CYBERSECURITY AND ARTIFICIAL INTELLIGENCE IN M&A TRANSACTIONS – THE POLISH PERSPECTIVE

Anna Dąbrowska

Introduction

It seems that cybersecurity and artificial intelligence are almost all anyone talks about these days. Visions of hackers acquiring our most sensitive secrets and running countries while lawyers become redundant because of technology straight from Terminator movies is enough to keep anyone, especially lawyers, awake at night. But is the threat real? Do lawyers have to start looking for new jobs?

Cybersecurity – the current legal background

The first half of 2018 was marked with a frenzy of measures taken in anticipation for the GDPR. The overwhelming amount of efforts that were put into preparing for the regulations that entered into force this past May, fueled by the threat of potential significant sanctions for failure to do so, overshadowed works on another set of important cybersecurity rules - those contained in Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ("**NIS Directive**"). The need to undertake additional measures to implement the latter rules caused a majority of Member States to miss the May 9, 2018 deadline for introducing the NIS Directive into their legal systems.

Poland implemented the Act on the National Cybersecurity System ("**ANCS**") on July 5, 2018, and the law entered into force on August 28, 2018. The ANCS created a national cybersecurity system, which includes the largest service providers from various sectors of economy, as well as governmental and local administration. The objective of the new law is to create an efficient and secure system which increases the level of cybersecurity in Poland. It is also meant to provide a platform for swift co-operation with other EU Member States. Many comment that it is high time for such law to be created, however, sceptics warn that this only produces a set of bureaucratic regulations and procedures against a dynamic and ever evolving community of cyber criminals.

In designing a national cybersecurity system the ANCS establishes "operators of key services" who will be chosen from amongst providers of services deemed vital for maintaining Polish economy and society, in particular, ICTs and entities from the banking, financial market infrastructure, digital infrastructure, energy, transport, and healthcare sectors. Entities for specific sectors will be named "operators of key services" pursuant to a decision issued by the relevant authority and subsequently entered into an official registry, maintained by the Minister of Digitization. The deadline for these decisions is November 9, 2018.

The ANCS imposes several obligations on the operators making it necessary for them to take appropriate security measures, conduct periodical risk assessments in relation to cybersecurity and notify serious incidents within 24 hours to the relevant authority. They are also obliged to co-operate with the relevant Computer Security Incident Response Team (CSIRT) in case a cybersecurity incident does occur, by which the ANCS means "any event having an actual adverse effect on cybersecurity" or "an incident that will cause or may cause a serious

deterioration or interruption of the provision of a key service“, which makes it a serious incident. Each operator will need to appoint a specifically designated cyber security “officer” responsible, among others, for serious incident notification and staff training.

The time line is ambitious as once the decision is issued an operator will have three months to implement most of its obligations. The first audit of the IT systems of an operator is to take place within a year from the decision.

The ANCS foresees a number of new obligations that apply to digital service providers, i.e. online marketplaces, search engines and cloud services. These include, in particular security and incident notification requirements.

The National Cybersecurity System will cover both the private and governmental sector and will include a Serious Incident Response Team to manage on the working level and a Governmental Representative for Cybersecurity and the Board for Cybersecurity – on the institutional level. A single point of contact for cybersecurity will be created by and reporting to the Polish Minister of Digitization. This contact point will be responsible for the exchange of information on the national level and co-operation on the EU level.

Three Computer Security Incident Response Teams will be assigned to respond to specific occurrences depending on the type of cyber incident. CSIRT GOV acting under the Agency of Internal Security - ABW, CSIRT NASK acting under the National Academic Computer Web - NASK, and CSIRT MON acting under the Minister of Defense. Each of CSIRTs will co-operate with the relevant cybersecurity authorities, Minister of Digitization and the Governmental Representative for Cybersecurity. All of these entities are to act as a coherent and complete risk management system on the national level.

The ANCS also foresees notifications to CSIRT NASK being made by natural persons, but such notices will be given lesser priority.

