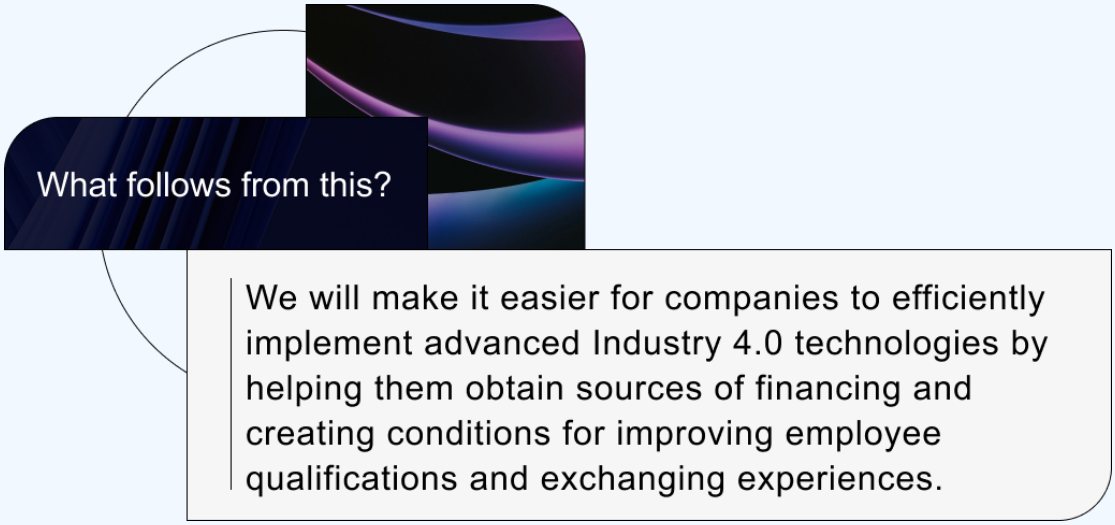
Objective 5: Industry entrepreneurs are aware of the benefits of Industry 4.0 technologies and are implementing them in their companies

What will make it possible to achieve the objective:

a) Fostering the adoption of advanced Industry 4.0 technologies by stimulating inter-institutional cooperation, including collaboration with technical academia to develop programmes to upgrade the skills of industrial workers, cooperation between the public and private sectors to build modern data centres and digital platforms;

b) Creating online knowledge-sharing platforms that enable companies to share experiences and best Industry 4.0 practices;

c) Making it easier for entrepreneurs to access funding sources for Industry 4.0 technologies, including tax credits and innovation grants, technology loans and pilot deployment programmes.



4.2 Artificial intelligence

Diagnosis – what is it like?

The implementation of state-of-the-art technologies and the use of systems based on human-centred, sustainable, trustworthy, secure and inclusive artificial intelligence (AI) are key to Poland's development.

This technology can significantly improve industry capacity, efficiency and quality of service delivery, as well as support decision-making and resource management.

As a process automation technology, AI is also a key tool to reduce the negative impact of demographic trends. Last but not least, it has transformative potential in collaboration with other disruptive technologies such as cloud computing and the Internet of Things. This conglomerate, of which AI is a central element, is sometimes referred to as AI+. The number and scale of investments in AI[44] products and services is increasing. What is at stake in this race is a share of the rapidly-growing AI market and its associated benefits — ICT exports, productivity growth and innovation. Today's estimates indicate that by the end of the decade, these benefits will reach 10% of the gross world product, with the value of the AI market alone exceeding USD 1.3 trillion. Countries are participating in this race by creating an attractive environment for investors and innovators. Poland is behind the world leaders in this race, overtaken by — apart from the global giants — such European countries as the UK, Germany, Sweden and Spain.[45] However, this race is at an early stage and change is necessary and possible.

Poland faces several structural challenges in the context of AI development. Building and developing a friendly AI ecosystem in Poland requires simultaneous acceleration of the rate of growth of both public and private investment in research and innovation, the latter being a particular challenge for small and medium-sized enterprises. To be among the leaders, it is also necessary to increase awareness among entrepreneurs of the benefits of AI/AI+, as well as to improve access to expertise and computing power.

Specialists are a key asset for the AI sector's development. Between early 2020 and the first half of 2023, some 19,000 doctoral degrees were awarded in Poland, including 622 in IT-related disciplines and 207 in the field of artificial intelligence. This places Poland outside the top 15 in Europe in terms of IT graduates, both in terms of their total number and their number per 100,000 inhabitants[46].

44 https://www.goldmansachs.com/insights/articles/ai-investment-forecast-to-approach-200-billion-globally-by-2025.html

45 https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/760392/EPRS_ATA(2024)760392_EN.pdf

46 Stanford Institute for Human-Centered Artificial Intelligence, 2024 AI Index Report, Chapter Education, 2024

It is necessary to adopt and enforce a coherent legal framework, apply standards and codes of good practice and increase the level of access to high-quality infrastructure (ICT, computing, energy). Poland is obliged to carry out a legislative process to bring the domestic legislation in line with the EU AI Act and international law, which will effectively establish artificial intelligence laws in Poland. Poland also faces the implementation of the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law adopted by the Committee of Ministers of the Council of Europe, which corresponds to EU regulations.

It is essential to implement these regulations in an innovation-friendly fashion, balancing the concern for trustworthy, secure AI with care for the development and implementation of business innovation.

This balance should be reflected in the institutional approach (the role and scope of the Polish supervisory authorities working with the European AI Office) as well as in the investment financing system. At the same time, the Polish state cannot decide to implement a specific technology without in-depth analyses of the expected effects and risks of doing so. Accordingly, the state should employ AI which will make life as easy as possible for citizens and realistically respond to societal needs while not generating undue risks.

Hence, there is a strong need to update public policy on the development of artificial intelligence in Poland, including the identification of strategic areas for the development of the economy where AI should be implemented as a priority. Such a policy must address the current trends and challenges and ensure coherence and coordination at the governmental and international levels. The new policy will be drafted based on four pillars: innovation, investment, education and implementation.

Poles are well aware of artificial intelligence, with 98.8 per cent declaring that they have heard of it[47]. Half of Poles (51.1 per cent) believe that artificial intelligence will bring more benefits than harm to society. Simultaneously, 25 per cent of respondents are convinced that the detrimental impact of AI will outweigh its advantages. Poles have considerable confidence in AI, with 41 per cent of respondents willing to rely on information provided by artificial intelligence. Despite this, 40 per cent indicate the need for human oversight of AI development.

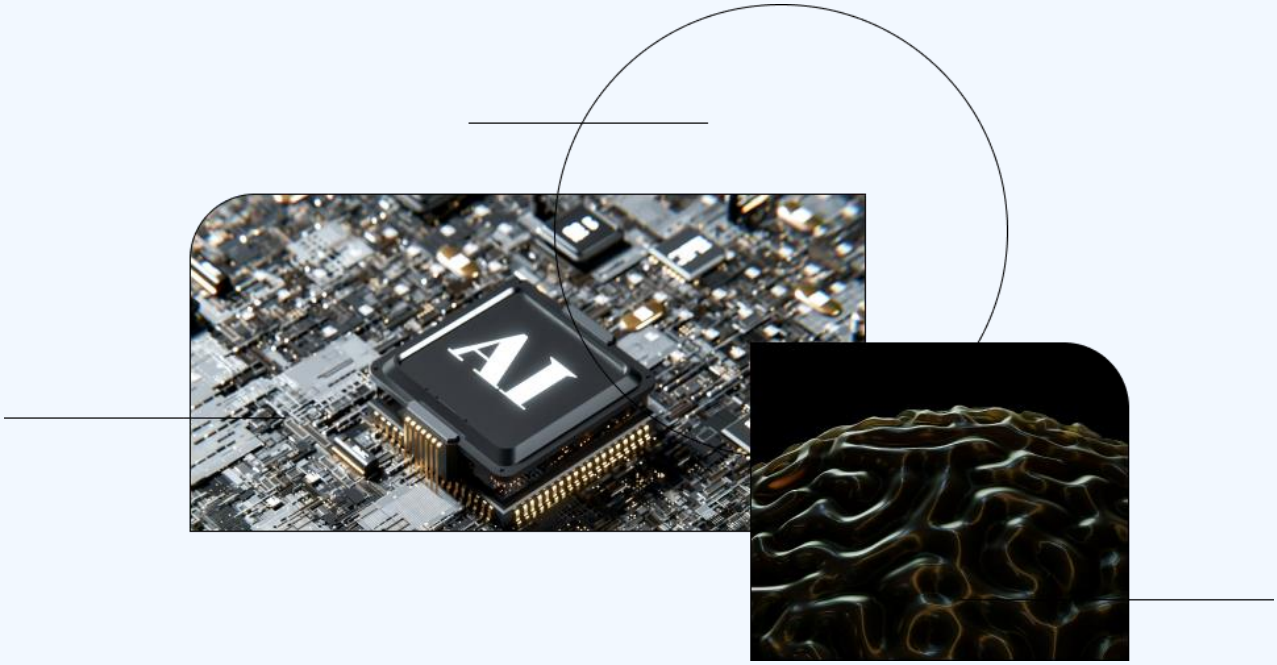
Poles largely [48]support the use of AI by the state. According to 60.4 per cent, artificial intelligence should be used in the creation of digital public services. Further, 32 per cent of those surveyed believe that artificial intelligence can speed up and automate administrative processes and reduce public service delivery times. Another expectation often raised by respondents for the use of AI in public services is to make them more accessible to people with disabilities. Notably, Poles are reluctant to permit the use of artificial intelligence to make automated administrative decisions that may affect their lives. In contrast, there is a higher

47 https://pie.net.pl/wp-content/uploads/2024/09/Sztuczna-inteligencja-w-administracji-publicznej.pdf

48 https://pie.net.pl/wp-content/uploads/2024/09/Sztuczna-inteligencja-w-administracji-publicznej.pdf

level of support for the possibility of automating simple administrative tasks and emergency alerts, as well as using AI to support citizens in filling out documents.

In summary, creating a broad AI+ ecosystem that includes collaboration between public and private actors in education, research, innovation, production and secure deployment of AI solutions is key to the development of this technology.



