

# THE WOLF THEISS GUIDE TO:

Corporate Investigations  
in Central, Eastern &  
Southeastern Europe

# THE WOLF THEISS GUIDE TO:

## Corporate Investigations in Central, Eastern & Southeastern Europe

This 2021 Wolf Theiss Guide to Corporate Crises and Investigations is intended as a practical guide to the general principles and features of the basic legislation and procedures in countries included in the publication.

While every effort has been made to ensure that the content is accurate when finalised, it should be used only as a general reference guide and should not be relied upon as definitive for planning or making definitive legal decisions. In these rapidly changing legal markets, the laws and regulations are frequently revised, either by amended legislation or by administrative interpretation.

Status of information: Current as of 1 July 2021

**Conception, design, and editing:**

WOLF THEISS Rechtsanwälte GmbH & Co KG, Attorneys-at-Law  
Schubertring 6, 1010 Vienna, Austria  
[www.wolftheiss.com](http://www.wolftheiss.com)

TABLE OF CONTENTS

FOREWORD	04
COUNTRY CHAPTERS	06
ALBANIA	06
AUSTRIA	15
BOSNIA AND HERZEGOVINA	25
BULGARIA	36
CROATIA	45
CZECH REPUBLIC	53
HUNGARY	62
POLAND	71
ROMANIA	82
SERBIA	93
SLOVAK REPUBLIC	103
SLOVENIA	113
UKRAINE	123
OUR OFFICES	131

# FOREWORD

## New edition reflects rising importance of digital aspects of investigations

Two years after we published the first edition of the **Guide to Corporate Investigations in Central, Eastern and Southeastern Europe**, we are pleased to share its second and significantly revised version.

2020 was deeply shaped by the Covid-19 pandemic, which also had a powerful impact on the way corporate investigations are conducted.

**Corporate criminal liability** has been an important trigger for most corporate investigations in CEE/SEE. The drivers were *not only local laws and local prosecution but also foreign anti-corruptions laws* such as the *Foreign Corrupt Practices Act*, anti-money laundering legislation and more recently also whistleblowing protection legislation, which includes a specific obligation for companies to properly investigate reported misconduct internally.

## Regional network and local knowledge offer advantages for our clients

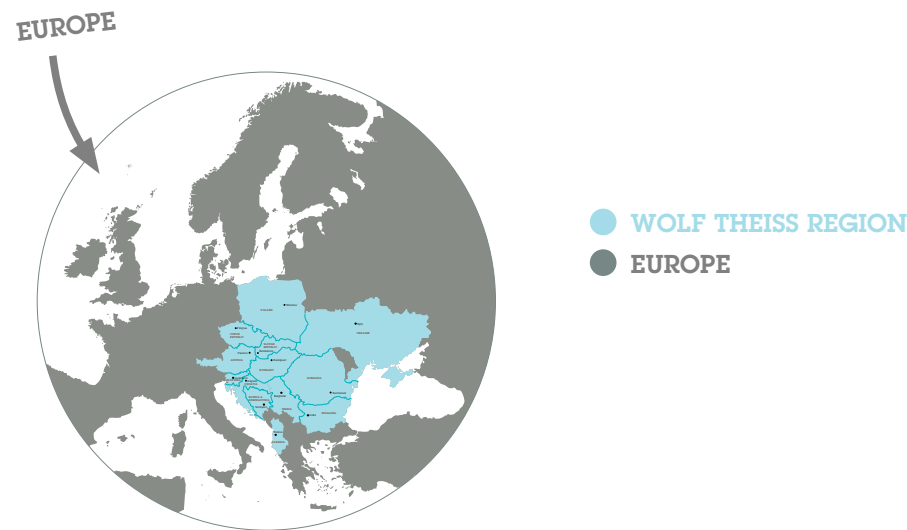
With 340 lawyers across 13 countries located throughout the region, the strength of Wolf Theiss has always been its regional coverage and experience. This is particularly true for our Corporate Investigations Team. With local contacts and regional knowledge, we are familiar both with the risks inherent in large-scale cross-border investigations and with the particularities of smaller, targeted investigations. We have capitalised on our knowledge and experience in our previous Guide to Corporate Investigations published in 2019 to reflect in this edition *the rising importance of the digital aspects of investigations*.

If you have any questions about how to prepare for investigations or how the contents of this guide may impact your business, please do not hesitate to contact us directly.