Failure to comply with the obligations stated in the ANCS will render the breaching entity at risk of a sanction of up to PLN 150,000 (approximately USD 40,000) for a single occurrence of non-compliance and up to PLN 1,000,000 (approx. USD 270,000) for ongoing non-compliance leading to severe risks to national cybersecurity.

A set of implementing regulations is also foreseen by the ANCS, which will include more specific requirements for particular sectors and institutions. These regulations are currently under legislation.

Cybersecurity in M&A

The ANCS will surely impact the work of transaction lawyers who will need to take the provisions of the new law into account, among others when conducting due diligence and structuring transaction documentation.

However, cybersecurity and data privacy concerns arise regardless of whether an entity is considered an operator of key services or not. The awareness of cybersecurity threats is rising and the need to secure potential risks connected with it is becoming M&A reality also in Poland. Starting the due diligence, providing relevant provisions in transaction documents, finishing with post-closing compliance exercises, guiding clients in putting in place of necessary

cybersecurity procedures and acquiring sufficient insurance, transaction lawyers today are forced to make cybersecurity a new element of their everyday reality.

It seems, however, that although more and more is being said on the subject, cybersecurity still isn't a top priority for Polish entrepreneurs. What's more, in response to this lack of sufficiently high interest, not many insurance providers acting on the Polish market are ready to offer policies securing against cybercrime events.

In 2018, there are seven insurance providers offering cybersecurity insurance policies (compared to 2 in the previous year). It is approximated that only 8% of Polish companies hold insurance policies with regard to potential cyber risks that the company is exposed to (this is a meager number compared to the global percent of companies holding such policy which is 59%).

Not only is this a clear indication that the awareness of Polish entrepreneurs when it comes to cyber risks is low, but it also brings attention to the potential reasons for their reluctance towards such additional safety triggers. The most common ground for such behavior is a price of the insurance policy, as well as the list of exemptions included therein.

The most important clause that should be included in every cyber-insurance policy is the indemnification for the cost of investigating a data breach and, as GDPR provides that persons impacted must be notified of the occurrence of the breach, the cost of such notification (meaning "first party" costs). However, under the new regulation such notification may be required even though there is no determination of the occurrence of a breach, but only a suspicion thereof. Some cyber policies offered on the market do not provide coverage for the costs of a notification costs based on suspicion of a breach only. Such language of the insurance policy could come into conflict with the rules provided by GDPR.

On the other hand, most of the policies offered on the Polish market do not cover the administrative fines that may be imposed on the company on the basis of specific cybersecurity related regulations. This, however, is not only a Polish problem. For example, in a report prepared by DLA Piper and Aon reviewing the insurability of GDPR fines across Europe it was found that GDPR fines were insurable in only two of the reviewed countries - Finland and Norway. The problem is that for the most of the Polish companies it's the administrative fines that are considered as the biggest potential cost of the potential cyber breach. The entrepreneurs' awareness related to the costs of the remedy actions that need to be taken in case a breach occurs is still low.

Cybersecurity - from the perspective of the law firm

The problem of cyberattacks does not only concern parties to a transaction but also their advisors and service providers, including law firms. Consequently, the need to ensure that the highest levels of cybersecurity are provided by all those who carry large amounts of sensitive information concerning a given deal and its players.

Apart from obtaining relevant certificates, such as ISO/IEC, law firms are becoming more and more aware of the importance of the suitable standards and software ensuring the proper security of data.

Special care must be taken at the stage of a due diligence when considerable amounts of sensitive information concerning the target entity are disclosed to a potential acquirer. Usually

provided by way of a professional platform, it is nonetheless that this point of the transaction when several independent groups of people – the interested acquirer and its advisors, sometimes the insurer, possibly the financing bank, etc. – have access to documentation posted in a virtual data room. As a countermeasure against illegal acquisition of information in case of a cyberattack more and more data room providers are ensuring pseudonymisation of information provided in data rooms, which takes place at the moment of its introduction into the system, for the purposes of due diligence reviews.