Objective 1: Supporting economic and digital industry development, as well as social well-being and human autonomy, by an efficient and coordinated artificial intelligence ecosystem

What will make it possible to achieve the objective:

a) Creating an EU-compliant and business-friendly oversight system for AI models and systems, so that citizens, consumers and companies are aware and confident that AI solutions used in the market and public administration are safe, compliant and ethical;

b) Identifying a lead institution for AI research and coordinating the collaboration of AI research institutions that are part of the AI ecosystem;

c) Ensuring transparent, coordinated and effective funding for the development of Polish companies in the area of AI and digital innovation, as well as increasing the level of support (private and public) for entrepreneurs developing and implementing AI;

d) Establishing regulatory sandboxes for innovators in line with the EU approach;

e) Creating a uniform, publicly available list of AI systems used in public administration with a description of the functions and the basic technical parameters available to citizens to increase the transparency of public administration. Drafting and enforcing rules for the use of AI in public administration;

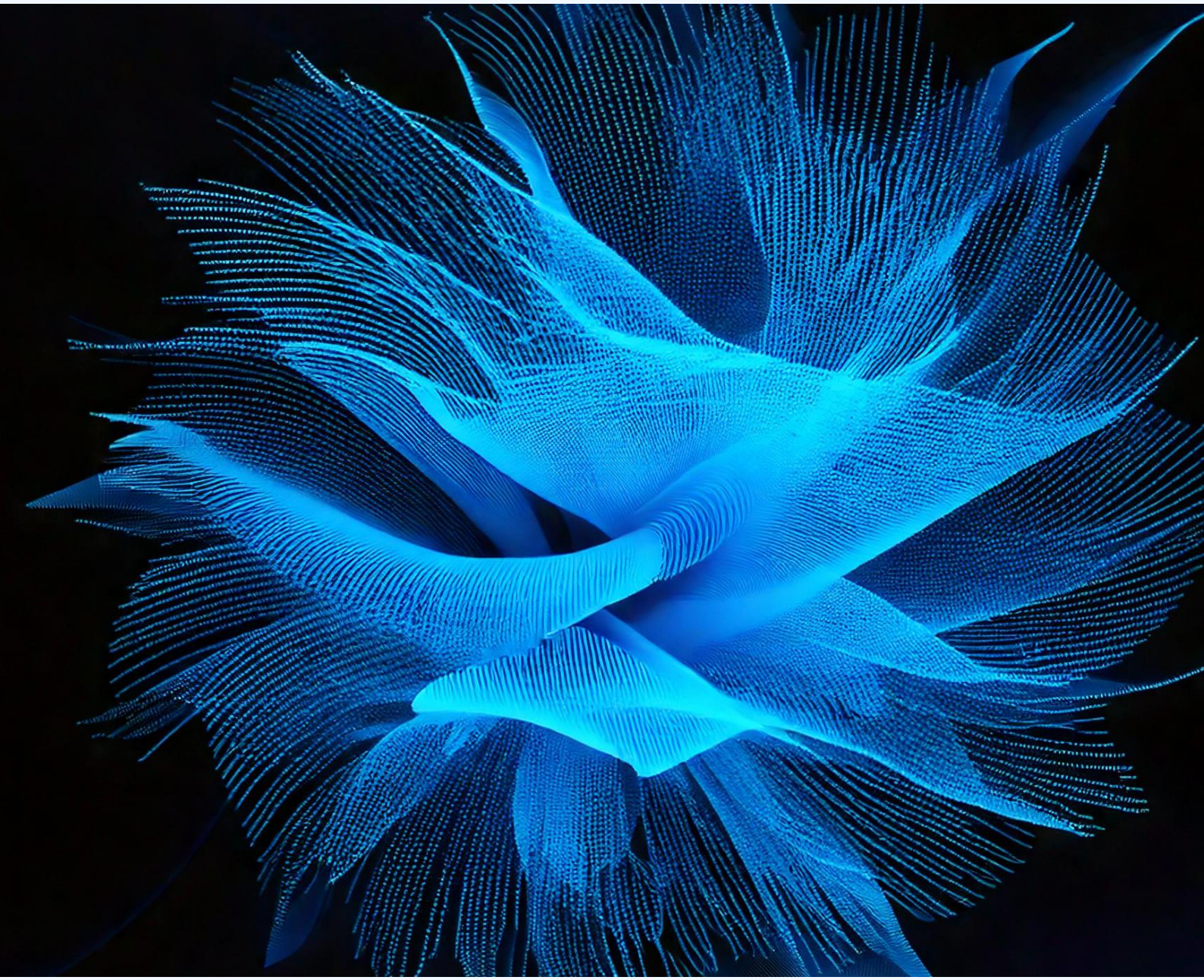
f) Creating or identifying a global-level AI security authority tasked with investigating the latest risks associated with the rapid development of this technology, as well as supporting the oversight of the security of AI applications. Its activities would relate to the safe use and future development of AI on the one hand, and the cyber security of AI solutions and protection against cyber attacks involving this technology on the other. The institution in question would also pursue global cooperation with other similar bodies;

g) Working with partners (Polish and international) to develop tools and conduct regular applied research in the creation of public policies dedicated to the impact of AI technologies on the labour market, economy, environment and society, taking into account both potentials and risks, including the situation of people at risk of exclusion;

h) Creating ISO- and IEC-compliant digital data structure standards for all industries to build and teach AI models.

What follows from this?

The AI development will be ensured by research, protection against cyber attacks and a coordinated financing system. The use of AI solutions will be safe and compliant with regulations and ethics.



Objective 2: Efficient and transparent implementation and funding of R&D and deployment of artificial intelligence

What will make it possible to achieve the objective:

a) Establishing and managing a mechanism to coordinate current funds, tenders and delivery methods to avoid duplication of activities and inefficient spending of investment funds, including the need to centralise the research, development and implementation agenda;

b) Prioritising the funding of the development, commercialisation and deployment of innovations, including the adaptation and use of artificial intelligence technologies by startups, the public administration, SMEs and large enterprises;

c) Creating a single point of access to information on all sources of funding for AI projects, where it would be possible to find the most appropriate fund for the given project,

d) Supporting SMEs to implement AI through access to low-cost consultancy services and improving digital competencies in both businesses and the public sector by supporting programmes that help implement lifelong learning, including AI vocational training;

e) Providing 50% of national funding for EU co-funded AI projects;

f) Development and implementation of AI projects with the greatest potential for economic development and social well-being in Poland, as well as those with significant social or economic value and with the greatest potential for enabling Poland to become a major player in the global artificial intelligence market;

g) Implementation and dissemination of the Polish large-scale language model on an open-source basis, with a licence that allows its use in the market and further improvement, as well as a good quality language dataset for the Polish market.

Objective 3: Ensuring an appropriate computing infrastructure and data resources to facilitate the development of artificial intelligence

What will make it possible to achieve the objective:

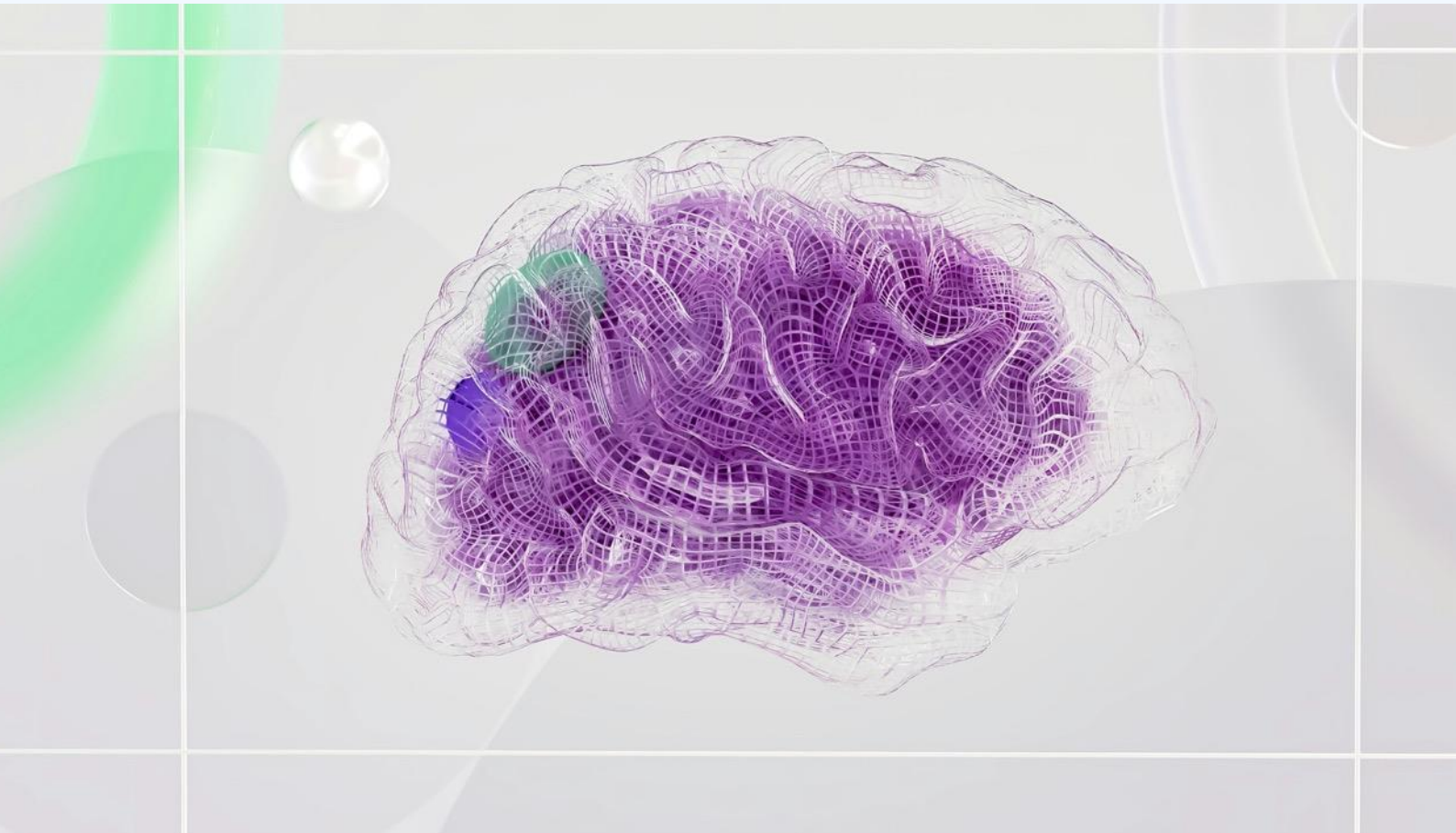
a) Providing decentralised publicly-available computing power for artificial intelligence projects, including by expanding and promoting such initiatives as PLGrid;

b) Increasing the transparency of the access to computing power, e.g. PLGrid, for research and commercialisation;

c) Facilitating access to datasets for companies and research centres to test and develop AI algorithms;

d) Defining a standard for the generation of data for feeding artificial intelligence systems in accordance with interoperability, ethical principles and human rights and in line with EU and international standards;

e) Active participation of Polish representatives in work on international standards related to AI, ICT and data structure development.



4.3 Other disruptive technologies

Diagnosis – what is it like?

Disruptive technologies for digital transformation (irrespective of the separately identified area of artificial intelligence) include solutions like quantum technologies, edge computing, VR/AR, blockchain and space technologies. Whether necessary or expected, state intervention determines — both in the Polish and European dimensions — if the opportunity to maintain strategic economic autonomy and reduce the risk of technological dependence on foreign actors can be seized. The various support mechanisms for industrial investment, the R&D sector, facilitators for startups, investments in hard skills in the vocational training process, as well as the implementation of disruptive technologies in the public sector, are expected to encourage new technological ventures in Poland.

