Tax&Legal Highlights

Poland

Change in certain double taxation avoidance regulations applicable to individuals generating income abroad. Multilateral Instrument coming into effect

On 1 July 2018, Multilateral Instrument to Modify Bilateral Tax Treaties (MLI) came into force, modifying certain double tax avoidance principles arising from international agreements concluded by Poland.

MLI provisions will supersede or supplement international treaties concluded by Poland, provided that:

- Poland has indicated or will indicate a treaty as included in MLI (notification);
- the other country being a party thereto does the same; and
- both parties ratify MLI.

Four jurisdictions (Austria, Jersey, Slovenia and the Isle of Man) and Poland were the first to ratify MLI.

Poland accessed MLI on a broad basis, including 78 DTAA treaties and adopting nearly all provisions, among others the intention to amend and unify the double tax avoidance method by adopting the tax credit method.
This means DTAA concluded by Poland and including a tax exemption clause as the method to avoid double taxation shall be modified and the clause shall be replaced with the tax credit method. The amendments shall include DTAA concluded with Austria, Norway, Slovakia, UK and Italy.

New DTA methods and abolition relief
Please note that under the tax exemption method, income taxable abroad is tax-exempted in Poland. However, it is included in the calculation of an effective tax rate applicable to other income (if any) generated by taxpayers and taxable in Poland on general terms.

When the tax credit method is applied, taxpayers are obliged to calculated the Polish tax on their foreign income. Then, they can deduct the tax paid abroad on this income. The deduction cannot exceed the amount of tax payable in Poland on that income.

Taxpayers using the tax credit method in Poland are usually obliged to pay taxes that are higher than those paid in the states where the exemption method is applied, if the total tax charge is considered (i.e. including the tax paid in the state of residence and the tax paid in the state of origin).

In order to equalize Polish tax charges for individuals working abroad, arising from differences in DTA methods applied, the lawmakers have introduced the so-called abolition relief to the PIT Act. The relief allows deducting the difference between the tax calculated using the tax credit method and that calculated using the exception method from the Polish tax liability. It is limited, though, to certain income types, such as employment, managerial contracts and contracts of mandate/of specific work, sole proprietorship, freelancer activities, and certain property rights.

In light of the above, taxpayers should expect additional tax charges related to income formerly exempted under DTAA and not included in the abolition relief, such as income from rent of real property, pension or property disposal.

Importantly, both tax credit method and abolition relief are available only in the form of filing annual tax returns. Thus, taxpayers who have generated only income exempted from tax in Poland under an appropriate DTAA and often did not file annual tax returns in Poland (since they did not generate any taxable income), once a given country joins MLI, will be obliged to prepare such annual tax returns and file them with competent tax offices by the end of April in the year following the fiscal year they pertain to.

Follow up on the taxpayer side
In states that access MLI, provisions thereof shall supersede any bilateral DTAA. At the same time, contents of the latter shall not be amended if more states join MLI. Therefore, taxpayers who do not monitor changes in international tax law on an ongoing basis, being unaware that their respective state has joined MLI, may experience problems with correct fulfilment of their tax obligations in Poland. In many cases they will not realize their obligation to prepare tax returns in Poland (assuming they are not obliged to report tax-exempted income in Poland), or will prepare their annual returns in compliance with then invalid guidelines arising from a respective DTAA.

In order to avoid exposure to adverse consequences of incorrect fulfilment of tax obligations, taxpayers should monitor possible changes in taxation related to new states joining MLI on an ongoing basis.

Additionally, we recommend an analysis of transactions concluded in light of the changes in tax settlement methods.

Contact details:

Adam Mariuk
Partner
Tax Advisory Services
Tel.: +48 22 511 05 57
e-mail: admariuk@deloitteCE.com

Joanna Świerzyńska
Partner
Tax Advisory Services
Tel.: +48 22 511 04 23
e-mail: jswierzynska@deloitteCE.com

Rafał Garbarz
Partner Associate
Tax Advisory Services
Tel.: +48 22 348 37 10
e-mail: rgarbarz@deloitteCE.com

New draft Regulation on Polish Investment Zone approved. Quantity criterion significantly relaxed

On Thursday 26 July Permanent Committee of the Council of Ministers approved a new draft Secondary Regulation to the Act on Supporting New Investments (henceforth: "New SEZ Regulation").

An extended list of investments whose quantity criterion shall include the **qualified expense of at least PLN 10 million** (i.e. the lowest obligatory amount as referred to in Article 3.1 of the New SEZ Regulation) shall be an important change related to the obtaining of the Support Decision (henceforth: "SD"). According to the current assumptions, the projected provision should read as follows (the newest amendments bolded):

1. A business which has applied for the aid, depending on the unemployment rate in the county (powiat) in which the project is to be carried out, must satisfy one of the following quantitative criteria:

7) In the county where the employment rate is 250 percent higher than the country average**, in a town that loses its socio-economic functions referred to in Appendix 1 to Table 3 and in a municipality adjacent to such town,** a business shall commit to incur qualified expenses of at least PLN 10 million.

What does this mean?
Consequently, in extreme cases, thanks to the amendment, a large business intending to carry out a new investment in the industrial processing sector

will have to commit to invest PLN 10 million instead of the former PLN 100 million of qualified expenses to obtain SD.

