A Booster Shot of Compliance for Companies in Central and Eastern Europe

Bogdan Bibicu, Jitka Logesová and Jaromír Pumr
Wolf Theiss

IN SUMMARY

The increased focus of companies in Central and Eastern Europe (CEE) in tackling large-scale corruption through corporate criminal liability has resulted in an increasing number of companies being prosecuted each year. Companies have, therefore, been paying closer attention to their compliance efforts. This article discusses the influence of the covid-19 pandemic on the shifting focuses of prosecuting authorities in the CEE region, the compliance status of companies and corporate investigations, and provides an outlook on the future.

DISCUSSION POINTS

- States' shopping sprees for medical devices during the pandemic
- Influence of the pandemic on corporate investigation and compliance processes
- Digital corporate investigations and internal policies for digital-age compliance
- Zero-based redesign of the compliance management system
- Commencement of activity of the European Public Prosecution Office
- War in Ukraine and further related shifts

REFERENCED IN THIS ARTICLE

- Association of Certified Fraud Examiners' report 'Fraud in the Wake of COVID-19: Benchmarking Report'
- US Department of Justice's 'Evaluation of Corporate Compliance Programs'
- Group of States against Corruption
- OECD working groups on bribery and non-trial resolutions
- European Commission's reports on anti-corruption matters

Common ground in the CEE region

The region of Central and Eastern Europe (CEE) is a unique place that stands out owing to its rich tapestry of languages and its abundance of cultures – each embedded in national histories vastly different from one another. This contrasts with the closeness kept by a few groups of nations that share substantial parts of their histories (eg, Slovakia and the Czech Republic – formerly Czechoslovakia).

The legislative and legal landscape of CEE countries and their approach towards compliance is also influenced by each of their current political affiliations. The concept of corporate criminal liability is still a relatively new concept for many white-collar crime practitioners and prosecuting authorities in CEE countries. The concept more or less followed the concept of individual criminal liability, which has created room for many difficulties in application.

Most CEE jurisdictions either allow companies to release themselves from criminal liability if they prove that they have an effective compliance management system (CMS) in place that is able to prevent the investigated criminal behaviour, or consider an effective CMS as a mitigating circumstance for which the company must react with zero tolerance to non-compliant behaviour. Having an internal process in place to investigate non-compliance is understood to be a part of any effective CMS.

For example, in the Czech Republic, companies can release themselves from criminal liability if they prove that they have adequate measures (an effective CMS) in place that could have prevented the crime. In September 2018, non-binding internal guidelines – later modified in 2020 – for Czech public prosecutors were issued. This is relatively atypical for the CEE region. The guidelines were inspired by international guidelines, such as those by the US Department of Justice (DOJ), the UK Bribery Act guidelines and the compliance standards ISO37001 and ISO19600, and are in the form of an internal document that is intended to be used as non-binding guidelines by public prosecutors.

The investigation process in each CEE country is unique, and cross-border investigations across several European jurisdictions have often presented an array of practical challenges. However, thanks to the decades of work put in by the European Union, the Organisation for Economic Co-operation and Development (OECD) and the Council of Europe, a clear trend is becoming apparent in which divergencies can be converged, and multi-jurisdictional corporate investigations or compliance audits can be conducted more easily than ever before.

Unfortunately for some companies, this does not only apply to corporate investigations and compliance audits; law enforcement authorities are also actively cooperating with each other much more frequently and much more swiftly, with this cooperation also extending abroad to their counterparts in jurisdictions such as the United States, the United Kingdom, France, other EU countries and Canada, among others.

Anti-corruption, anti-terrorist financing, anti-money laundering and foreign tax evasion efforts have also started to improve in terms of both the quantity and quality of enhanced coordination and communication at the multi-jurisdictional and global levels. As a result, there is an increasing number of local and multi-jurisdictional corporate investigations that have been triggered by vigilant companies that are highly observant of any signs of non-compliance that could trigger, for example, an investigation in respect of the Foreign Corrupt Practices Act (FCPA), the UK Bribery Act or the French Sapin II should the CEE authorities open an investigation and request information from their foreign counterparts.

This makes sense as companies are handsomely rewarded with significantly milder repercussions – under, for instance, the FCPA by the DOJ – if they detect misconduct early and if they investigate and report their findings to the DOJ.

