AMERYKAŃSKA IZBA HANDLOWA W POLSCE
Spectrum Tower, ul. Twarda 18, 00-105 Warszawa
Tel: +48 22 520-5999, e-mail: office@amcham.com.pl

Warsaw, September 24, 2024

Mr. Jim Lindley
Counselor for Commercial Affairs at U.S. Commercial Service
U.S. Embassy in Poland

Dear Mr. Lindley,

On behalf of the American Chamber of Commerce in Poland (AmCham Poland) and its affiliated member companies, following up on previous correspondence, I am submitting below a list of regulatory and economic issues of greatest importance to American investors in Poland today. We would be grateful if you take them into account for the purposes of U.S. Poland Economic and Commercial Dialogue as well as the further activities of the Commercial Service in Poland.

Digital Economy

I. The Polish Presidency in the Council of the European Union and digital diplomacy

January 2025 marks the start of the Polish Presidency of the Council of the EU, during which Poland has a great opportunity to raise the profile of digital diplomacy on the EU political agenda. The EU should strengthen its openness to trade to shape new technologies as a strategic partner with like-minded countries and in international forums such as the G7 and the EU-US Trade and Technology Council. The transatlantic partnership is a key driver of competitiveness in the EU single market, where bilateral investment, job creation, trade or data flows between the EU and the US support economic growth in both regions. Deploying the latest digital technologies is key to maintaining and further strengthening the EU's competitiveness. The growing tendency toward strategic autonomy, especially in the face of geopolitical threats, should be replaced by strategic partnerships.

Key concerns:

1. **Strengthening transatlantic ties**

   Creating a favorable environment for investors is key to enhancing Europe's security and economic growth. This will enable faster delivery and deployment of new technologies that can grow EU exports. The transatlantic partnership is a key driver of competitiveness in the EU's single market.

2. **Developing an agenda for the development of digital trade**

   Recent crises have made it clear that resilience flows from the digitization of individual economic sectors. The efficiency of carrying out these processes depends on partnerships that help remove barriers to digital trade and establish standards that prevent global fragmentation and divergence in digital policies.

3. Data flow

Data localization requirements, which mandate that data be stored and processed within a specific jurisdiction, have gained popularity in recent years as a way to address issues of data privacy, security and national sovereignty. In particular, the Polish Interior Ministry recently announced new work on data storage localisation requirements. However, these requirements come with significant challenges for Poland's the European Union's digital economy, limiting the potential for innovation. Disadvantages of data localization requirements include, in particular, increased costs hampering economic growth and competitiveness, fragmentation of the digital market and limiting innovation.

As we move forward with new rules for data governance, there is an unprecedented need for global, interoperable solutions. It is essential to create new legal and technical tools, define interoperability standards and, most importantly, continuously agree on new frameworks for maintaining privacy and ensuring data flow. Once the EU-U.S. Data Privacy Framework (DPF) is finalized, the EU and the U.S. should continue to provide legal certainty for data flows while moving toward a more scalable and effective global approach to data flows. This includes finalizing negotiations on the U.S.-EU CLOUD Act to facilitate access to e-evidence.

4. Strengthening EU cyber resilience and security

The EU should seek to strengthen existing security cooperation mechanisms between private and public partners in countries with similar value systems. We encourage the Community to establish a cybersecurity framework to be designed in a way that allows European governments to benefit from leading solutions in this area.

II. Cybersecurity

At a time of heightened geopolitical instability and in the aftermath of the war in Ukraine, Poland should take care of cybersecurity for both critical elements of state functioning and citizen security. Cyber security is a multidimensional challenge. It requires preparedness on the part of both the state and citizens. Polish government needs to invest in infrastructure and build risk awareness in society. At the same time, citizens, supported by the government, should take steps to protect their devices. National cybersecurity should be based on a clear assumption of non-exclusion/discrimination of entities coming from allied countries, including the US.