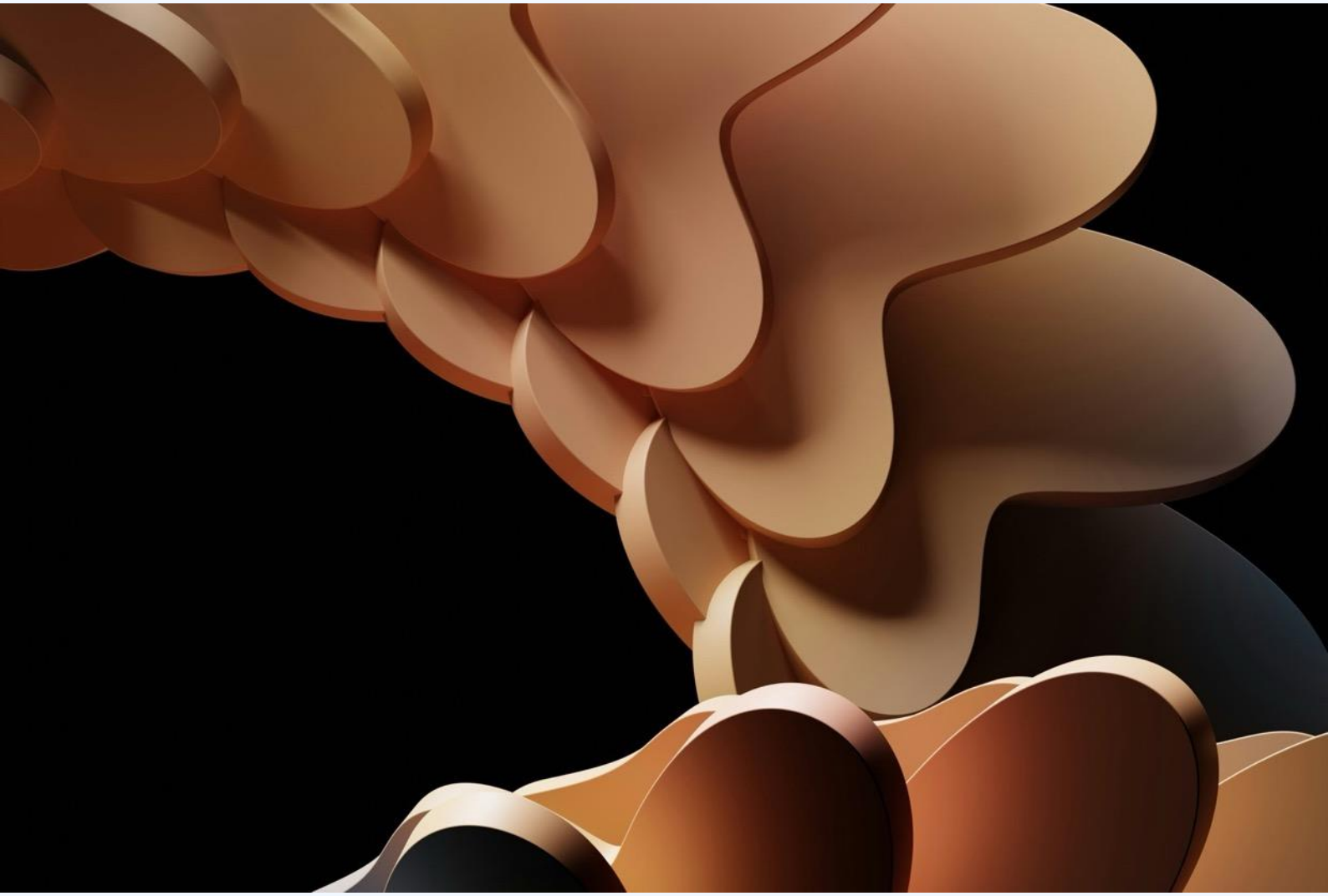
Development activities for the most important technological trends are planned at the European Union level. Poland is actively involved in these endeavours through international projects providing the opportunity to achieve the economies of scale necessary in global competition, both in terms of supply chain efficiency and bringing practical applications to the market. It is also a signatory to the European Declaration on Quantum Technologies and has joined the Quantum Coordination Board. Some projects already underway, such as the EuroQCI (European Quantum Communication Infrastructure) quantum communication network, including both terrestrial optical fibre and space segments, and the construction of a quantum computer in Poland as part of the EuroHPCie European infrastructure, would have no chance of success without the cooperation of many countries. Outstanding challenges include applications, metrology (sensors), post-quantum cryptography and the production of post-quantum era microprocessors.

Increasing the number of nodes in edge computing systems has become one of the EU's 2030 policy objectives, providing the market with incentives to optimise data processing networks. By and large, data network infrastructure is currently built and maintained primarily by the private sector; however, the aspirations for the development of AI systems, IoT, smart cities and 5G networks are not always matched by private investment plans. There is a public policy rationale for ensuring energy-efficient development and cybersecurity.

Poland has been a member of the European Blockchain Partnership since 2018. In 2024, the European Blockchain Services Infrastructure (EBSI) network being built under this partnership will be transferred to EUROPEUM-EDIC, a new entity created with Polish participation under a new legal framework for multi-country projects. This is another area where European cooperation offers the opportunity to implement large-scale projects for the application of breakthrough technologies in public sector services, which will catalyse deployments in other areas.

The semiconductor industry, which is key to the development of the digital economy, is poorly developed in Poland, with no mass production of semiconductors currently taking place in the country. It is being implemented on a pilot scale or, at most, a low-volume production scale. This mainly includes semiconductors for special applications manufactured at the Łukasiewicz — Institute of Microelectronics and Photonics. Also specific to Poland is the small number of qualified personnel, which raises concerns in the industry about their potential departure from Polish companies and research centres should a foreign entity

offering substantial investments in this area appear in Poland. Teaching activities are concentrated in a small group of academic centres such as the Warsaw University of Technology and the AGH University of Kraków; there are also promising co-leadership projects at the Poznań University of Technology. However, one opportunity in the coming years is the recognition given to this issue at the EU level, as expressed by the adoption of the Chip Act or the Union's aspiration to reach 20 per cent of global semiconductor production by 2030. It is also vital to note the creation of the National Framework for Supporting Strategic Semiconductor Investments, a programme designed to support the establishment of costly advanced manufacturing facilities in Poland.



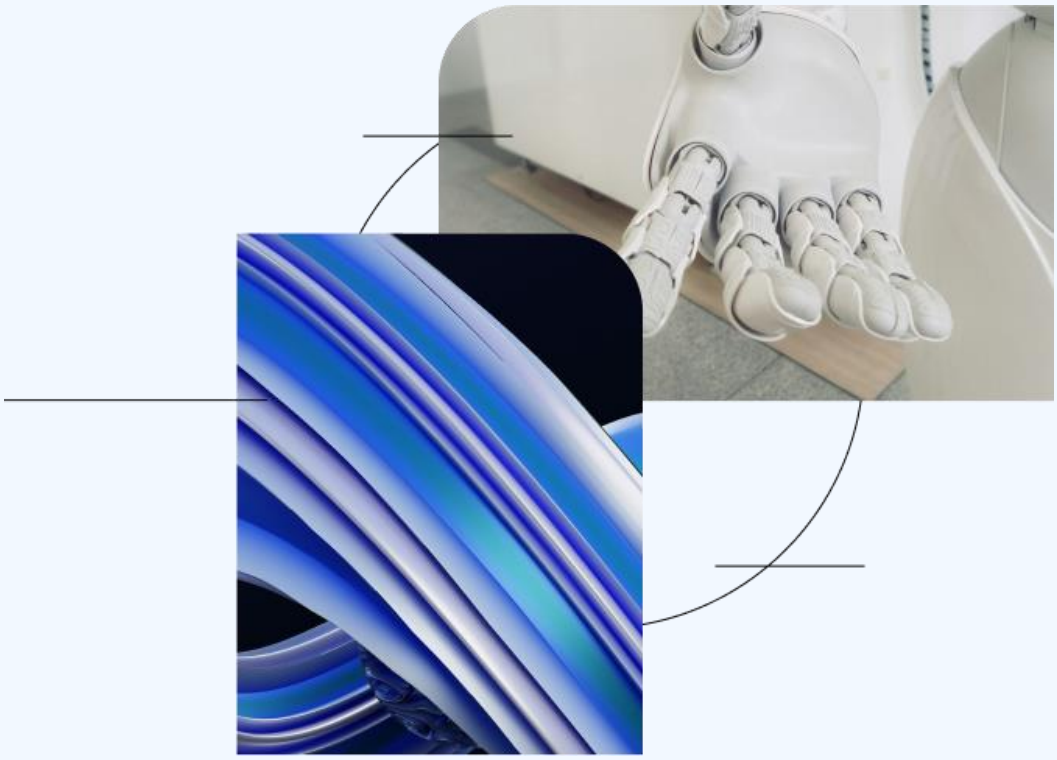
Objective 1: Expanded research and competencies ecosystem promotes development in the area of disruptive technologies

What will make it possible to achieve the objective:

a) Creating a multi-annual programme to support the development of disruptive technologies to coordinate the research agenda, consolidate efforts and resources and set high-level guidelines for the coming years. The programme will be flexible and adaptable to technological change. It will make it possible to stabilise scientific work and funding for interdisciplinary research teams. At the same time, however, it must rely on high-quality international collaborations and access to the best global know-how;

b) Consolidating the management of the research agenda around disruptive technologies in collaboration with the scientific, business and academic communities;

c) Establishing partnerships with world-leading disruptive technology research centres.



Objective 2: Quantum technologies are being applied in key industries and areas of government activity

What will make it possible to achieve the objective:

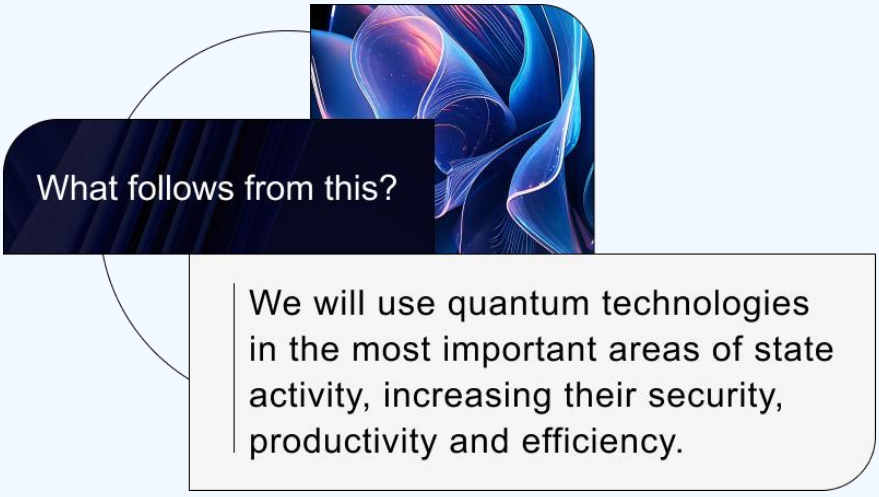
a) Identifying key areas where quantum technology has the potential to increase productivity, safety and efficiency in the Polish context;

b) Providing access to quantum know-how and infrastructure to academia and business;

c) Utilising quantum technologies, including communications and quantum cryptography, to safeguard critical infrastructure and enhance national security. Harnessing quantum technology in a dual-use model for defence;

d) Applying quantum metrology to the economy, particularly in the exploration and location of natural resource deposits;

e) Fostering entrepreneurship based on quantum technology products/services (e.g. startup accelerator, competitions)



Objective 3: Internet of Things technologies are being used in key economic sectors in urban and rural centres

What will make it possible to achieve the objective:

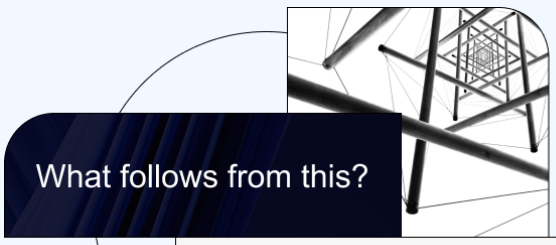
a) Metering of water bodies, especially major rivers and lakes to monitor water quality and water levels, and making this data publicly available to residents and citizens;

b) Developing smog monitoring networks in cities and towns to diagnose air quality; Metering major traffic routes to monitor traffic and optimise transport;

c) Building demonstration farms containing the latest Internet of Things (IoT) solutions, for example, soil moisture sensors in each voivodeship, to educate and implement IoT in the agricultural sector;

d) Establishing 1,000 edge processing nodes to efficiently process data collected from IoT devices;

e) Building an open-source smart city platform, which would be accessible to smaller towns and villages, to popularise smart city and village solutions in less connected regions, while ensuring the privacy of residents.



What follows from this?

Villages and cities will have access to smart city knowledge and solutions. The use of IoT technology will improve the operation of the key economy sectors, including monitoring water and air quality, monitoring traffic and optimising transport.