At present, there are no practical out-of-court solutions in the CEE countries once a company is investigated or prosecuted. Unless the charges are dropped by the prosecuting authorities, the company faces lengthy prosecution in public proceedings. Nevertheless, discussions and proposals around structured settlements, non-trial resolutions and other tools available in other jurisdictions have commenced.

The growing vigilance of companies is accompanied by increased interest among CEE authorities in investigating and prosecuting companies, which is a trend that started more than 10 years ago when CEE jurisdictions, pushed by the OECD and its Working Group on Bribery,[1] the Council of Europe's Group of States against

1 For example, its report on the Czech Republic highlighted that the relatively recently enacted corporate criminal liability and the increasing prosecution of companies was showing promising results, and that increasing international cooperation and joint-investigation teams were signs of good practices. (Available at 'Czech Republic - OECD Anti-Bribery Convention – OECD'). Similar highlights can also be found in respect of other countries, such as Austria (see 'Austria - OECD Anti-Bribery Convention') and Poland (see 'Poland: Follow-up to the Phase 3 Report & Recommendations'). Progress in other states (eg, Romania and Bulgaria) has also been noted (eg, in reports issued by the European Commission).

Corruption or the European Commission, started to focus on corruption by also implementing and pursuing corporate criminal liability, not only individual criminal liability.

It took some time before prosecuting authorities turned their attention towards companies. Nowadays, it may at times be increasingly difficult to lead multi-jurisdictional investigations while satisfying all the relevant countries' laws and to make sure that the company is not punished twice for the same crime. This is one reason for which there is more and quicker cooperation between judicial authorities in different states.

To some extent, this trend was slowed down by the covid-19 pandemic and related local restrictions. The pandemic compelled several countries in the CEE region to, among other things, close their doors to their neighbours, except for essential travel; declare a state of emergency; and shift their attention towards domestic concerns.

Although this trend may have slowed down at a 'formal' level, prosecuting authorities are nonetheless becoming more and more digitally savvy and are developing their IT capabilities, thus enabling them to investigate and communicate on an informal basis while waiting for the formalities to be completed – a process that can be enormously lengthy. This trend is expected to continue despite the recent war in Ukraine, during which the focus may appear to have been shifted more to the war and its immediate local, neighbouring and trickle-down effects.

This article discusses the influence of the covid-19 pandemic on the shifting focuses of prosecuting authorities in the CEE region, the compliance status of companies and corporate investigations, and offers a brief outlook on the future. This article was also based on results in the new edition of the 'Wolf Theiss Guide to Corporate Investigations in Central, Eastern and Southeastern Europe', which addresses corporate investigation matters in detail in individual countries.

State-of-emergency bonanza

As soon as the covid-19 pandemic hit the CEE region, national governments declared states of emergency, arguing that a general lockdown was needed and that certain items and services needed immediate, non-tendered purchasing. The demand for medical supplies (face masks, gloves, ventilators, hospital beds, intensive care supplies, covid-19 tests, laboratory supplies and hospital infrastructure) and services (including non-medical related services) skyrocketed, at one time peaking by several thousand percentage points.

Public procurement contracts also soared in number, many of them deviating from standard procedure and failing to apply appropriate (or any) checks. This simplification (or inobservance) of the public procurement process has also resulted in governments hand-picking their contractors without public bidding or other competitive procedures.

Most governments kept the state of emergency or similar measures in place even after the markets in those items had soared. This led to price hikes, the development of a huge resellers' market and a number of scandals where governments used the covid-19 pandemic as an excuse to justify buying massive quantities of low-quality items from shell companies affiliated with public servants, overlooking local distributors in the process.

For example, the Czech government paid more than US$10 million to a shell company connected with money laundering schemes.[2] The Supreme Audit Office of the Czech Republic, which audited most of the transactions, noted: 'Purchases of protective equipment were accompanied by chaos, significant price differences, shortcomings in their quality, and transportation issues.'[3]

A similar situation arose throughout the CEE region: in Romania, several similar reports have been issued, and similar cases are being investigated by the authorities, including by prosecutorial bodies. In Ukraine, authorities have been able to deal directly with suppliers without going through the federal procurement system Prozorro, although it is suspected that this streamlining may have resulted in abuses of procurement procedures during the pandemic.

In Serbia, a purchase of medical supplements for approximately €10 million was executed without a public tender. The Ministry of Health approached a small number of bidders on its own initiative, and the contract was awarded to a pharmaceutical company whose management allegedly has close ties with the current ruling political elite.