**Jitka Logesová ■ July 2021**

Partner, Wolf Theiss, Head of firm-wide Corporate Investigations Practice Group





# ALBANIA

## KEY TAKEAWAYS

- Companies may be criminally liable for the misconduct or criminal offences of their employees and board members committed on its behalf or for its benefit.
- Investigating misconduct is included in management's fiduciary duties.
- Processing of employees' data during an investigation process must be fully compliant with internal regulations on data protection.
- Legal privilege is limited to the obligation of licensed attorneys to preserve in confidentiality information received from their clients.
- Self-reporting or cooperation with prosecuting authorities might be considered as mitigating circumstances.

## OBLIGATION TO INVESTIGATE CRIMINAL MISCONDUCT INTERNALLY

### ? Are companies obliged to investigate misconduct internally?

Subject to Art 91 and Art 150 of Albanian Company Law, the shareholders' meeting may decide to initiate a special investigation with respect to irregularities during the company's formation, in relation to the conduct of ongoing business or on the grounds that there is serious suspicion of a breach of law or Statute. The special investigation must be conducted by an independent auditor, appointed by the shareholders. The investigation primarily aims to identify claims for compensation against members of the administrative organs and shareholders.

Initiation of special investigations and the nomination of a special auditor may also be requested by minority shareholders representing at least 5% of the votes, as well as by creditors of the company. The special investigation must be requested within three years of the date of the alleged irregularity. If the general meeting refuses to initiate a special investigation, the requesting shareholders or creditors may file with the court the request to initiate such an investigation.

### ? In which situations will a decision to internally investigate be necessary to prevent the civil or criminal liability of board members?

All legal entities are liable for criminal offences perpetrated while carrying out their activity. The criminal liability of a legal entity does not exclude the criminal liability of the natural person who contributed to the offence. In addition, a legal entity shall be liable for criminal offences carried out by its representatives or corporate bodies, in the name of or for the benefit of the legal entity.<sup>1</sup> A company is liable to pay for any damages resulting from its unlawful acts.<sup>2</sup>

In case of any reasonable suspicion of a possible wrongdoing, the management is expected to take all appropriate steps to review (and rectify, if necessary) the situation. Unless an internal investigation is conducted, the directors risk being found in breach of their fiduciary duties and could, therefore, become liable for any prejudice (including damages) to the company that could have been prevented, had the wrongdoing been discovered in time.

1 Art. 3 of Law No. 9754, of 14.6.2007 On Criminal Liability of the Legal Entities.

2 Art. 32 of Law No. 7850, of 29.7.1994 On the Civil Code as amended from time to time.



Criminal sanctions may be brought against both the legal entity and the individuals who committed the criminal offence, i.e. non-reporting of alleged corruption, etc.

There is no specific threshold to trigger criminal liability.

**? Is there a duty to report the outcome of the internal investigation or any information obtained during the internal investigation to enforcement authorities?  
If so, who is subject to the reporting duty and who is exempt?  
Are companies obliged to self-report?**

All individuals and companies are bound by the legal obligation to immediately report (or prevent happening) any crime or criminal offence. Only the following categories may be exempted by such an obligation: close relatives and the persons who acquire knowledge about such a crime or criminal offence due to their profession are bound by a confidentiality obligation.<sup>3</sup>

In order to avoid any false reporting, diligence must be shown during the investigation process, evaluation of the credibility of the source, etc. and reporting would then be made once the suspicion is confirmed.

Moreover, any proof or evidence that is found during the investigation process must be handed to the competent enforcement authorities. Only the author of the crime/criminal offence and the persons who acquire knowledge about such proof/evidence due to their duty or profession are exempted from such an obligation<sup>4</sup>. Elimination, destruction, altering or falsification of proof/evidence is considered a crime.

**? Would cooperation and voluntary self-disclosure be taken into account by the law enforcement authorities in relation to both individual and corporate liability?**

Cooperation and voluntary self-disclosure should be considered at least as mitigating circumstances (i.e. leading to a lower sanction).

## PLANNING AND STRUCTURING INTERNAL INVESTIGATIONS

**? How should internal investigations be structured?  
When should an internal investigation be conducted by an attorney?**

Any internal investigation must be conducted in compliance with the rules provided under an internal regulation on investigation procedure which the company must adopt as part of the compliance management system. It should specify the persons responsible for dealing with internal investigations (usually an independent compliance function) and how the structure of the internal investigation should be decided, including a process for independent reporting.