Key concerns:

1. Protection of critical data

Above all, the focus should be on reliable tools for backing up and maintaining critical national data and services resilient to disruptions (such as large-scale cyber-attacks or other crises). Such a tool could be data embassies, which are part of the European Union's broader policy discussion on data security and resilience or preserving the continuity of digital infrastructure with respect to cloud services.

2. Building on proven international standards

Following the latest research and security guidelines set forth by organizations such as the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), Organization for the Advancement of Structured Information Standards (OASIS) and the Open Worldwide Application Security Project (OWASP) is critical to mitigating threats and employing advanced security assurance methods.

3. Cloud services and non-discrimination of verified partners according to geographical criteria

Equally important is ensuring the free flow of cloud services across Europe and a non-discriminatory approach based on strong transatlantic relations, thus resisting attempts to exclude non-European providers (especially those from NATO) from being able to provide services within the EU. This is particularly relevant to the work on the next digital regulations, e.g. in the context of the work on EUCS (cloud certification scheme).
It is necessary to raise awareness of the importance of the process of digitizing public services and moving data to the cloud in the event of a physical threat and the risks associated with data localization. It is important to move away from the dogma of data localization in Poland. In this context, it is extremely important to establish a sustainable and effective legal framework for data exchange between the EU and the US.

4. Removing unsupported, obsolete and high-risk digital devices from critical networks

Critical infrastructure operators should be required to remove from their networks devices whose software is no longer updated by their manufacturers. While some exceptions to this may be warranted depending on the risks involved, the default policy should be to migrate to a supported product before it reaches the end of its useful life.
The EU has created a strong legal framework requiring critical infrastructure operators to adopt cyber-security measures (Directive on measures for a high common level of cyber-security within the Union - the so-called NIS Directive 2) and requiring manufacturers to provide support for their products (Regulation on Horizontal Cyber-Security Requirements for products with digital components - the so-called CRA regulation). A binding obligation to remove obsolete devices would solve the gap between these regulations.
In addition, the NIS 2 Directive has still not been implemented in Poland. It is necessary to accelerate work on the introduction of relevant national legislation.

5. Need to establish rules for managing security gaps

Polish government bodies should make public their internal policies on the handling and disclosure of vulnerabilities, and make appropriate safeguards available to ensure the principle of openness.Under the NIS2 Directive, EU Member States are required to implement a Coordinated Vulnerability Disclosure (CVD) process relating to principles and methods of protection intended for use by external researchers for the purpose of detecting and reporting vulnerabilities to public and private sector organizations, and for handling by civilian cyber security authorities. However, Poland still lacks established rules for handling vulnerabilities that threaten government bodies, as well as for informing software developers about them.

We are concerned that government authorities may be tempted to keep information about security vulnerabilities to themselves and not disclose it to manufacturers, thus opening the door to possible exploitation of these vulnerabilities by intelligence or law enforcement agencies. This poses significant economic and reputational risks for companies and individuals, which may not be adequately considered in the decision-making process.

III. Artificial Intelligence

Artificial intelligence must be regulated - it is too economically and socially important an innovative technology not to do so. Whenever we work with technology, we must learn to take advantage of its benefits while minimizing its risks.

The current regulatory landscape for artificial intelligence is becoming increasingly complex. Key pieces of legislation governing AI include the AI Act, the Artificial Intelligence Liability Directive, or the Product Liability Directive, among others. The provisions of GDPR apply, as well as the regulations contained in the European Cyber Resilience Act (CRA), or NIS Directive 2. In addition, the rules on algorithm transparency contained in the Digital Services Act (DSA) are causing an even greater accumulation of AI regulations. In addition to EU law, new bodies and voluntary tools have emerged from international and multilateral initiatives, such as the G7 Code of Conduct and the AI Security Summit.

This proliferation of regulations and authorities has led to a highly complex legal environment. Without coordinated enforcement of these regulations, there is a significant risk of unnecessary legal ambiguity, which could consequently hinder the development of the AI ecosystem and the deployment of innovative AI solutions in Europe, which in turn is critical to its competitiveness.