Czech Members of Parliament have already set up a parliamentary commission for investigating government spending during the state of emergency, which could amount to US$1 billion over the year of its duration.

2 Sabina Slonková, 'Nákup testů do škol: podezření z praní špinavých peněz', *Neovlivní* (20 February 2021).

3 Supreme Audit Office of the Czech Republic, Data Annex to Audit Report No 20/32.

In several CEE countries, there have been parliamentary commissions or other processes for investigating government spending during the pandemic or similar periods, which could amount to billions of euros. Moreover, a stringent review is ongoing into the compensation paid to companies during the lockdowns, penalising companies for any mistakes they made and often reclaiming the compensation.

As countries have gradually emerged from lockdown and restrictions have been eased, many companies – particularly in the European Union – are readying themselves to pick up the crumbs of the massive €1.8 trillion recovery fund and NextGenerationEU programme, which will be used to reignite the European economy through public grants to fund modernisation, innovation and environmental protection. Since, in the CEE countries that are EU member states, the focus of local prosecution authorities and the focus of the European Public Prosecution Office on areas involving EU and public funds and related subsidies and public tenders is a priority, companies must ensure that they stay compliant.

The lack of visible enforcement in certain cases does not mean that prosecutorial investigations are not being carried out. As seen from previous economic crises, there are delays between the occurrence of EU and public-related fraud and the time the prosecutorial investigations become visible. The current war in Ukraine is also likely to increase some delays in at least some countries. Proactive internal checks by companies in investigating the relevant pandemic period is far more preferable to limit pending higher risks than addressing a crisis in the upcoming months or years.

Is compliance immune to covid-19 or war?

As the impact of the covid-19 pandemic continues to affect economies, companies and their management have been focusing on how to survive in the short term. A similar reaction is being seen in response to the war in Ukraine. Some areas of business have been clearly struggling to stay afloat or have had to cope with severe disruption, whereas others have been experiencing rapid growth in their operations and sales.

Overall, 'business-first' logic seems to rule the roost, and the mantra of 'no time for compliance' has – unfortunately – been increasingly applied; however, even where the situation is desperate, the ends do not justify the means. Criminal activity is no less prohibited, and a state of emergency makes the consequences more, not less, severe.

Although government authorities may appear to be busy dealing with more urgent matters (eg, the war in Ukraine), prosecuting authorities are active in investigating crimes pertaining to the pandemic. Some of those authorities are now more experienced and more equipped than they had been during economic crises that generated more non-compliance.

Not only were most businesses affected by the pandemic, but fraudsters and criminals were also affected, as indicated in a report from the Association of Certified Fraud Examiners.[4] The longer the lockdowns and other restrictions persisted, the more frequent fraudulent and corrupt behaviour became, increasing by almost 80 per cent on average.

By contrast, companies admitted that it had become more difficult to investigate and, in particular, detect misconduct.[5] This poses an especially high risk to companies whose employees have had to endure a work environment fraught with uncertainty, prolonged lockdown and other restrictions, and a sense of urgency in their day-to-day business.

Altogether, this has created a particularly demanding scenario for companies' board members and managing directors, who, on the one hand, had to deal with short-term to medium-term lacks of liquidity, restrictions and supplier shortages and, on the other hand, had to ensure compliance within their companies – all of which form part of their management duties.

Although all those events and risks have been clouding companies' compliance goggles, now is a crucial time for companies to endorse culture. How do you protect your business and eliminate unnecessary risk? And what should be done to prevent various entities from using these times as an opportunity for self-gain?

A representative of a company who is wondering whether its CMS is effective may consider the following questions.

- Is the company's management on all levels committed to compliance, with a zero-tolerance attitude? Would the company's subordinates confirm it if asked anonymously?
- Can the company convincingly explain to local prosecuting authorities, among others, why it has opted for the measures it has implemented and how they could detect a crime?
- Can the employees explain why they follow concrete procedures?
- Are the company's internal procedures adjusted to take into account changes in local laws and circumstances?

4 Association of Certified Fraud Examiners' report 'Fraud in the Wake of COVID-19: Benchmarking Report'.

5 ibid.

Conduct and (online) tone from the top

With the focus during the pandemic and the war on financial resilience, we have often looked at leadership's approach to a company's compliance; however, is the role leadership really the only one that is key?