Objective 4: Poland develops the semiconductor sector through increased investments

What will make it possible to achieve the objective:

a) Formulating a detailed policy for the development of the semiconductor sector in Poland, taking into account the international context (including cooperation with key supply chain countries and EU support), as well as identifying barriers to development and existing areas of Polish specialisation;

b) Supporting the expansion of the Polish semiconductor ecosystem — including actors from across the value chain — and integrating Polish companies and research units into Europe's growing supply chain;

c) Ensuring continued cooperation between ministries and institutions key to the development of the semiconductor sector to secure investment synergies, including in the European context, building favourable conditions for investors and bringing in foreign investment;

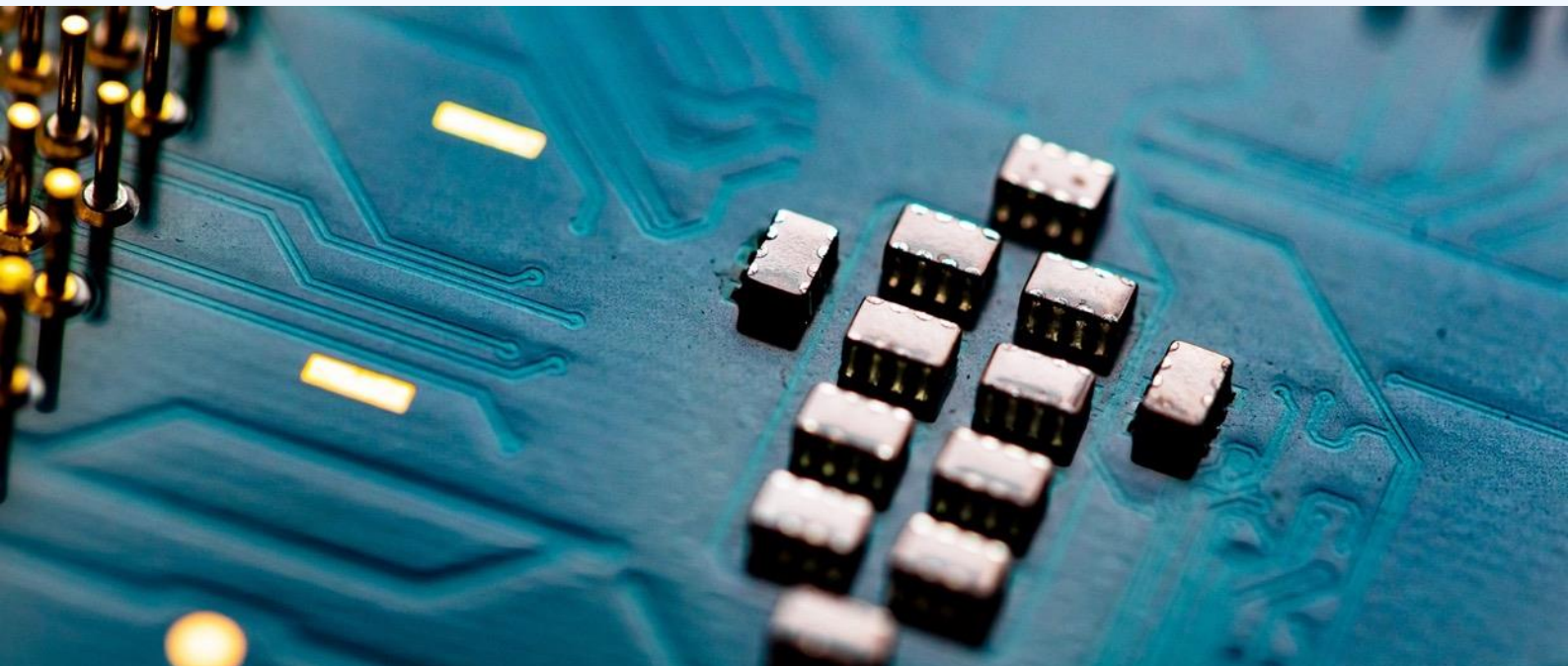
d) Establishing a Polish semiconductor competencies centre;

e) Securing funding for Polish companies (especially SMEs) to cover the cost of access to a cloud-based semiconductor design platform and pilot production lines;

f) Long-term maintenance of the National Framework for Supporting Strategic Semiconductor Investments programme;

g) Supporting the development of pilot and low-volume production lines in the country based on the foundry model;

h) Supporting the creation of small open-source electronics.



Objective 5: Blockchain technologies are being used and developed, including in the European dimension

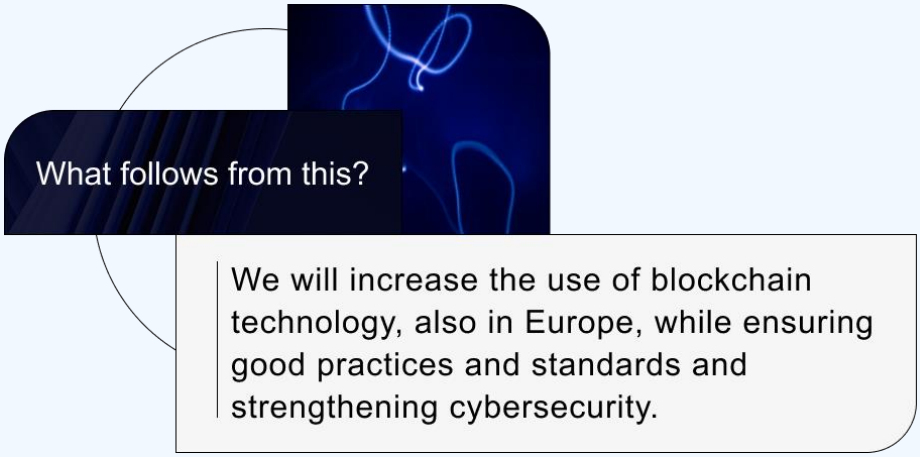
What will make it possible to achieve the objective:

a) Deploying blockchain technology, with a key factor being to increase the transparency and accountability of selected processes in government, the public sector and the economy, including removing the room for fraud or manipulation, as well as using such means as verifiable credentials, sovereign identity, the EU digital identity wallet, electronic bills of exchange, electronic seals and durable media;

b) Developing the capacity of the EBSI network and blockchain applications in public sector services through the EUROPEUM EDIC multi-country actor co-founded by Poland. Developing good practices in all tested and implemented applications of blockchain technology in cross-border services. Standardising processes in services and interoperability across distributed systems of registers and service providers, while preserving their local sovereignty, equitable access and usability within the European ecosystem;

c) Integrating blockchain technology applications into financial and capital markets infrastructure, including the ability to tokenise different categories of securities and different categories of holding rights, as well as payment systems and share registries;

d) Strengthening the cybersecurity of blockchain technology and using blockchain to solve certain cybersecurity problems e.g. in AI systems.



4.4. Space technologies

Diagnosis – what is it like?

Although the space industry is embracing digital technologies and is ready to introduce new ones, it still faces problems in cooperation between participants in advanced projects. The space domain has to implement digitisation in a constrained context, driven by processes, organisation and technological experience. This involves ensuring that the interoperability needs of all tools are met between disciplines, across the lifecycle and throughout the supply chain. To that end, in its “ESA AGENDA 2025: Make space for Europe”, the European Space Agency (ESA) harmonised the necessary undertakings by indicating to the space sector, and especially to ESA Member State Delegations, the lines of action for the development and implementation of complex and ambitious space missions and programmes together with industry. ESA has also ensured that it will fully digitalise project management, enabling the development of replicable digital twins through model-based systems engineering and procurement and finance, achieving full digital compatibility with the industry.

Similarly to other countries, Poland considers an indigenous space sector as a strategic and business resource, which is gaining increasing importance for the national economy and is driving more and more international cooperation.

Poland’s accession to the ESA has enabled even greater progress in the development of space technologies and satellite solutions by Polish industry, and the increased level of investment from the state budget, both in optional and mandatory programmes, makes it possible to provide the state administration with satellite data, support Polish entities in acquiring space experience, invest in dedicated laboratory and test infrastructure, and develop capabilities in selected areas of space technology that have an impact on enhancing the broadly understood security of our country.

However, Poland's membership and the participation of Polish space companies in ESA projects also involve the strict implementation of guidelines resulting from regulations, standards and other documents covering, among other things, the need for digitisation in the field of engineering. As a result, Polish actors gain the invaluable experience required in the space sector. This allows systems engineers and project teams to master the complexity of a space system, express the concept of operations clearly, structure the requirements and follow them from design and production through to testing. These practical skills clearly indicate that Poland is in line with the digitisation goals indicated by ESA while fostering technological progress at home and contributing to meeting national needs, as well as increasing the competitive potential of the Polish space industry on global markets.

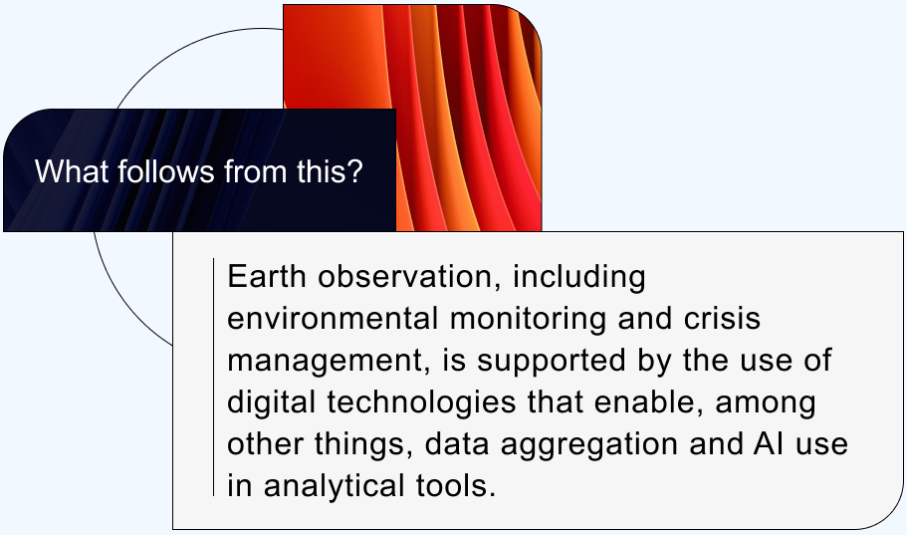
Objective 1: Earth observation technologies are being improved for environmental monitoring and disaster management

What will make it possible to achieve the objective:

a) Creating a centralised platform to aggregate data from various space missions, satellites and sensors;

b) Implementing advanced analytical tools using AI to process and interpret data for forecasting and real-time decision support, e.g. in crisis management;

c) Using digital satellite twin technology to optimise satellite performance, fault prediction and lifecycle management.



