**Analysis of the changes in National Cybersecurity Act and Public Tender Act - analysis**

On 7th of September the government announced the plans to change and modify existing regulations with the National Cybersecurity Act and Public Tender Act.

The new regulations refer to the 5G Toolbox and European Union recommendations regarding ensuring cybersecurity in the member states.

The suggested regulations put the additional obligation on the suppliers of telecommunication and network access to

“conduct regular and systematic risk assessment of potential risk event” and “ take necessary technical and organizational actions to ensure the safety adequate to the level of identified risk”

Additionally, the Collegium may provide risk assessment of the suppliers crucial for cybersecurity. Elements that are being analysed and considered:

1. Analysis of the national security risk regarding the economic security, counter intelligence and terrorist as well as the risk to fulfill the commitments toward allies and European partners
2. Analysis if the supplier may be under the influence of the non-European Union or non-NATO member country/government:
   1. The degree and type of relations between supplier and that country
   2. Legislature of that country in reference to human and citizen rights
   3. Legislature toward the protection of personal data, especially in the cases when the country has no agreements with EU in that matter
   4. Ownership structure of the supplier (hardware and software)
   5. Capability of that country to affect the economic freedom of the supplier
3. Number and type of people and time to eliminate the events
4. The degree the supplier controls the production and supply processes
5. The previously provided recommendations related to the hardware or software of the supplier

Supplier can receive 4 grades:

**High risk**: if the supplier can cause serious risk to cybersecurity of the state, and minimizing the risk by implementing technical or organizational means is not possible

In case of identifying the supplier as a high risk, the supplier is forbidden to implements its hardware, software and services and is required to withdraw from use its hardware and software no later but within 5 year after the publishing of the high risk grade0

**Medium risk:** if the supplier can cause serious risk to cybersecurity of the state but it can be limited by implementing technical and organizational means

In case of identifying the supplier as medium risk, the supplier is forbidden to implements its hardware, software and services btu are allowed to use the existing infrastructure without the need to dismantle it.

**Low risk:** if the supplier can cause minimal risk to cybersecurity of the country

**No risk:** no risk related to the supplier

Comments:

1. This is the proposition of the new regulation that has been given toward consultations. Companies, individuals or parties can provide their comments and suggestion to the current proposition
2. There seems to be conflict within the government referring to these changes. Ministry of Foreign Affairs and well as the Ministry of Economy seems to be reluctant to these changes as they perceive this act to be directed at Chinese suppliers, mainly Huawei.
3. The publishing of these regulations after the visit of Mike Pompeo is not probably not a coincidence and is supported by the USA. It is in accordance to our previous assessment that we should expect some movements within the government toward cybersecurity.
4. These changes might create the legal base for further actions toward outside EU suppliers of 5G and network, communication hardware suppliers – banning Huawei and Chinese suppliers from entering Polish market
5. There is a strong opposition toward these changes within the network operators (except PLUS which is using primarily Ericsson hardware) which are worried about the costs of replacing Huawei hardware – estimated to be about 7 bln PLN (about 2 bln USD) and which government is reluctant to reimburse.