<sup>3</sup> Art. 300 Criminal Code of the Republic of Albania

<sup>4</sup> Art. 304 Criminal Code of the Republic of Albania

## CONFIDENTIALITY AND LEGAL PRIVILEGE

- ? Who can be protected by attorney-client privilege ("legal privilege")?  
Which information/data is and is not protected by legal privilege, and  
what (if any) are the exceptions from legal privilege?**

"Legal privilege" under Albanian law is extended to communication between attorneys and their clients as well as the documentation/information obtained by the attorney in the course of providing legal advice; i.e. not just during regulatory or criminal investigations, but during all administrative authority procedures as well as all court procedures launched by Albanian authorities or before Albanian courts.

Such legal privilege will prevent Albanian authorities from reviewing or using as evidence any communication containing legal advice, as well as the documentation/information obtained by the attorney in the course of providing legal advice.

The attorney has a duty to protect the confidentiality of information received from the client and may not disclose any information to a third party without the client's prior consent, except to the extent the attorney is required to do so by any applicable law, rules or court order. The attorney may not use such information or otherwise refer to it in any documents that might be created after the respective documents that contain such type of information are handed over to the client.

- ? Does legal privilege extend to documents created by attorneys after they are handed over to the client?**

The confidentiality obligation shall be extended to any information or documents received from the client during provision of legal services.

- ? Does legal privilege apply to in-house lawyers?**

Legal privilege may be applied if the in-house lawyer qualifies as an attorney (i.e. is registered with the Albanian Bar Association and the tax authorities) and not as an employee.

- ? Does legal privilege apply to other types of service providers?  
Can legal privilege be extended to them if they are subcontracted by attorneys?**

Legal privilege is reserved for attorneys (and attorneys' personnel) and in our view it extends to third parties subcontracted by the attorney to represent the client.

Other regulated professions such as auditors, notaries etc. are also bound by certain secrecy obligations, but these privileges fall rather within the client-provider relationship.

## COLLECTING AND PROCESSING DATA AND DATA PRIVACY PROTECTION

### ? How should the company ensure that evidence is properly collected?

The company should notify the employees about the processing and preservation of the data relevant for the matter investigated.

Implementation of specific IT safeguarding measures in the process of collection and preservation of evidence would be recommended.

### ? What conditions must be met to allow investigators access to employees' emails/other records which potentially contain private information? Is the consent of the custodian necessary before data collection begins?

In principle, personal data processing may take place only on grounds specified by Albanian Data Protection Law.

With regard to processing employee data, an employer may collect, process and transfer data concerning its employees only to the extent that the data relates to the employee's suitability for employment or is necessary for the performance of the employment contract,<sup>5</sup> i.e. the data processing is necessary in the legitimate interests of the controller or any third parties (i.e. the necessity to perform contractual obligations), except where such interests are clearly in contradiction with the privacy right of the data subject.

The following elements need to be considered: the reason for collecting the information/data; the limit to which data controllers are able to use the personal data collected, the individual consent given by the employee for the employer to access the employee's email, and the security measures in place. Further to the consent of the employee, we recommend that the following is taken into consideration by the employer:

- The access and use of email correspondence should be strictly for legitimate purposes and only for the purposes for which the employee has given consent. The employee has the right to withdraw consent at any time. Such a withdrawal does not affect the validity of any actions carried out up to that point and which were within the scope of the consent previously given.
- The confidentiality of personal data must be ensured at all times; therefore, email communications must be accessed only by authorised personnel for legally authorised purposes.
- Any personal data collected during the access of the employee's email should be protected against accidental or unlawful destruction, storage, processing, access or disclosure of data.
- There should be an internal policy in place regulating the use of IT equipment, such as sending emails for private purposes, and the consequences in the event of any breach thereof. Employees should be informed in writing and should sign their acknowledgment of the policy.
- The employer must inform the data subject of their rights; such as the right to withdraw consent at any time, the period for which the data will be stored, as well as the employee's right to access/correct information.