Indubitably. Commitment by management (on all levels) is the most critical element of a functioning CMS – even more so in times of great uncertainty. Exemplary leadership is a key driver for employee behaviour. Senior and middle management should frequently express their commitment to compliance to help ensure employees understand that compliance remains a priority for the company, as employees will look to their leaders for guidance on how to do business and how to work despite restrictions, as well as for peace of mind.

This requires some clarification. Employees often incorrectly assume that phrases such as 'expressing commitment to compliance' are merely 'empty corporate speak'; however, a leader does not have to be detached from employees. On the contrary, the more the leader detaches himself or herself from his or her subordinates, the less genuine and credible he or she is perceived. There is no reason why a leader cannot express commitment to compliance through, for example, a meme posted in a team WhatsApp chat if appropriate.

CMS: fake versus real

Despite its key role, it still comes as a surprise to many companies that authorities in the CEE region also expect them to have a real CMS in place. A real CMS must be effective and well implemented, with a clearly defined and simple process flow. It must be adapted to the firm's needs and support its business.

By contrast, a 'fake' or superficial CMS exists where risk assessment is only theoretical, where it does not operate as an organic process, does not adapt to the business set-up and where responsibilities and process flow are only superficially defined. This type of 'compliance' is compliance by declaration only, and it is increasingly being sanctioned. Further, tremendous risks and future costs arise for companies, directors and shareholders that do not address fake compliance.

What if non-compliance results in investigations under lockdown?

Compliance is also a business concern, and it is costly if performed badly. Failures in this area are extremely expensive and damaging to reputation. Companies and members of their boards face significant criminal sanctions, fines or bans from participating in

tenders if they fail to investigate non-compliance, as most countries in the CEE region actively prosecute companies for crimes, in particular those pertaining to corruption, money laundering and tax evasion.

Companies' board members must not only implement appropriate procedures to prevent misconduct, but must also investigate any detected misconduct, which often includes formal corporate investigations. If a board member suspects misconduct but does not ensure that it is diligently investigated, then he or she risks liability for breach of fiduciary duties, and the company could hardly claim that it had an effective CMS in place if its board members, managers, etc, do not follow it.

Most jurisdictions in the CEE region either allow companies to release themselves from criminal liability if they prove that they had an effective CMS in place or consider an effective CMS as a mitigating circumstance; thus, the company must react with zero tolerance to any non-compliance and conduct its root cause analysis to be able to effectively improve the CMS.

This may be problematic from a practical point of view. Many activities are still being carried out remotely. Trips and personal meetings have been cancelled and continue to be limited. Consequently, conducting investigations, third-party checks or compliance training is a challenge, and many companies are either withholding their internal compliance meetings and trainings or doing them via videoconferencing. These are vital elements of a CMS.

The same applies for dealing with misconduct. Remote hearings of witnesses or potential suspects takes time and might be more complicated, but companies should not feel discouraged by this, since a great deal of corporate investigations can be done remotely. The trend of shifting investigations into the digital sphere was becoming apparent even before the covid-19 pandemic.

On this basis, companies should apply and strictly abide by the 'document everything' rule so that, at a later date, they are able to prove how certain decisions were taken. Whistle-blower protection is also increasing in importance, with various irregularities and fraud becoming more frequent.

Companies should, therefore, invest further attention in maintaining and developing whistle-blowing platforms to sustain their level of compliance and prepare their business for the aftermath in the event that non-compliance occurs and the authorities return with questions.

For corporate investigations, the situation in the field has changed rapidly. Companies' corporate investigation environments may look very different today from what they looked like one to two years ago and certainly from what they will look

like in the coming years – perhaps because the covid-19 virus has become a common threat or perhaps because its constant mutations will keep human vaccination efforts busy for a few years yet. The war in Ukraine will also bring changes.

For example, the impact of the covid-19 pandemic and the war on interpersonal relationships is enormous. There is little to no direct interaction between co-workers, which is often one of the sources of non-compliance in companies, since colleagues feel safer confiding in their colleagues than in their superiors.

There is also reduced motivation to report issues of concern as the uncertainty and sense of urgency caused by the pandemic or the war might make employees more disorganised, meaning that chaos and non-compliance suddenly becomes more of a standard way of working. Disruption of employees' working routines may also cause problems for investigators, who may struggle to find suspicious working patterns, given that there may not be any reliable routines to follow – even usual work might appear suspicious.

The absence of the usual tools – human resources, time and personal interaction – and logistical barriers to conducting in-person interviews, also makes investigations more detached from employees. Usually, the smallest changes in facial expression and body language can be hugely important sources of information for interviewers, and personal contact affects the interviewee subconsciously in terms of their reaction to the situation, the presence of interviewers and the inescapability of the interview.