Objective 2: Space infrastructure is secure

What will make it possible to achieve the objective:

a) Implementing comprehensive cybersecurity measures to protect space systems and data from threats, ensuring operational continuity;

b) Implementing quantum communication systems for secure data transmission;

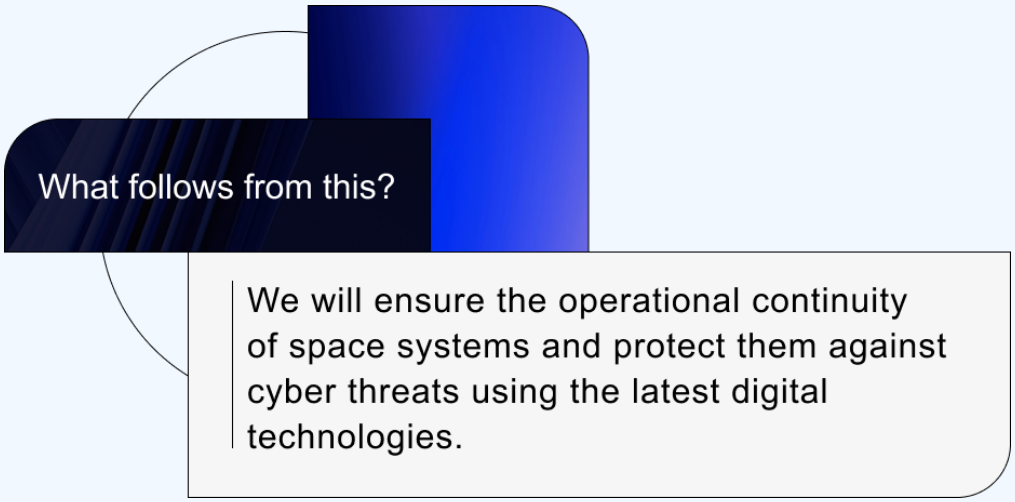
c) Developing and implementing advanced space traffic management systems — space debris and satellite collision tracking and management technologies;

d) Supporting the development of AI, automation and robotics for autonomous satellite operations, anomaly detection, servicing, repair and on-orbit assembly.

e) Developing and implementing IT tools for the control of launch systems and space vehicles and ensuring their flight safety;

f) On-board computers (ACOS) — control algorithms for rocket manoeuvres, in-orbit approach manoeuvres, space vehicle fuel optimisation, etc.;

g) Developing software for calculation of space vehicle manoeuvres: calculation of rocket trajectories, fall zones, aerodynamic and thrust vector control modelling and special dual-use modules.



4.5 Financing and support for innovation

Diagnosis – what is it like?

In 2023, Poland ranked as low as 17th in the European Union and 20th in Europe in terms of capital invested in startups at different stages of growth. Despite the increase in the scale of funding, Poland's percentage share of total capital invested by venture capital/private equity (VC/PE) funds in Europe in the last three years (2021–2023) decreased slightly compared to the previous three-year period (2018–2020). The Netherlands, Norway, Estonia, Austria and Germany recorded the largest increases. In 2023, Warsaw came in a high 3rd place among CEE cities in terms of nominal value of invested capital; however, the CEE itself is still 70% lower than, for example, the DACH region (Germany, Austria, Switzerland) in terms of the share of startup funding in the GDP. Funding for startups at the pre-seed and seed stages has increased in Poland in recent years, but funding at later stages of development is still an issue.

At the national level, several measures have been taken in recent years to increase funding, not least of which is the increased activity of the Polish Development Fund (PFR). It has played a key role in increasing funding, supporting more than 60 funds through PFR Ventures, based on a Fund of Funds basis. PFR's activities have attracted a number of foreign VC funds to Poland.

Diagnosed problems in the area of financing include the lack of possibility for pension funds to finance startups, the lack of effective cooperation between commercial banks and Bank Gospodarstwa Krajowego (BGK), many legal barriers in the banking sector for financing startups through debt instruments and the insufficiently effective activities of publicly funded accelerators. While the data shows a relatively high number of startups in Poland, this is because the Polish economy is one of the largest in the EU.

In terms of the number of all startups, including those without secured funding, Poland ranks 9th in the EU and 11th in Europe. Yet, when it comes to the number of startups that have received funding per capita, Poland ranks as low as 23rd in the EU. The same applies in the case of the so-called unicorn companies (innovative enterprises valued at more than USD 1 billion): while Poland nominally ranks 9th, it ranks only 22nd per capita.

Over the past five years, the CEE region's share of the total value of startups in Europe has increased from 4.9% in 2019 to 5.7% in 2023. In terms of growth in the total value of startups over the past five years, Poland ranked 6th in the CEE region (a 240 per cent increase, compared to 740 per cent in Croatia). As regards its share of the total value of the TOP100 largest technology companies in the CEE, Poland ranks 1st with a share of 38%.

One can notice several differences when comparing the Polish startup ecosystem with that of leading EU countries, including the lack of a comprehensive programme to facilitate cooperation between state-owned companies and startups, insufficient support for the development of the innovation ecosystem and insufficient promotion of Poland as an innovation hub.

Objective 1: An integrated and efficient funding system for startups and scaleups is in place

What will make it possible to achieve the objective:

a) Integrating the financial community (VC funds, BGK, Warsaw Stock Exchange, private banks) to intensify cooperation and develop solutions for mobilising capital for startups;

b) Introducing fiscal incentives for domestic and foreign institutional and private investors (including large companies) for investments in startups;

c) Improving the ecosystem of publicly funded accelerators, in partnership with private investors, and seeking co-investment opportunities with the world's leading accelerators.

Objective 2: Startups and scaleups grow without investment barriers

What will make it possible to achieve the objective:

a) Identifying and removing regulatory barriers to startup growth and scaling;

b) Enabling the creation of targeted special purpose vehicles (SPVs) to invest in funds or startups;

c) Adapting administrative procedures to increase interest among foreign entities in running innovative companies and investing in Poland;

d) Developing legal solutions to attract talent from abroad.

Objective 3: The state is increasing the talent pool and the number of ecosystem players in Poland

What will make it possible to achieve the objective:

a) Recognising the so-called ICT digital nomads from outside the EU as preferable from the point of view of migration policy; creating a programme showing them the advantages of settling permanently in Poland;

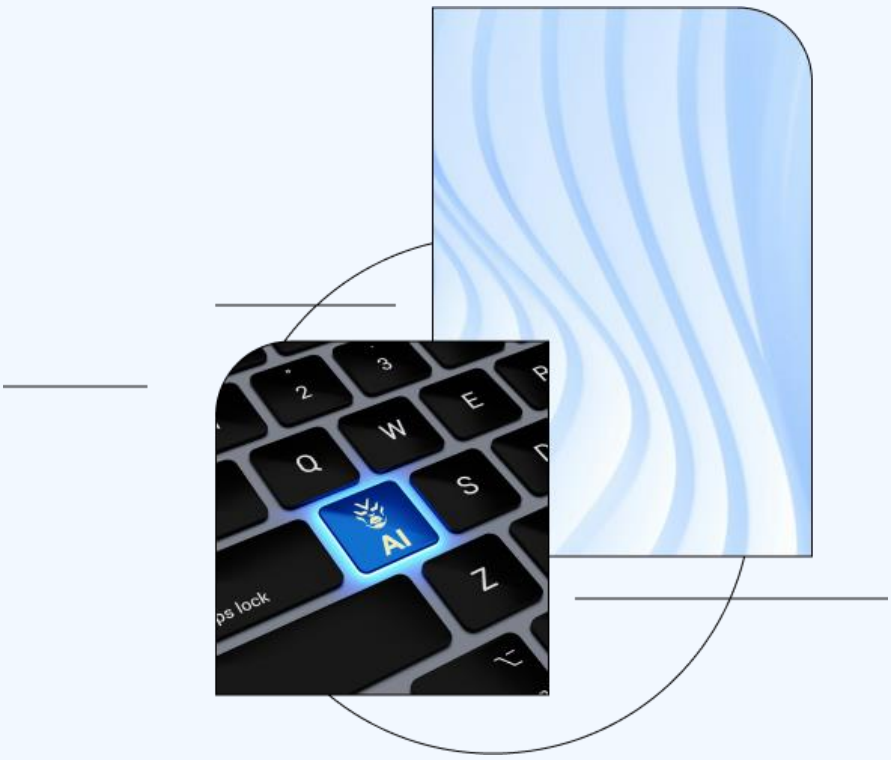
b) Developing public administration support for a certain pool of foreign ICT talent before they arrived in Poland, in cooperation with employment and relocation support agencies. Its scope will include administrative procedures and logistical assistance.

4.6. Open source

Diagnosis – what is it like?

Although Poland is a country with a strong IT sector, it makes little use of the potential of open-source software. Indeed, it is one of the few EU countries that do not have a strategy to develop and support open-source software[49]. Such software is underutilised in public administration, even though it is complementary to the development of the open data ecosystem, which is at a high level in Poland.

At the same time, the creation and use of open-source software is a vital tool to ensure digital sovereignty. It reduces reliance on specific commercial software, increases transparency and control over the technologies used, and is more cost-effective. Open source software also helps build links between the IT sector and the diverse communities developing and using the technology. One example of this approach in recent years is the development of Polish open-language models.



49 Blind, K.; Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Pätsch, S., Schubert, T. (2021). The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy, Final Study Report. Brussels, p. 226.

Objective 1: Polish public administration is making greater use of open-source software.

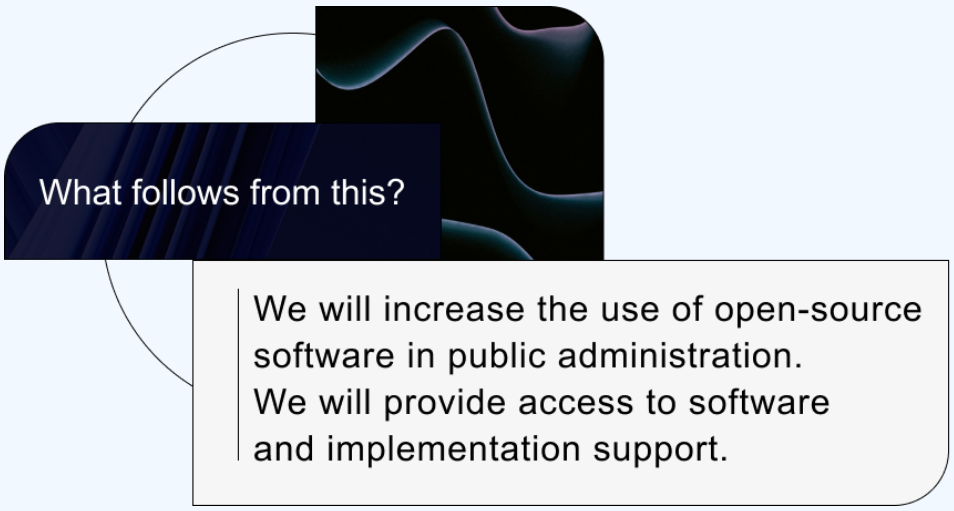
What will make it possible to achieve the objective:

a) Identifying an entity responsible for coordinating the development and implementation of open-source software in the Polish public administration, as well as the development of competencies in this area;

b) Developing a programme for the implementation of open-source software in the Polish administration, including standards for software use and pilot projects;

c) Defining tender rules for IT solution implementations in public administration that will support the use of open-source software;

d) Establishing an open-source software repository for the Polish administration.



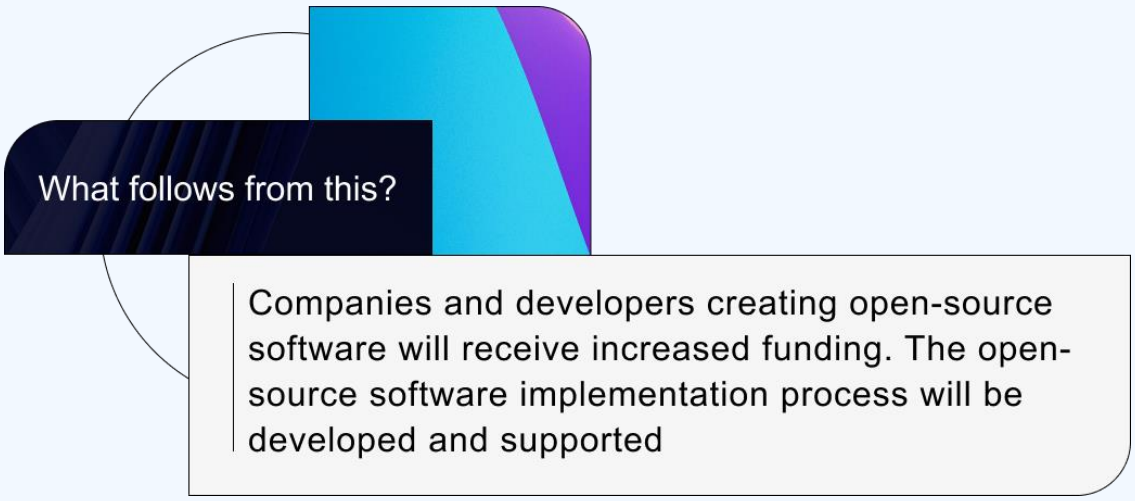
Objective 2: Increased open-source software development and use by Polish companies and Polish developers.