---

5 Instruction no. 11, of 8. 9.2011 of the DCM.

The processing of sensitive data is lawful if there is a legitimate reason. However, the employee's explicit written consent is required and the personal data may be processed only for the purpose for which the data subject has given consent. The consent must be absolutely clear and should cover the specific processing/transfer details: (i) the type of information (or even the specific information itself), (ii) the purpose of the processing/transfer, (iii) the category of recipients, and (iv) any special aspects that may affect the individual, such as any disclosures that may be made during the retention period.

The Data Protection Law further establishes certain minimal and standard requirements for the protection of personal data. Under Data Protection Law the data collector is obliged to ensure that organizational and technical measures are in place to protect personal data from: (i) being illegally destroyed or accidentally lost, (ii) unauthorized access and persons, and (iii) illegal processing.

The extent of the processing must be that strictly necessary to achieve the aim of the investigation, and there must be no less-invasive measures available. The information included in the investigation should be carefully selected prior to review and no private information should be accessed as part of the investigation. It is essential that the right key words are selected, and the reviewers are sufficiently trained.

The company must notify the employees that their data may be processed as part of any investigation as well as about the legal basis and purposes of the data processing and the corresponding rights of the employee.

**? Are there any restrictions in relation to cross-border transfers of data collected during an investigation?**

Strict conditions apply to cross-border transfers of data collected during investigations to countries that do not provide sufficient levels of data protection (i.e. outside of the EU or EEA). In principle, personal data processing may take place only on the grounds specified by Albanian Data Protection Law.

Cross-border transfer of data collected during an investigation to a third country is subject to strict requirements. In particular, companies must ensure adequate protection of the data even after its transfer to a third country. Available and adequate means include binding corporate rules and standard data protection clauses adopted by the Commissioner Office.

**? What should the company do once the internal investigation is finished?**

Once the internal investigation is finished, all the personal data gathered and processed during the internal investigation must be destroyed except for the final findings/conclusions which will be used internally i.e. during disciplinary proceedings. In case there are sufficient grounds to report the case to the prosecution office, the findings shall be reported along with the evidence or indications found.

## **INTERVIEWING EMPLOYEES**

**? Does an employee have an obligation to actively participate in interviews organised by the counsel of the employer?  
Is an employee required to participate and cooperate in interviews?**

No, the employee is not explicitly bound by such an obligation. However, employees are bound by the legal obligation to inform the employer of all circumstances that affect or may affect the performance of their duties, as well as to refrain from taking any actions that may incur material damages or might be considered as detrimental to the employer.

If the employee decides to cooperate, the interviews should take place within the working hours of employees and should be strictly connected to their work.

**? Do employees have the right to receive minutes from the interview?**

No.

**? Do employees have the right to be informed of the outcome of the investigation?**

No.

## WHISTLEBLOWING

**? Is there any specific regulation relating to whistleblowers?  
If so, is there any obligation to react to whistleblowing/to have a system in place for reacting to whistleblowing?**

Yes, there are specific regulations for employers operating whistleblowing systems. By law<sup>6</sup> all public institutions and private companies operating in Albania, and which have more than 100 employees, have to set up a special unit to register and investigate alleged cases of corruption. Any allegations of corruption be reported to the High Inspectorate of Declaration and Audit of Assets (HIDAA) and/or the prosecution office.

A whistleblower may choose to remain anonymous and the employer must respect this (also in case of anonymous reports). Generally, whistleblowers are protected from retaliation and cannot be fired or demoted. They cannot be penalized in any other way either, such as blacklisting, reduction of pay, reassignment, salary decrease, loss of office or privileges or change in duties. Failure to comply with this obligation may lead to a fine of up to ALL 500,000 (approx. EUR 4,000). In addition, any failure by the employer to initiate an investigation after receiving an indication of corruption by an employee, may also lead to a fine of ALL 500,000 (approx. EUR 4,000).

Any act of retaliation against the whistleblower will be investigated by the competent authorities, i.e. HIDAA, or the prosecution office, and the whistleblower has the right to ask for compensation for any damages incurred as a result thereof.

## CRIMINAL PROCEEDINGS AGAINST THE COMPANY

**? Is there corporate criminal liability in the country?**

Yes. All legal entities are liable for criminal offences perpetrated while carrying out their activity. The criminal liability of a legal entity does not exclude the criminal liability of the natural person who contributed to the offence. In addition, a legal entity shall be liable for criminal offences carried out by its representatives or corporate bodies, in the name of or for the benefit of the legal entity.<sup>7</sup> A company is liable to pay for any damages resulting from its unlawful acts.<sup>8</sup>

---

<sup>6</sup> Law No. 60/2016 On Whistleblowing.