With videoconferencing tools, the only sign the interviewer can rely on is the voice of the interviewee. Moreover, a convenient internet outage on the interviewee's side following an unpleasant question can bring an early end to the surprise question. The problem of how video interviews can be seen by interviewees as confidential enough also remains, which results in interviewees being cautious.

On the other hand, remote interviews have several benefits, especially for non-confrontational interviews: interviewees tend to be more open and talkative; elimination of the need to have several people physically in the same place allows for a larger number of interviews to be held within a shorter time frame, which increases efficiency; and the possibility of screen sharing and simultaneous discussion on the contents of certain documents by participants appears to have been very useful in practice.

Finally, having limited access to potentially relevant data means that existing IT infrastructures must provide complete data sets for investigations. Companies that are not yet using clouds should find a dependable solution for collecting data on the work of remote employees.

Such data might not be available owing to privacy concerns; therefore, companies should strive to have in place, or swiftly adopt, the internal policies necessary to govern working conditions during the pandemic and the war, and should inform employees about any compliance audits that may include their personal data.

In some CEE countries, companies are completely prohibited from reviewing data relating to employees who have not been informed beforehand that their data may be reviewed in the event of non-compliance. In others, the review must be very carefully balanced against employees' privacy interests.

An opportunity to improve processes

If the best time to prepare for the crisis was before it happened, the second-best time is now. Crises and urgency help companies to focus. Focus is particularly important when it comes to setting up compliance measures as it enables companies – driven by a sense of urgency – to select only the truly important measures and omit the less important ones.

In theory, this is a no-brainer. CMSs must be simple, clear and easily understandable to employees. This would exclude complex and lengthy processes in which important measures are often diluted by unimportant ones, which often results in less focus but greater obligation. This, in turn, feeds the sense of chaos felt by the average employee who, in the end, may choose simply to ignore it.

So what should be done with existing policies and procedures? Companies' CMSs are generally designed to function under 'normal' operating conditions. A CMS that mitigated risks effectively before may have now become ineffective or even too restrictive, obstructing the normal operation of day-to-day tasks. Other measures may be ineffective and may give companies a false sense of security.

It is, therefore, essential for companies to conduct new risk assessments to understand the areas where they may have new exposures or gaps. Existing risks may need to be reprioritised. One highly recommended solution is the implementation of a graded CMS that is designed to work under various conditions. With this solution, the 'covid-19 mode' (including post-covid-19) could be triggered if the situation deteriorates, with some measures being alleviated and other more stringent measures being established, and vice versa if the situation improves.

Regarding the current war in Ukraine, it is likely that the changes brought to CMSs during the covid-19 pandemic will require fewer adjustments than those pre-pandemic. There are also likely to be war-related effects and changes from a compliance perspective.

At the same time, both with regard to the pandemic and the migration of companies and employees from war zones, the digital world removes the geographical obstacles to business, compliance and corporate investigations, greatly enhancing their efficiency; however, this is a double-edged sword. CEE countries regulate many things differently (privacy laws, employee interviews, data-gathering and reviewing, etc), and the regulations have geographical obstacles.

Companies should have local jurisdictional obstacles in mind when implementing or unifying regional measures. There have been several occasions where a local company had no local internal policies but had merely adopted other companies' European, US or other foreign policies, which were inadequate locally.

Corporate investigations should not be exempt from this process. The trend in digitalisation and the shifting of companies' employees, documentation and activities online (where possible) will continue regardless of the covid-19 pandemic or the war, which are merely accelerating change. Companies have been handed an opportunity to understand new obstacles to their investigative activities, revisit policies, re-establish priorities and develop a better understanding of their IT infrastructure and employees.

Zero-based redesign of the CMS

Corporate criminal liability being implemented almost CEE-wide, together with the push from international and European organisations to investigate and prosecute corruption, including the European Public Prosecution Office, has resulted in FCPA-like investigations, which are more common and professional.

The best way to significantly improve CMSs and processes – in particular for larger companies – is to apply a zero-based redesign.

For most people (sometimes also the ones tasked with maintaining or creating a CMS), the decision to omit or delete something and to focus on selected key areas is notoriously difficult. The fear of omitting some measures, even though in practice they pose no benefit or do not mitigate any risk, may be paralysing. Minor measures have been stacked on top of one another in old CMSs, resulting in an overcomplicated and stiff set of procedures and rules.