What will make it possible to achieve the objective:

a) Introducing a funding instrument for companies and developers to create open-source software;

b) Supporting the development of open artificial intelligence systems and their implementation in public administration;

c) Supporting the development of open solutions for local governments — combined support for local companies and municipalities implementing software.



4.7 Digital and green transition

Diagnosis – what is it like?

In Poland today, the implementation of green and digital transition initiatives is mainly driven by EU regulatory requirements and guidelines for financing projects from EU funds rather than by the ambitious strategy chosen by the state for the so-called twin transition. The activities proposed in this area in the National Plan for the “Path to the Digital Decade” policy programme focus primarily on the creation of sandboxes for AI solutions, participation in the European Commission's Earth Destination initiative, as well as investments and requirements related to the implementation of environmental innovations (primarily the closed loop economy). The impact of state digital solutions on the environment and climate change has also received little attention to date. At the same time, it is known that the carbon footprint generated by the production and use of digital solutions is steadily increasing in Poland and worldwide. Global emissions from the ICT sector are estimated to be between 4% and 10%[50] higher than those generated by the aviation industry.

There is therefore a need for a more comprehensive approach to digital and green transition than has been the case to date.

Further, inter-ministerial cooperation is required to address the issues of the energy intensity of digital tools, the potential of technology to combat climate change and reduce emissions, as well as digital ecology.

There is a growing awareness among Polish entrepreneurs of the impact of new technologies on the environment and climate. According to recent data,[51] more than 64% of ICT companies pay attention to issues such as energy consumption and the ease of replacing parts when choosing equipment or service providers. At the same time, there is a lack of systems to monitor the environmental impact of digital technologies used by companies. For the time being, the obligation to report on climate risk issues under the Corporate Sustainability Reporting Directive (CSRD) only applies to the largest listed companies. This, in turn, can lead to limited reporting or greenwashing (misrepresenting products or services as green) by smaller and unlisted entities. In terms of certification, there are EU technology verification schemes, such as ETV[52] (Environmental Technology Verification). However, they relate primarily to environmental technologies (i.e. those aimed at reducing greenhouse gas emissions and limiting the consumption of resources like water and raw materials) rather than to ICT sector products, which are increasingly responsible for

50 https://www.sciencedirect.com/science/article/pii/S2666389921001884

51https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_in_enterprises_and_the_environment.

52 https://lifeproetv.eu/pl/strona-glowna/

energy consumption. Moreover, they are voluntary, which may cast doubt as to their effectiveness.

The first Polish survey on digital ecology[53] suggests that the citizens' awareness in this regard is low.

Terms such as "digital footprint" and "digital ecology" are clear to as few as 19% and 12%, respectively, of those not involved in the ICT sector. This percentage was higher among people involved in the IT industry but was still only 25%. The term "digital ecology" proved even less widely known, as only 23% of IT professionals and 12% of other respondents were familiar with it.

53 https://blog.theprotocol.it/artykul/cyfrowa-ekologia-w-pracy-i-zyciu-polakow-raport-theprotocol

Objective 1: Energy, environment and climate data are available and re-used by both public administration bodies and third-party stakeholders to conduct analyses and research for the optimisation of the energy sector

What will make it possible to achieve the objective:

a) Revising the model for conducting statistical surveys in such areas as the condition and protection of the environment, materials and fuel and energy markets, as well as forestry and hunting. Access to the results of statistical surveys commissioned by the relevant minister should, in principle, be equitable, equivalent and simultaneous,[54] and should also be free of charge. To achieve this, it is necessary to remove barriers to data accessibility such as payments for accessing content published by statistical research providers and to enforce high standards of data openness (elimination of file formats that block machine reading of data). It is also crucial to ensure the consistency of reported data and the coherence of the methodology used by the institutions sharing responsibility for conducting statistical surveys;

b) Mobilising the national energy and mining sectors to voluntarily publish data of significant social value, e.g. information on pollution and environmental use as well as employment and local impacts. Developing and implementing a data plan and governance model in line with the EU Data Governance Act (DGA) and focused on regularly increasing the dataset made available based on the needs of government, civil society, the private sector and the expert community.

54 https://bip.stat.gov.pl/files/gfx/bip/pl/defaultstronaopisowa/566/1/1/zasady_postepowania_z_danymi_statystycznymi_streszczenie.docx

What follows from this?

Public administration bodies and external entities can use data to conduct energy sector studies. Study results will be published free of charge and in a machine-readable manner.

Objective 2: Energy systems, including district heating, are based on innovative management and optimisation systems

What will make it possible to achieve the objective:

a) Bolstering cybersecurity and providing digital infrastructure to support innovation, such as advanced energy storage, artificial intelligence in the energy sector and grid-edge devices, which will allow the integration of RES energy into existing generation capacity, distribution and transmission networks and ensure continuity of supply and the smooth operation of the energy system;

b) Inter-ministerial cooperation on updating and implementing strategic documents on energy sector transition (e.g. the National Energy and Climate Plan [NECP] for 2021–2030) to comprehensively address the digitisation of the energy system;

c) Further development of smart grids in line with EU interoperability rules, “Clean Energy Package” Working Group guidelines55 and NECP project assumptions. The increasing use of smart meters enables the expansion of smart grids and the digitisation of the energy system (with improved metering, efficiency and smart control). In the future, it will also be crucial to deploy increasingly sophisticated AI tools to process real-time knowledge about the shape of the local and national energy markets — analysing increasing amounts of data from a growing set of prosumers, as well as atmospheric phenomena to forecast energy consumption, and data from sensors and IoT devices that report on the habits of energy consumers;

d) Supporting, in parallel with the digitisation of the electricity system, the development of similar solutions in district heating. These solutions will enable the mapping of the entire district heating network or the creation of a complete digital network model, integrated with other systems used at the given district heating company;

e) Fostering innovation in the energy sector through investment in research and development (R&D) and training of ICT professionals focused on creating digital solutions for the energy sector.

55 https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Smart Grids and Meters/Smart Grids/finalreportwg-cep_2019.pdf

What follows from this?

We will improve the functioning of the energy sector by increasing the use of digital solutions, investing in research and development and ensuring the development of ICT specialists.

Objective 3: The environmental impact of ICT solutions used by public administration is reviewed and reduced

What will make it possible to achieve the objective:

a) Measuring the digital carbon footprint of the public administration as generated by the use of electronic devices and the Internet in the public sector, as well as the energy consumption required to maintain the national infrastructure (data centres, servers);

b) Mapping and monitoring the supply chain of ICT systems and services used in public administration. Developing energy consumption standards for ICT systems and services that are factored into public procurement, and rewarding ICT system and service providers that have committed to achieving climate neutrality by 2050 (in line with the Paris Agreement) or sooner by providing a robust action plan and demonstrating documented progress towards meeting their milestones;

c) Formulating the principles of sustainable ICT and digital ecology in public administration bodies and considering them when designing national public policies and strategies.

Objective 4: An environmentally friendly ICT sector

What will make it possible to achieve the objective:

a) Promoting the development and use of energy-efficient solutions among telecommunications undertakings. Striving for greater energy efficiency in network design, construction and operation, including ensuring that network equipment is replaced with more energy-efficient hardware incorporating energy-saving features in idle components and AI-driven optimisation;

b) Working with the ICT sector, technology industry companies, higher education institutions and research institutes to prepare guidelines and best practices on sustainability in the design of digital products and services;

c) Encouraging data centre operators to take into account the good practices listed in the European Code of Conduct for Energy Efficiency of Data Centres[56];

d) Encouraging the development of environmentally friendly digital tools generating solutions through thematic competitions and “hackathons”.

56https://joint-research-centre.ec.europa.eu/scientific-activities-z/energy-efficiency/energy-efficiency-products/code-conduct-ict/european-code-conduct-energy-efficiency-data-centres_en

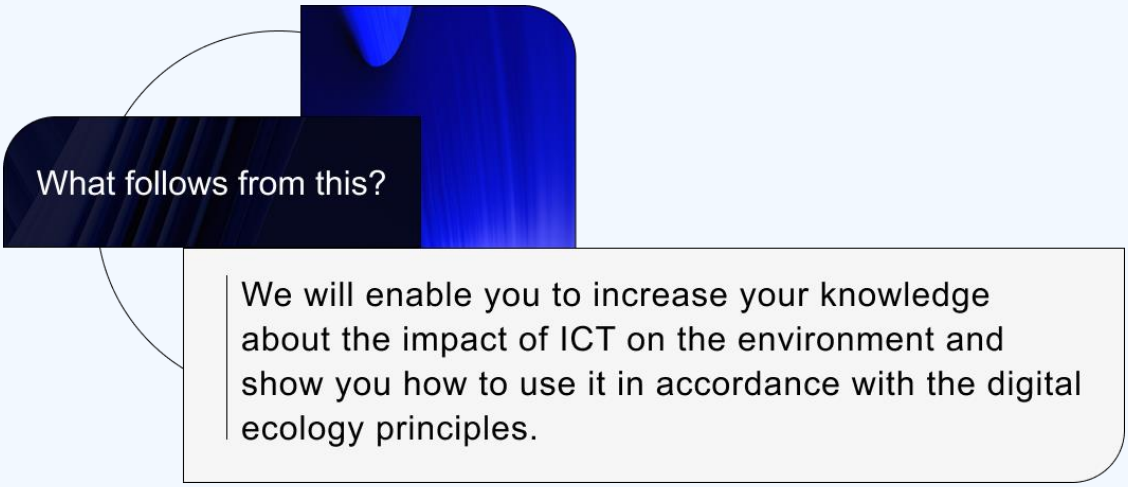
Objective 5: Citizens are aware of the impact of ICT on the environment and have a basic knowledge of digital ecology