<sup>7</sup> Art. 3 of Law No. 9754, of 14.6.2007 On Criminal Liability of the Legal Entities.

<sup>8</sup> Art. 32 of Law No. 7850, of 29.7.1994 On the Civil Code as amended from time to time.

**? Can individuals and companies both be prosecuted for the same misconduct (parallel prosecution)?**

Yes. Both the company and the individual may be prosecuted for the same misconduct; although they face different criminal sanctions.

**? Can corporate criminal liability be avoided or mitigated?**

Yes. All legal entities are liable for criminal offences perpetrated while carrying out their activity. The criminal liability of a legal entity does not exclude the criminal liability of the natural person who contributed to the offence. In addition, a legal entity shall be liable for criminal offences carried out by its representatives or corporate bodies, in the name of or for the benefit of the legal entity.<sup>9</sup> A company is liable to pay for any damages resulting from its unlawful acts.<sup>10</sup>

**? Can criminal proceedings be settled with the enforcement authorities, or through leniency programmes?**

There are full or partial leniency programmes for those legal entities that cooperate or provide important information for the identification and prevention of prohibited agreements, or the identification of the responsible persons or for those that disclose or provide important information in cases of active or passive bribery. The same would be applicable for tax offenses. Mitigating circumstances that might lead to a lower sanction for the legal entity would be also when the legal entity has fully disclosed and made available their incomes for the purpose of confiscation or if the legal entity shows that it has duly implemented effective measures to prevent the criminal activity.

## UPCOMING DEVELOPMENTS

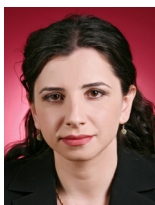
Generally, since companies became liable for criminal prosecution thirteen years ago, prosecution of companies remains of low profile and prosecuting authorities have mainly focused their attention on tax infringements. This may however change in consideration of the ongoing reform affecting prosecutions authorities and courts in Albania. However, it appears that substantial change will require years to become perceptible and produce the desired effects.

---

9 Art. 3 of Law No. 9754, of 14.6.2007 On Criminal Liability of the Legal Entities.

10 Art. 32 of Law No. 7850, of 29.7.1994 On the Civil Code as amended from time to time.

*This chapter was written by Jonida Braja Melani and Denis Selimi.*



**JONIDA BRAJA MELANI**  
Associate

**Wolf Theiss, Albania**

T. +355 4 227 4521 213  
[jonida.braja@wolftheiss.com](mailto:jonida.braja@wolftheiss.com)



**DENIS SELIMI**  
Associate

**Wolf Theiss, Albania**

T. +355 4 227 4521 203  
[denis.selimi@wolftheiss.com](mailto:denis.selimi@wolftheiss.com)



WOLF THEISS

AUSTRIA



## KEY TAKEAWAYS

- Under the Corporate Criminal Liability Act, national or foreign companies can be held criminally liable for the misconduct of their decision-makers and employees. In recent years, crimes prosecuted under this Act have significantly increased.
- The obligation to investigate misconduct results from the statutory duty of care of board members and forms part of a sound compliance management system.
- Internal directives regarding the storage of data by employees can potentially facilitate (future) internal investigations.
- Statutory provisions on legal privilege do not extend to in-house lawyers.
- Self-reporting and cooperating with prosecuting authorities can, under certain circumstances, be beneficial to the company.

## OBLIGATION TO INVESTIGATE CRIMINAL MISCONDUCT INTERNALLY

### ? Are companies obliged to investigate misconduct internally?

There is no general statutory obligation under Austrian law according to which the company must conduct internal investigations when misconduct is detected (see exemptions in the next paragraph). However, it is advisable to conduct internal investigations, in order to (i) avert potential damages to the company, (ii) cooperate with official authorities as soon as criminal investigations should be conducted and (iii) have the opportunity to demonstrate cooperation and remorse after a crime has been committed. The conduct of the company after the commission of a crime must be duly considered by the authorities in various ways (e.g. the public prosecutor can, under certain circumstances, refrain from initiating criminal proceedings against the company, taking into account the company's behaviour after the crime).

### ? In which situations will a decision to internally investigate be necessary to prevent the civil or criminal liability of board members?