In light of the above, investments in towns that lose socio-economic functions or in an adjacent municipality may be critical for a business to qualify for SD. Please note that determining whether a given municipality (in which the investment is to be located) is adjacent to such a town (listed in Appendix 1 to Table 3 of the New SEZ Regulation) will be of importance.

Contact details:

Marek Sienkiewicz
Partner Associate
Tax Advisory Department
Tel.: +48 12 394 43 29
e-mail: msienkiewicz@deloitteCE.com

Bartłomiej Węgrzyn
Consultant
Tax Advisory Department
Tel.: +48 12 394 43 51
e-mail: bwegrzyn@deloitteCE.com

Act on National Cybersecurity System: new obligations of key utility operators and digital services providers

Businesses in the energy, transport, banking, payment services and healthcare sectors, suppliers of drinkable water or digital infrastructure, classified as so-called key utility operators, as well as digital service suppliers, must prepare to stand up to new challenges, this time regarding cybersecurity.

3 August 2018 The President of Polish Republic signed the Act on National Cybersecurity System, implementing the Network and Information Systems Directive (NIS). Along with GDPR, the Directive is a key element of the Unified Digital Market Strategy pursued by the European Union. The key assumption of the new regulation is to ensure a unified model of security and resistance, including an effective and consistent system of responding to cyberattacks and cyberthreats.

Who will be affected?
The new regulatory challenges apply to:

1) Key utility operators
The group includes businesses that provide services in the following sectors: **banking, financial market infrastructure, energy, transport and healthcare,** i.e. the ones whose security is of key importance for the society and national economy.

Authorities competent to supervise cybersecurity issues shall decide which businesses operating in the above sectors shall be considered the key utility operators. With this respect, individual **administrative decisions** regarding each business shall be issued.

Authorities competent to supervise cybersecurity issues include ministers in charge of each economy sector, except for the sector of banking and financial market infrastructure, which will be supervised by PFSA.

Appropriate classification decisions shall be issued **by 9 November 2018.** The entities designated as key utility providers shall have **very little time to achieve compliance with the new statutory obligations (three to six months** of the decision delivery date).

2) Digital service providers
Digital service providers shall be understood as **Internet trading platforms, providers of cloud services and browsers.**

What will the new statutory obligations involve?
The Act focuses on providing security of information systems of critical businesses ensuring confidentiality, accessibility, integrity and authenticity of the processed data and services offered by these systems.

Among others, key utility operators shall be obliged to:

- **Implement a security management system within their operation systems**

The system will involve implementation of appropriate organizational and technical measures (policies, procedures, processes) supporting IT security, systemic risk management, collection and analysis of information on threats, susceptibility identification and incident management.

- **Implement handling procedures and notify competent bodies about incidents**

The notification should take place within 24 hours of incident detection and should include its description, its effect on the provision of key utilities by other operators, its reason and course, as well as information about preventive and correcting measures undertaken. Incident handling information should be provided to the appropriate supervising body on an ongoing basis. Businesses must be aware that sometimes disclosure of confidential information, including trade secrets, to supervisory bodies may be necessary.

Supervisory bodies may decide to publish information regarding a given incident.

Implement a procedure of classifying incidents as serious or significant - thresholds regarding their effects on each key utility shall be determined by a regulation issued by the Council of Ministers;

- with regard to digital service suppliers, the requirements are defined in Regulation 2018/151.
- **Establish internal structures in charge of cybersecurity** (which may mean establishing separate organizational units or assigning new tasks to current employees; please note, though, that these units will be of interdisciplinary nature), or concluding an agreement with a specialized cybersecurity service provider.
- **Cooperate with supervisory bodies**.
- **Carry out a security audit** of the information system used to provide the key utility (at least once every two years).
- Provide users with appropriate information allowing them to understand cyberthreats and appropriate preventive measures.

Similar obligations apply to digital service suppliers. Further, if they provide services to key utility operators, they will be obliged to provide them with information regarding incidents.

The Act on National Cybersecurity System shall pose a challenge for entities obliged to comply with it, both in terms of providing appropriate organizational measures (strategy, management information, operational risk management procedures), implementation and proper functioning of preventive measures, detection and response, as well as ensuring continuous employee awareness building, security tests of each organization, ensuring readiness for threats and appropriate response to incidents, to include effective cooperation and communication, collection and analysis of evidence and post-hacking procedures.

Key utility operators and digital service providers who fail to comply with the Act can be fined with the amount of up to PLN 200,000 (in extreme cases, up to PLN 1 million).

Additionally, in May, the European Central Bank published Threat Intelligence Based Ethical Red Teaming Framework (abbreviated as TIBER-EU Framework), which supports the financial sector and key utility operators in of carrying out security tests.

Contact details

Katarzyna Sawicka
Senior Associate, Deloitte Legal
Trainee Lawyer
Tel.: +48 22 511 05 33
e-mail: ksawicka@deloitteCE.com

Marcin Ludwiszewski
Director
Cybersecurity Leader
Tel.: +48 53 844 28 15
e-mail: mludwiszewski@deloitteCE.com