Key concerns:

1. **Implementation and application of a large number of regulations affecting AI.**

   Enforcing consistent implementation of the AI Act will require coordination at the EU level to prevent divergent interpretations of the law across member states. Consistent implementation of the Act is crucial to ensure legal consistency and clarity across the EU. Effective enforcement will also require coordination between authorities responsible for related legislation on national level, such as DSA, GDPR, CRA or NIS2. A harmonized approach will help mitigate the risk of conflicting obligations and streamline compliance processes for businesses. Comprehensive guidelines should be created to make it easier for the private sector to navigate among AI-related regulations. These guidelines should aim to make the regulatory framework transparent, flexible and streamlined, facilitating compliance while fostering innovation and thus Poland’s competitiveness. In particular, the coexistence of GDPR and AI Act regulations will require the development of detailed guidelines. The upcoming Polish Presidency of the EU Council presents a great opportunity to draw attention to the need for uniform implementation of EU regulations and increased legal certainty.

2. **Effective use of the opportunities arising from the development of AI in Poland.**

   A thorough review of Poland's artificial intelligence development strategy should be carried out in order to take immediate steps to enable Poland to take advantage of the opportunities arising from the development of this technology. Poland should use its competitive advantages

derived from the potential of American investors present in the country who have been developing this technology for years and its talent pool to reap the benefits of this next technological revolution. A prerequisite is the responsible preparation of regulations on artificial intelligence.

IV. Ensuring a level playing field in e-commerce

It is essential to level the playing field in the e-commerce market and promote compliance with EU and national regulations on trade, tax, security of goods, etc. Ineffective enforcement of existing regulations promotes unfair competition from Asian players.

Key concerns:

1. VAT IOSS

The current design of the system for collecting VAT on imports of small-value shipments (IOSS) has a very serious drawback - it is not a mandatory system. This results in a situation where various types of platforms can easily and legally arrange themselves in such a way as to avoid the obligation to collect VAT from their sellers. The obligation then falls on domestic postal operators and couriers, who become responsible for collecting import VAT on behalf of the end customer.

Such a system generates a noticeable risk of shifting not entirely honest sellers to platforms that do not use IOSS, thus significantly reducing the incentive for well-intentioned platforms to use it. Moreover, it significantly undermines the effectiveness of VAT collection. That's why it's important to quickly adopt solutions that establish a mandatory IOSS registration requirement on an EU-wide level, so that all platforms are subject to the same set of rules with regard to the recognized reseller's VAT obligation for low-value imports, which in turn will increase the efficiency of VAT collection for imports of goods under €150 traded online.

2. Drop shipping

In addition, a challenge for Polish and European e-commerce is the uneven framework in which European and American players compete with Asian players operating in a direct-to-consumers model, in which goods produced in one country are exported directly to consumers in another EU country. Currently, there is a lack of capacity for effective regulatory enforcement due to the lack of effective representation of such players within the EU and the fact that current e-commerce regulations apply almost exclusively to platforms (marketplaces), leaving out traditional e-commerce retailers.

As early as the end of 2020, the Supreme Audit Office (NIK) indicated that the Polish Post was incapable of controlling shipments on a massive scale. It did not have, among other things, the electronic data necessary for customs and fiscal control, and oversight of parcel transportation was based on physical inspection of 1 percent of parcels entering Poland. In the direction of sealing the borders, the European Commission is working, having recently presented draft amendments to the EU Customs Code. Among other things, Brussels plans to create an EU Customs Office, which will oversee an EU customs data center. The legislation will also introduce the principle of a "deemed importer" entity for those selling imported goods directly to consumers, and will abolish the customs exemption for goods

worth up to 150 euros. The legislation in question will most likely be at the stage of final discussions (trilogues) during the Polish presidency, which deserves special attention.