Typically, compliance measures are not monitored for effectiveness over the long term. The worst-case scenario is that, despite employees changing as the companies grow, measures continue to be applied just because they have been applied since time immemorial – even though new compliance employees may have no idea why the measures were set in the first place, and there is no original risk analysis nor other

documentation. In that scenario, the companies would be functioning with a set of old, ineffective and redundant measures based on pre-digital risk assessment that should no longer be relied upon.

If an event of non-compliance occurs and local or international prosecuting authorities open an investigation, they will assess the company's CMS.[6] Companies must shine and show that their CMS is effective and that the criminal activity was possible only because of its sophistication and its bypassing of the CMS. The worst-case scenario tends to be that the company cannot show either of those points.

6 This assessment is becoming similar to the US Department of Justice's 'Evaluation of Corporate Compliance Programs'.

BOGDAN BIBICU
Wolf Theiss

Bogdan Bibicu is a member of the firm-wide investigations, crisis response and compliance practice at Wolf Theiss and he coordinates the practice in Romania. He specialises in corporate investigations, compliance, corporate criminal liability/white-collar crime, asset recovery and related matters.

Prior to joining Wolf Theiss, Bogdan established and built up the local and firm-wide compliance, risk and sensitive investigations practice at another regional law firm. Bogdan has gained extensive experience in various sectors, particularly life sciences, infrastructure, IT/TMT, professional services, engineering, transport and the public sector, where he advised clients on locally and internationally triggered issues and investigations.

Bogdan has also led a number of internal investigations in CEE/SEE and advised on various compliance issues, including setting up various compliance programmes. His expertise is complemented by a wealth of experience in the areas of finance, restructuring and insolvency, projects, TMT, life sciences and pharmaceuticals.

As of 2022, he serves as officer of the Anti-Corruption Committee of the International Bar Association. Bogdan has also published extensively and is a frequent speaker at compliance and anti-corruption events.

JITKA LOGESOVÁ
Wolf Theiss

Jitka Logesová heads the regional investigations, crisis response and compliance practice at Wolf Theiss and specialises in corporate investigations, compliance, corporate criminal liability/white-collar crime and asset recovery.

Before joining Wolf Theiss, Jitka established and built up the firm-wide compliance, risk and sensitive investigations practice at another regional law firm. She was also tasked by the Czech Prosecutor General's Office to help draft the methodology for state prosecutors to evaluate corporate compliance management systems and to educate the Czech state prosecutors in this respect.

Jitka has a breadth of experience in various sectors, where she has advised clients on FCPA-triggered issues and investigations, led a number of internal corporate investigations in Central and Eastern Europe and advised on various compliance issues, including setting up anti-corruption and compliance programmes. She has led multiple pre-acquisition anti-bribery and anti-corruption due diligence processes.

Jitka is the immediate past chair of the IBA's Anti-Corruption Committee and a current member of the advisory board of the IBA's Anti-Corruption Committee. Besides her legal qualifications, she is a certified auditor for ISO 19600 (compliance management systems) and ISO 37001 (anti-bribery management systems). She has also published extensively and is a frequent speaker at compliance and anti-corruption conferences.

JAROMÍR PUMR
Wolf Theiss

Jaromír Pumr specialises in compliance and corporate investigations. His work focuses on corporate criminal liability issues in the Czech Republic, as well as anti-bribery and fraud-related advisory. He regularly assists clients in revising and creating compliance management systems to protect their businesses and minimise potential risks.

Before joining Wolf Theiss, Jaromír gained experience as a government lawyer at the Law and Administration Department of the Czech Ministry of Education. He also worked as a legal trainee at two local law firms, specialising in dispute resolution law.

Wolf Theiss

Wolf Theiss is one of the leading European law firms in Central, Eastern and South-Eastern Europe with a focus on international business law. With 340 lawyers in 13 countries, over 80 per cent of the firm's work involves cross-border representation of international clients. Combining expertise in law and business, Wolf Theiss develops innovative solutions that integrate legal, financial and business know-how.

Pobřežní 12
186 00 Prague 8
Czech Republic
Tel: +420 234 765 111
www.wolftheiss.com

Bogdan Bibicu
bogdan.bibicu@wolftheiss.com

Jitka Logesová
jitka.logesova@wolftheiss.com

Jaromír Pumr
jaromir.pumr@wolftheiss.com