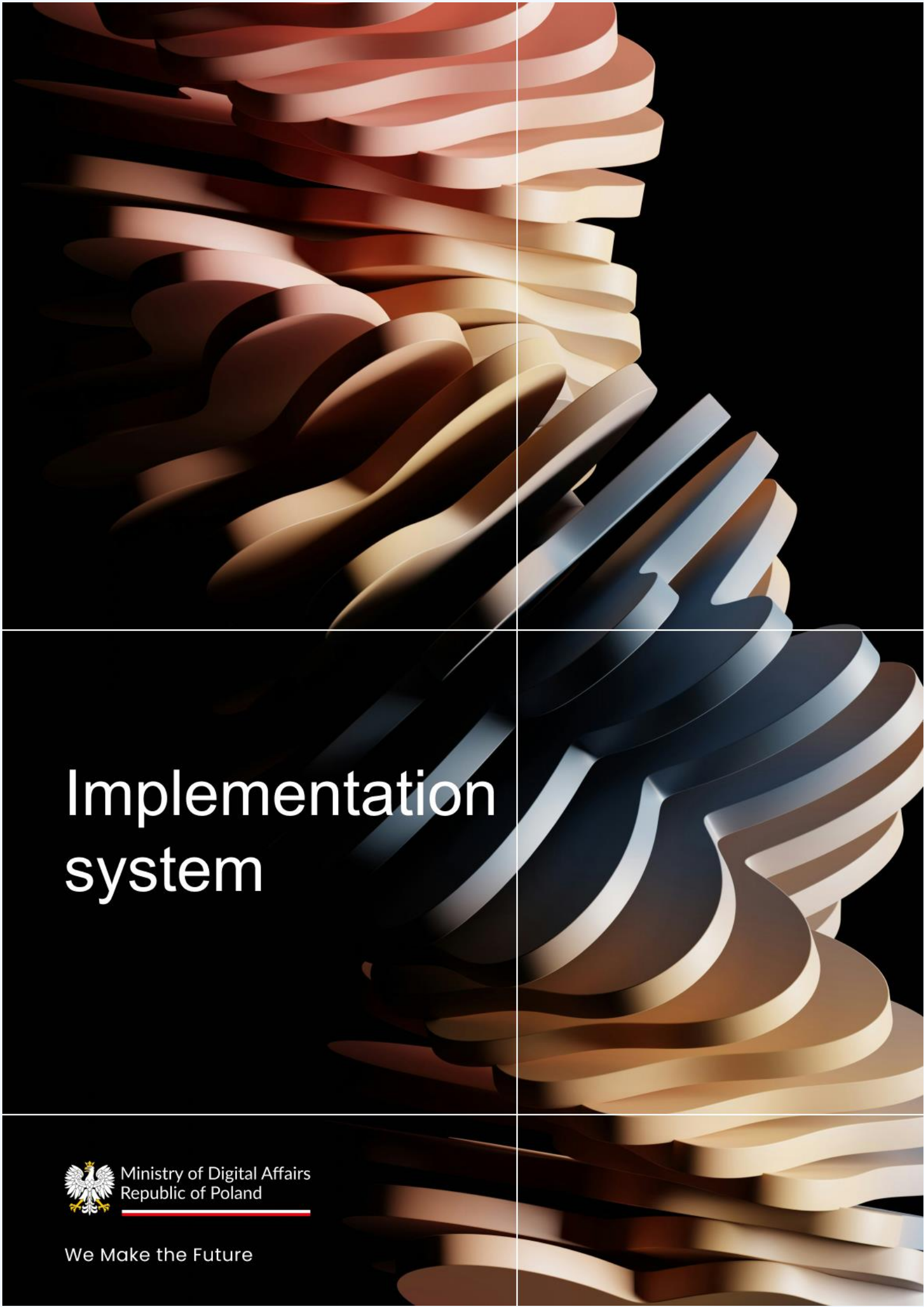
What will make it possible to achieve the objective:

a) Integrating the environmental impact of using ICT services into curricula and educating on how to use technology in a more sustainable way. Conducting social and educational campaigns to raise awareness of the above issues;

b) Raising awareness of the importance of recycling appliances and increasing the availability of electronic waste collection centres;

c) Promoting sustainability standards and labels for digital products and services.





Implementation system

Ministry of Digital Affairs
Republic of Poland

We Make the Future

Implementation system

Coordination

Responsibility for coordinating the activities aimed at implementing the Strategy will rest with the minister responsible for computerisation.

Digitisation is a cross-cutting and multidimensional process, as reflected in the broad focus of this Strategy. Achieving its main objective of enhancing quality of life through digitisation requires the involvement and close cooperation of many public sector actors. However, the intervention in this regard is not limited to the sphere of state operation but also implies inspiring digital transition efforts with the involvement of the private sector.

A special role in the process of implementing the Strategy will be played by plenipotentiaries for computerisation, who must be appointed in offices serving the ministers in charge of government administration departments and in the Chancellery of the Prime Minister (and optionally in other offices). The plenipotentiaries' activities will focus on matters falling within the competencies of the government administration department headed by the relevant minister, including those managed by organisational units or bodies subordinate to and supervised by that minister. Their main task will be to coordinate the Strategy's implementation, including through the preparation of updates on progress and related risks, as well as to diagnose areas requiring change for further implementation of the Strategy and the introduction of new digital technologies.

Implementing the Strategy requires coherent, harmonised and consistent actions which, however, often cut across the traditional division of state activity and areas vertical with respect to government departments. It is expected that this will be facilitated by the day-to-day interaction of the appointed plenipotentiaries for computerisation and, on an institutional level, will be made possible by the role of the Committee for Digitisation.

The Committee for Digitalisation will be tasked with ensuring the coordination of the state's digitalisation activities and supporting its digital development, which is essential for the implementation of the Strategy. The activity of the Committee for Digitalisation, which involves reviewing and monitoring public-use IT projects, will enhance the coordination of such projects by ensuring their consistency with the state's strategic activities, including their alignment with the Strategy and the State Information Architecture (AIP). On the other hand, making public funding for public-use IT projects conditional on a positive assessment by the Committee for Digitalisation will have a positive impact on increasing the interoperability and complementarity of national IT solutions, as well as on increasing the efficiency of managing public funds.

Achieving the main objective of the Strategy requires that this involvement of multiple public sector actors, as referred to above, should be multidirectional and multilevel. Indeed, measures to achieve the objective will be implemented in the form of programmes, projects, legislation and technical regulations.

Reviewing

Considering the need for good planning, consistency and continuity in the state's digitalisation processes, the Strategy covers a multi-year perspective. However, the pace of technological development and the difficulty in predicting its long-term trends necessitates that the Strategy be regularly reviewed and updated as required. The minister in charge of computerisation will work with members of the Council of Ministers to review the Strategy every 2 years and submit a report on this to the Council of Ministers within 2 months of completing the review. Plenipotentiaries for computerisation will be required to compile information on the Strategy's implementation for review.

Monitoring

The Minister in charge of computerisation will monitor the implementation of the Strategy once a year. The monitoring system includes an examination of the progress of planned activities under the horizontal and directional objectives and a quantitative study of the degree to which the adopted performance indicators included in Table 1 have been achieved. The results of the Strategy implementation monitoring will be submitted to the Committee for Digitalisation in the form of a report and published on the website of the Ministry of Digital Affairs within 3 months after the end of the preceding calendar year.

The report will be drawn up by the minister in charge of computerisation and be based on the following in particular:

a) information provided by the plenipotentiaries for computerisation on each of the actions planned in the Strategy and statistical data in relation to the indicators adopted, in accordance with the jurisdiction of each member of the Council of Ministers;

b) analysis of data sources for the key performance indicators identified in Table 1.

The report will include: descriptions of the actions taken, as planned in the Strategy, together with an assessment of their progress, any identified problems with their implementation, and recommendations for the individual members of the Committee for Digitalisation for the next period.

An integral element of the Strategy's monitoring will be a set of performance indicators relating to the objectives set in each area, with an indication of the baseline and target values. The data sources for the measurement of indicators will be primarily official statistics, but also the Inventory System for ICT Systems (SIST), reports on the activities of the Committee for Digitalisation, own data of the entities responsible for the implementation of individual activities and available cyclical reports and market research.

The table below presents the indicators identified for the Strategy.

Table 1 — performance indicators

No.	Area	Indicator name	Baseline	Target	Attainment deadline	Data source
1	Coordinating the digital transition of the country	Share of offices serving ministers in charge of government administration departments, which have appointed a plenipotentiary for computerisation, in the overall number of offices serving ministers in charge of public administration departments and the Chancellery of the Prime Minister	0%	100%	2026	Own data of the Ministry of Digital Affairs/Committee for Digitalisation
2		Share of public-use IT projects whose assumptions are in line with the State Information Architecture's principles, standards, guidelines and architectural recommendations in the total number of public-use IT projects whose assumptions are reviewed by the Committee for Digitalisation.	0%	100%	2035	MonaLiza/Committee for Digitalisation
3	Electronic communications	Universal access to mobile telecommunications services of at least 100 Mbps	57%	100% of the country's area	2035	Office of Electronic Communications
4	Digital competencies	Percentage of people with at least basic digital skills	44.3% (2023 data)	85% of people aged 16–74	2035	Statistics Poland
5		Percentage of people with digital competencies above the basic level	20.1% (2023 data)	50% of people aged 16–74	2035	Statistics Poland
6		Share of ICT specialists in the workforce	4.3%	10% of the workforce	2035	Statistics Poland
7		Share of women among ICT professionals	19.1%	35%	2035	Statistics Poland

8	Cybersecurity	Establishment of a central institution responsible for cybersecurity at the national level	0	1	2025/2026	Own data of the Ministry of Digital Affairs
9		Creation of a classified cloud — full operational capability	0	1	2029	Own data of the Ministry of Digital Affairs
10		Implementation of a mechanism to exclude high-risk suppliers	0	1	2026	Own data of the Ministry of Digital Affairs
11		Percentage of incidents reported to CSIRT teams in a timely manner by legally obliged entities of the National Cybersecurity System	Baseline to be determined at a later stage	100%	2035	CSIRT teams
12	Public e-services	All key e-services are available through the mObywatel app	Baseline to be determined at a later stage	100%	2035	Own data of the Centre for Information Technology
13		Percentage of cases handled electronically by entities performing public activities in relation to all cases	Baseline to be determined at a later stage	100%	2035	
14		Integrating at least one institution/office in each of Poland’s local government units with the ePłatności service	2%	100%	2035	Own data of the Centre for Information Technology
15	Digitalising administrative processes and judicial proceedings	Share of entities performing public tasks using an Electronic Document Management system in relation to their total number	86% (2022 data)	100%	2035	Statistics Poland report

16		Percentage of public administration offices using artificial intelligence technologies	Baseline to be determined at a later stage	80%	2035	
17	Systems and registers	Share of public ICT systems for which API descriptions have been made available in the interoperability repository, relative to the number of public ICT systems monitored in the Inventory System for ICT Systems (SIST).	0%	100%	2035	Inventory System for ICT Systems (SIST)
18		Legal status of reference public registers	0	1	2027	Own data of the Ministry of Digital Affairs
19	Digital identity	Number of electronic identification means issued for legal persons and natural persons representing legal persons (whether there is a representative with such means at the given legal entity)	0%	50% of eligible entities	2035	Own data of the Centre for Information Technology
20		Number of EU digital identity wallets activated	0	20 mln users	2035	Own data of the Centre for Information Technology
21	Cloud computing	A minimum of 70% of the systems for providing digital public services use a shared computing infrastructure (cloud computing)	0	70%	2035	Own data of the Centre for Information Technology
22	Open data and data sharing	Number of data resources shared at dane.gov.pl	41,500 (as of the end of 2024)	100,000	2035	dane.gov.pl

23	Secure digital space	Creating and introducing a system to evaluate the ethical dimension of AI tools used by the state	0	1	2025	Own data of the Ministry of Digital Affairs
24		Establishing a body responsible for overseeing and integrating the activities of the various actors involved in countering disinformation	0	1	2026	Own data of the Ministry of Digital Affairs
25	Digital health	Percentage of medical entities maintaining an EHR system, connected to the P1 system and exchanging documentation electronically	18%	100%	2035	e-Health Centre
26		Number of completed scientific studies and research projects based on available real-world data in the first 3 years of operation of the developed data sharing system	0	3500	2035	e-Health Centre
27		Introducing prediction and screening tools in the central system	0	Tools implemented for at least 100 disease entities	2035	e-Health Centre
28	Creative industries	Value growth of the Polish video games market	USD 1,286,000,000 (2022)	USD 3,669,000,00057 (10% annual growth)	2035	Polish Agency for Enterprise Development (PARP)
29	Digital academia	Number of ICT graduates (ISCED disciplines 0610, 0611, 0612, 0613, 0618, 0619, 0688)58	15,279 (as of the end of 2023)	20,000	2035	Ministry of Science and Higher Education,

57 In 2022 prices

58 ISCED — International Standard Classification of Education is a system for collecting, collating and analysing internationally comparable education statistics. Disciplines considered for the indicator: 0610 — Information and Communication Technologies (ICTs), not further defined; 0611 — Computer use; 0612 — Database and network design and administration; 0613 — Software and applications development and analysis; 0618 — Information and Communication Technologies (ICTs), inter-disciplinary programmes; 0619 — Information and

						POL_on System
30		Computing power for HPC computing available in PLGrid	70 petaflops	1 exaflop	2035	PLGrid report
31		Computing power for AI computing available in PLGrid	3 exaflops	40 exaflops	2035	PLGrid report
32	Digital transition of businesses	Share of SMEs using digital technologies at least at a basic level	50% (2023)	92%	2035	Statistics Poland
33		Percentage of SMEs using artificial intelligence technologies	3.7% (2023)	50%	2035	Statistics Poland
34	Artificial intelligence	Creating a mechanism to coordinate the implementation and financing of AI projects in public administration		0 1	2026	Own data of the Ministry of Digital Affairs
35	Other disruptive technologies	Establishing a multi-year programme to support the development of disruptive technologies		0 1	2026	Own data of the Ministry of Digital Affairs
36	Open source	Creation of an Open Source Programme Office		0 1	2035	Own data of the Ministry of Digital Affairs

Communication Technologies (ICTs), not elsewhere classified; 0688 — Information and Communication Technologies (ICTs), inter-disciplinary programmes.