V. Digital competencies

Developing digital competencies among citizens is key to boosting Poland's competitiveness, innovation and social inclusion. In the face of rapidly developing new technologies such as generative artificial intelligence it is crucial to determine what skills, training or education are needed to bridge the gap between the ambitious goals of the Digital Decade and the significant lack of digital competencies among the workforce and the shortage of IT professionals. Support programs for citizens and SMEs should reflect the complexity of the EU's single market and the different needs and strengths of regions, while aiming to harmonize educational standards and share best practices.

Key concerns:

1. **Meeting the Digital Decade 2030 goals for upskilling**

Poland should significantly increase investment in basic and advanced digital skills training in formal and informal education. To meet the challenge in a rapidly changing context, partnerships with the private sector will help ensure that formal education, vocational training and certifications actually meet the needs of citizens and businesses.

2. **Incorporating digital and media education as a formal component of civic education**

Building a strong and diverse workforce with media literacy and STEM and digital skills requires updating curricula and training, starting in kindergarten through elementary and high school. Effective use of digital technologies is essential, as is the ability to responsibly access, engage with and share content online.

Cooperation on Energy Sector

Key concerns:

1. **Development of nuclear energy**

Construction of nuclear plant in Poland will positively influence our country's energy independence, diversifying energy sources and ensuring access to affordable energy. This will result in lower cost of energy, consequently influencing prices not only for private individuals, but also businesses. Moreover, this has great importance from the ecological point of view and additional impulses for the job market and the development of education in Poland.

2. **Improving administrative procedures**

To accelerate the development of renewable energy sector, it is vital to improve the administrative procedures related to obtaining permits for the construction of energy installations. Shortening of waiting time, reducing bureaucracy, and introducing clear standards aids to create more friendly environment for investors, which speeds up project implementation.

3. **Conducting long-term policy and creating conditions and services of public administration in ways that encourage private investors to invest in green energy**

Key element of effective energy transformation is conducting long-term policy, which will provide stability and predictability for investors.

4. **Creating financial incentives, tax reliefs, as well as eliminating investment barriers is an important step towards attracting private investors to green energy sector**.

Cooperation between public and private sectors for creation of favorable investment climate is crucial to achieving sustainable energy development goals.

Supply Chain

Key concerns:

1. **Support instruments**

It is crucial that these support instruments are realistically accessible, meaning:

- Simple and clear rules for granting support instruments, both when applying and when settling accounts;
- Decisions regarding the granting of support should be quick, as the investment evaluation process cannot take months, as this delays decisions on the investor's side;
- The settlement rules for support should be as flexible as possible because market realities change, and sometimes the project needs to be adjusted to new conditions, but rigid public aid rules prevent this.

It is important to note that with the implementation of the global minimum tax (EU regulations), the profitability of typical tax exemptions will significantly decrease. Therefore, it is necessary to develop new grant instruments (as Ireland, for example, has done) so that the country does not lose its comparative advantage. Currently, Poland does not have such a replacement solution, and it is recommended to work on one.

2. **Efficient and quick procedures for implementing investments**

Investment incentives are not only financial instruments – efficient and quick procedures for implementing investments must also be created. A solution could be, for example, a fast track for strategic investors concerning issuing environmental decisions, building permits, work permits, and visas for key foreign employees, etc. Often, this is an important element that is not visible when choosing a country but becomes a huge problem (a threat to the schedule), leaving a negative impression and causing issues when considering future investments.

3. **Export regulation issues outside the EU**

Major problems for exporters to CIS countries arise in the context of sanctions and the interpretation of whether a given product is dual-use (EU sanctions interpretations). Customs offices differ in their interpretations between regions, holding up transports for several days,

AMERYKAŃSKA IZBA HANDLOWA W POLSCE
Spectrum Tower, ul. Twarda 18, 00-105 Warszawa
Tel: +48 22 520-5999, e-mail: office@amcham.com.pl

etc. New export control requirements are expected (e.g., the need to present documentation from third-country entities within 30 days), etc.

Should you require any additional information or clarification, we are ready to assist.

Yours sincerely,

Marta Paulak

Legal & Public Policy Director
American Chamber of Commerce in Poland