Needless to say, for their own safety, law firms are also seeking to secure their own interest by acquiring cybersecurity sensitive insurance policies, which are becoming more and more accessible.

Artificial intelligence – risks and challenges

The due diligence stage of a transaction is where artificial intelligence can be used in the most effective manner. The idea of limiting days' worth of documents review to just a few minutes is very seducing both from a client's and a lawyer's perspective. The ability to monitor the other party's activity on a due diligence platform can also provide valuable arguments for the negotiations stage of a transaction (e.g. when an argument is put forward by the buyer for the seller to provide guarantees for a specific area of a company's business due to the buyer's inability to review the source documentation properly in order to assess existence of risks - this may easily be confronted with the statistics collected by the DD platform).

But this works best in large transactions where the number of similar documents runs in the tens and hundreds and, preferably, when all these documents are in English. The quality of the documents fed into the machine also has an impact on the end result.

Law firms in Poland do not see many such projects. The Polish M&A market is a market of small to mid-size deals. The Fordata M&A report notes that of transactions reported in the second quarter of 2018 the largest one had a value of EUR 763 million while the next one in line only EUR 280 million. A majority of the deals did not reach the EUR 100 million mark. Smaller transactions usually mean that the amount of information to be reviewed during the due diligence is considerably lower. The opportunity to use the full potential of AI in legal analysis is not as significant as in the US and the Western countries. Consequently, law firms are faced with the question of whether now is the time to invest in the available instruments or whether they should wait for the market to develop further and for the price of AI solutions to be lower.

Considering this, as well as the more general concerns relating to reliability and liability seem to be making Polish law firms cautious about taking the AI plunge.

AI works well to collect and analyze information from standard and unambiguous terms in agreements. The review of ambiguous and not standardized terms may result in overlooking documents or provisions or in their misinterpretation due to a failure in the software (the algorithm) or insufficient training of the program. This exposes the law firm to liability. It goes without saying that manual contract review has natural human limitations and the ever increasing sophistication of AI solutions will provide more and more certainty in this respect. The question remains whether it will be possible to rely on a program to identify all serious risks, especially those, that are not easily quantifiable or fail to meet imposed value-criteria thresholds.

Another serious drawback also derives from AI's problems with languages other than English. Polish is an inflected language and therefore the program would have to use far more complicated algorithms to properly read the documents provided. None of the current solutions foresee Polish as an option in their products.

Artificial Intelligence – will Polish lawyers need to find new jobs?

It seems that computerization of legal services has become unstoppable. Although some prophesize that it will decrease the need for lawyers or even force them out of their jobs completely, these fears seem exaggerated. The question is how to use AI to work for us and not against us, to use it to our advantage as the punch that will give us an edge over our competition. The time saved on laborious research and documents analysis could be used instead to concentrate on more challenging tasks.

It is highly likely that anyway, in the end M&A AI will become an everyday norm so it good to start getting used to the idea of working with it.

The development of M&A related AI is more advanced and the questions and concerns connected with it arise more frequently in the US and Western Europe than in Poland and generally the SEE region where the markets are more shallow and transactions tend to be much smaller in size. This gives professionals from this part of the world a sense of security for their jobs. But is that feeling fully justified? The legal market is just as competitive here as it is in the West, and new IT solutions are developed daily. Eastern Europe is renowned for its IT talents so a vibrant and potent epicenter of AI solutions should not be surprising. Products offered by Treesk, Attachi, Dokrates, SzuKio, Umownik and others are among the many tools that are being constantly created to increase the effectiveness of legal life.

At the same time suppliers such as Kira, Luminance and Drooms are well known in this part of the world.

Whoever applies the best solutions first and in the most efficient manner may turn out to be the market leader and the opportunity should not be missed. At the same time eagerness to adopt new technologies for clients must be balanced with consideration of both suitability and security. Efficiency and effectiveness of new methods versus the old must be weighed carefully.