From a strategic point of view, it is advisable that as soon as the management board or the supervisory board members become aware of or suspect any wrongdoing that might constitute criminal liability (either for individuals or the company) inside their scope of responsibility, they initiate internal investigations as a mitigation measure.

Under certain circumstances the omission of mitigation measures might even lead to the criminal liability of the respective board members themselves. According to the Austrian Criminal Code, if the law criminalises causation of a result,<sup>1</sup> any person failing to avert that result shall also be criminally liable if the person has a legal duty to act.<sup>2</sup> The respective duty to act results from due diligence obligations under the relevant civil and commercial law provisions for companies.<sup>3</sup> If a board member becomes aware of a criminal act being committed, it is also possible that he/she becomes criminally liable as a participant.<sup>4</sup>

1 E.g. the occurrence of a damage pursuant to Art. 146 StGB – Fraud).

2 Art. 2 of the Austrian Criminal Code (*StGB, Strafgesetzbuch*).

3 I.e. Art. 84 para 1 AktG; Art. 25 para 1 *GmbHG*.

4 Any person contributing in any way to the offence is taken to have committed the offence apart from the immediate perpetrator Art. 12 StGB.

In addition, the management board can be obliged, according to their general duty of care,<sup>5</sup> to pursue claims of the company against other or former board members or employees for which the prior performance of an internal investigation is often necessary. Furthermore, the supervisory board can be obliged to conduct such investigations regarding potential wrongdoings of members of the management board. If the management or supervisory board violate their duty of care by failing to pursue such claims, they can be liable for the company's damage caused by such omission. In accordance with general standards of civil liability, even a board member's slightly negligent violation of his/her duty of care is sufficient.

In summary, if a board member becomes aware of a criminal act being committed by a decision-maker or an employee and knowingly omits to act in his/her duty of care for the company to prevent the crime or mitigate possible damage, the board member can be held criminally liable himself/herself. Therefore, the initiation of internal investigations is advisable and might even be obligatory under certain circumstances.

Furthermore, Austrian statutory law provides for certain cases, in which internal investigations shall be performed. For instance, a shareholder minority of at least 10% can file a court application for the appointment of a special investigator (*Sonderprüfer*), if a prior shareholder resolution aiming at conducting such investigations could not be passed in a prior shareholder meeting with the required majority.<sup>6</sup> The subject of such investigations can be *inter alia* every action performed by the managing directors within the last two years in respect of a joint stock corporation (AG). In respect of a limited liability company (*GmbH*), such investigation is generally limited to the audit of the latest financial statements.

**? Is there a duty to report the outcome of the internal investigation or any information obtained during the internal investigation to enforcement authorities?  
If so, who is subject to the reporting duty and who is exempt?  
Are companies obliged to self-report?**

In general, only public authorities are obliged to notify criminal authorities of any committed criminal offences of which they become aware.<sup>7</sup> Only in extraordinary cases are reporting duties of other persons triggered, for example:

- In the case of specific transactions, Austrian attorneys are obliged to report cases of money laundering<sup>8</sup> or terrorist financing<sup>9</sup> to the Federal Criminal Police Office (*Bundeskriminalamt*).
- If internal investigations, which include a special audit of the company's financial statements, are conducted on an investment firm or an investment services firm, and the auditor determines severe violations of statutory laws or the articles of association, the auditor is obliged to submit a respective report to the Austrian Financial Market Authority.<sup>10</sup>

**? Would cooperation and voluntary self-disclosure be taken into account by the law enforcement authorities in relation to both individual and corporate liability?**

The Austrian Criminal Procedure Code (*Strafprozessordnung, StPO*) provides for a leniency programme (*Kronzeugenregelung*).<sup>11</sup> The leniency programme applies *inter alia* for offences that fall under the jurisdiction of the Public Prosecutor's Office for Economic Crimes and Corruption (*Wirtschafts- und Korruptionsstaatsanwaltschaft, WKStA*)<sup>12</sup> (e.g. fraud and other white collar crimes causing damage exceeding EUR 5 Mio, crimes of corruption,