37	Digital and green transition	Percentage of households equipped with smart utility meters	33%	100%	2031	Monitoring the implementation of the Energy Policy of Poland until 2040 (PEP 2040)

Funding

The measures collected and proposed in the Strategy are cross-cutting and affect many areas, such as national security, maintaining a competitive economy, education and scientific and technological progress. The planned activities will be carried out by various actors, with financial contributions from the following sources in particular:

- state budget — the Strategy's objectives will be implemented through public interventions financed from portions of the state budget, which are managed by the individual ministers. Additionally, the state budget will provide co-financing for projects implemented with foreign funding;
- local government unit budgets;
- funding from other bodies carrying out public tasks;
- earmarked funds, including Broadband Fund, Cybersecurity Fund, Central Register of Vehicles and Drivers (CEPIK);
- Recovery and Resilience Facility (RRF): National Recovery and Resilience Plan;
- European funds for the Cohesion Policy (including the European Funds for Digital Development Programme for 2021–2027, the European Funds for Social Development Programme for 2021–2027, as well as the European Funds for the Modern Economy) and the Common Agricultural Policy 2021–2027 and 2028–2034;
- other European instruments and programmes, including the Connecting Europe Facility; Digital Europe; Horizon Europe and the Citizens, Equality, Rights And Values Programme (CERV);
- other public funds, including funds from foreign sources (e.g. the Norwegian Financial Mechanism), other instruments operating based on public funds, e.g. BGK's instruments included in the portfolio of the Polish Development Fund Group;
- financial instruments of international financial institutions (from loans, guarantees, shareholdings, Venture Capital funds);
- private funds — the implementation of the Strategy's objectives will also require the involvement of private funds, in particular, in providing co-financing for projects co-financed with EU funds;
- National Health Fund (NHF), as well as patient co-payments for healthcare services (e.g. in pharmacy reimbursement) and co-payment by technology providers (e.g. risk-sharing instruments, data stakeholders);

The costs of implementing the tasks and sustaining the effects of the Strategy will be financed within the annually set expenditure limit for the individual budget parts. The final amount of funds earmarked for individual projects will be planned annually by the Council of Ministers when preparing the Budget Act.

National expenditure will be supported by European funds in the 2021–2027 and 2028–2035 financial perspectives. EU funds are expected to remain important in the 2028–2035 financial perspective, although relatively less so. Public interventions will be financed to a greater extent with national public funds. It will be important to focus EU funds on projects with the highest added value and positive externalities. At the same time, considering the need to allocate significant resources to digitalisation, it may be necessary to revise the structure of funding for the industry's development, which largely focuses on the telecommunications sector’s contributions while leaving out other players who benefit from shared infrastructure.

Glossary

- State Information Architecture (AIP) — a method of managing state informatisation, based on architectural models and including basic principles, standards, guidelines and architectural recommendations;
- Blockchain — a complex combination of cryptographic and distributed systems technologies to authenticate data across different transaction processes. It allows parties who do not know each other to have confidence in processes, procedures or measurements, without the need for intermediaries to guarantee such confidence. It is sometimes also associated with the term WEB 3.0;
- Information Sharing and Analysis Centres (ISAC) — centres for sharing knowledge and experience of cybersecurity incidents in a particular sector of the economy;
- Cloud computing — modern technology for storing, processing and managing data. It is based on shared resources (software and infrastructure). It is provided by a supplier from within the organisation or by a third-party supplier. The resources are accessed online;
- Corporate Sustainability Reporting Directive (CSRD) — Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting. The directive requires reporting on climate risk issues;
- Digital Economy and Society Index (DESI) — a digital economy and society index launched by the European Commission as a tool to monitor indicators of digital progress in EU Member States;
- E-Doręczenia — the electronic equivalent of a registered letter with recorded delivery. With this service, public entities, citizens and companies can benefit from convenient and secure electronic delivery. Such delivery is legally equivalent to traditional registered mail with recorded delivery.
- Electronic Platform for Public Administration Services (ePUAP) — an ICT system in which public institutions make services available through a single online access point (Article 3(13) of the Act of 17 February 2005 on the computerisation of activities of entities performing public tasks (Dz.U. /Journal of Laws/ of 2024, items 304, 1222);
- European Interoperability Framework (EIF) — the EU’s commonly agreed approach to delivering European public services in an interoperable way. They set out basic interoperability guidelines in the form of common principles, models and recommendations;
- European High Performance Computing Joint Undertaking (EuroHPC JU) — a joint initiative between the EU, European countries and private partners to develop a World Class Supercomputing Ecosystem in Europe.

- Venture Capital Funds (VC Funds) — a high-risk financing model for investment in early-stage business ventures. VC funds generally invest in innovative ventures created by small companies, hoping for a high rate of return;
- Private Equity Funds (PE Funds) — a funding model where funds raised are invested in companies with high potential for value growth. Unlike VC funds, PE funds also invest in companies at later stages of development;
- Generative artificial intelligence (GenAI) — a technology that allows users to create new content using prompts. GenAI algorithms work based on data provided both at the development stage and during use;
- Hackathon — an event where programmers, designers and other specialists work together intensively to solve a specific problem or create a new product in a short time, usually between 24 and 72 hours;
- ICT (Information and Communication Technologies) — a family of technologies that enable the processing, collection and transmission of information in electronic form;
- Smart city — an urban area where technology and data collection help to improve the quality of life, as well as the sustainability and efficiency of city operations. One of the technologies used in smart cities is the Internet of Things (IoT);
- Smart village — a rural area that uses modern technology for sustainable and innovative development and to improve the quality and standard of living of its inhabitants;
- Application Programming Interface (API) — a set of technical functions enabling the connection and mutual exchange of data or metadata between computer software or ICT systems (Article 2(9) of the Act of 11 August 2021 on open data and reuse of public sector information (Dz.U. /Journal of Laws/ of 2023, item 1524);
- Internet of Things (IoT) — systems consisting of interconnected devices, often referred to as “smart devices”. These devices collect and exchange data with each other and can be controlled and monitored via the Internet;
- SME — a micro, small or medium-sized enterprise within the meaning of Article 2 of the Annex to Commission Recommendation 2003/361/EC59;
- Nationwide Educational Network (OSE) — a public telecommunications network programme offering schools fast (100 Mbps), free and secure internet access;
- Open source software — a type of software whose source code is publicly available and can be freely modified and distributed by users;
- PLGrid — a nationwide computing infrastructure built to support research and development work for a wide range of scientific and economic fields. The PLGrid provides access to supercomputers, quantum computers, specialised artificial intelligence accelerators, cloud computing, disk storage, optimised computing software and expert support from across Poland;
- Industry 4.0 — a term referring to the fourth industrial revolution, which entails the integration of intelligent machines and systems, as well as changes to production processes designed to increase manufacturing efficiency and enable flexible product

59Commission Recommendation 2003/361/CE of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36)

range changes. Industry 4.0 is not only about technology but also about new ways of working and the role of people in industry;

- Public register — a structured dataset for the performance of public tasks, maintained under statutory provisions by an entity performing public tasks;
- eIDAS 2.0 Regulation — Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (OJ L, 2024/1183, 30.4.2024);
- Gigabit Infrastructure Act (GIA) — the EU's gigabit infrastructure regulation, which aims to streamline and accelerate the deployment of very high capacity networks (VHCN), such as fibre and 5G, across Europe;
- Augmented Reality (AR) — a technology that combines virtual elements with the real world to create interactive and enriched experiences for users;
- Silver economy — a sector of the economy geared towards the elderly;
- Startup — a dynamic, usually early-stage, company or project that aims to bring an innovative product, service or solution to market and is looking for a business model to grow profitably;
- STEM — an acronym for science, technology, engineering and mathematics. It is a term used to describe the four interrelated areas that are crucial in the context of education and professional development;
- Electronic Document Management system — an ICT system for electronic management of documentation, enabling the performance of clerical activities, documentation of the course of affairs and the collection and creation of electronic documents (Article 2(13) of the Regulation of the Prime Minister of 18 January 2011 on the clerical instruction, uniform material lists of files and instruction on the organisation and scope of activity of company archives);
- EZD RP system — an Electronic Document Management system whose capabilities, structure and functions meet the real business needs of the Polish public administration. EZD RP was created as part of a project carried out by NASK — National Research Institute in partnership with the Podlaskie Voivode. It is being deployed in the working environments of more and more public administration units, streamlining their operations by providing modern and versatile digital back-office solutions in the area of electronic document management;
- Inventory System for ICT Systems (SIST) — an ICT system for collecting information on planned, existing and decommissioned ICT systems, cooperation between them, records maintained by public administration and the possibilities of using the information collected in them;
- ICT system — a set of IT devices and software working together to enable telecommunications networks to process, store, send and receive data via a telecommunications terminal device appropriate for a given type of network, within the meaning of the provisions of the Act of 16 July 2004 — Telecommunications Law (Dz.U. /Journal of Laws/ of 2016, items 1489, 1579, 1823, 1948, 1954 and 2003) (Article 3(3) of the Act of 17 February 2005 on the computerisation of activities of entities performing public tasks (Dz.U. /Journal of Laws/ of 2024, items 304, 1222); or

- S46 Cybersecurity Management System — an ICT system that supports the reporting and handling of incidents, information exchange and cooperation between participants in the national cyber security system (KSC). It also provides national-level risk estimation and warning of cybersecurity threats;
- Artificial Intelligence (AI) — a field of science encompassing such things as neural networks, robotics and the creation of models of intelligent behaviour as well as computer software to simulate this behaviour, also including machine learning, deep learning and reinforcement learning;
- Virtual Reality (VR) — a computer-generated three-dimensional image that imitates the real world or is a vision of a fictional world (computer-generated environment);
- High-Performance Computing (HPC) — advanced computing infrastructure for the most demanding scientific, engineering and commercial tasks;
- Security by design — an approach implying that the security of information systems should be a core part of the design and development process;
- Ethics by design — an approach that integrates ethical considerations at the technology design stage, particularly in the context of artificial intelligence (AI) and other modern technological solutions;
- Open by design/open by default — an approach that promotes the availability of data and information in a way that allows it to be freely used and reused, right from the design stage;
- Privacy by design — an approach that considers that privacy (data protection) issues should be an integral part of the design of systems, applications and services;
- Computer Security Incident Response Team (CSIRT) — a team responsible for coordinating the response to computer incidents in the area indicated in Article 26(7) of the Act of 5 July 2018 on the national cybersecurity system (Dz.U. /Journal of Laws/ of 2018, item 1560).