7 Art. 78 para 1 StPO.

8 Art. 165 StGB.

9 Art. 278d StGB.

10 Art. 93 para 1 Securities Supervision Act, (*Wertpapiersaufsichtsgesetz, WAG*).

11 Art. 209a StPO (and Art. 209b StPO in case of antitrust violations).

12 Art. 20a, 20b StPO.

anti-competitive collusion in tendering processes<sup>13</sup>, money laundering<sup>14</sup>, etc.). The Public Prosecutor may proceed with measures of diversion (rescission from prosecution) if the suspect contributes to solving the crime. In order for the Public Prosecutor to refrain from further prosecution, the suspect must *inter alia* remorsefully confess to the crime and voluntarily self-disclose information to the authorities that goes beyond his/her own contribution to the crime. Furthermore, the information disclosed must lead to the solving of a crime mentioned by law (e.g. corruption) or lead to the investigation of a person that was the lead individual of a crime or the lead individual of a criminal organisation. If these requirements for the contribution of the suspect are met, the Public Prosecutor must stop the proceedings against the suspect. In proceedings against companies, the provisions on the leniency programme apply *mutatis mutandis*.<sup>15</sup>

Furthermore, in relation to financial crimes committed under the FinStrG (e.g. tax evasion<sup>16</sup> or tax fraud<sup>17</sup>) the Austrian Financial Criminal Code (*Finanzstrafgesetz, FinStrG*) provides for the possibility of voluntary self-disclosure (*Selbstanzeige*), which prevents the perpetrator from criminal liability if the very narrow preconditions of this provision are met.<sup>18</sup>

For certain offences against the property of another,<sup>19</sup> the law stipulates active repentance (*Tätige Reue*) under the following preconditions:<sup>20</sup>

- the person fully rectifies any damage caused by the offence; or
- enters into a contractual obligation to fully compensate the victim; and
- before the authorities become aware of the person's culpability, even at the urging of the victim but without being forced to do so.

The person is also not liable if he/she fully rectifies any damage caused after reporting to the authorities (voluntary self-disclosure) and providing the relevant compensation to the authorities.<sup>21</sup>

The Austrian Criminal Code also determines special mitigation factors (*Milderungsgründe*) that the judge must consider in his/her verdict.<sup>22</sup> These include instances in which the person:

- deliberately refrained from causing major harm although the person had the opportunity to do so, or if the person or another person rectified the harm;<sup>23</sup>
- genuinely endeavoured to rectify any harm caused or sought to avoid further adverse consequences;<sup>24</sup>
- remorsefully confessed to the offence, or through the person's testimony made a significant contribution to ascertaining the truth.<sup>25</sup>

---

13 Art. 168b StGB (*Wettbewerbsbeschränkende Absprachen in Vergabeverfahren*).

14 Art. 165 StGB.

15 Art. 209a para 6 StPO.

16 Art. 33 FinStrG.

17 Art. 39 FinStrG.

18 Art. 29 FinStrG.

19 Art. 34 No 15 StGB.

20 Art. 34 No 17 StGB.

21 E.g. fraud pursuant to Art. 146 StGB, embezzlement pursuant to Art. 133 StGB or breach of trust pursuant to Art. 153 StGB).

22 Art. 167 para 2 StGB.

23 Art. 167 para 3 StGB.

24 Art. 34 StGB.

25 Art. 34 No 14 StGB.

In summary, cooperation and self-disclosure are considered by the Austrian enforcement, prosecution and judicial authorities. Furthermore, internal investigations can be a helpful procedure to create a basis for demonstrating contrition and subsequent leniency.

## PLANNING AND STRUCTURING INTERNAL INVESTIGATIONS

### ? **How should internal investigations be structured? When should an internal investigation be conducted by an attorney?**

The company should have internal regulations in place that govern the process of dealing with (the suspicion of) misconduct including internal investigation procedures as part of the compliance management system. It should specify the persons responsible for dealing with internal investigations (usually an independent compliance function) and how the structure of the internal investigation should be decided, including a process for independent reporting.

Conducting internal investigations through an external actor can be of benefit if the misconduct has not been discovered outside of the company. In such case, any information that is obtained by an attorney who is conducting the investigation is subject to legal privilege. External performance of internal investigations may strengthen the argument that the company is willing to independently investigate all misconduct in order to properly address potential problems.

## CONFIDENTIALITY AND LEGAL PRIVILEGE

### ? **Who can be protected by attorney-client privilege ("legal privilege")? Which information/data is and is not protected by legal privilege, and what (if any) are the exceptions from legal privilege?**

In general, an Austrian attorney is bound by professional secrecy obligations in all matters which have been confided to him/her and all facts which have otherwise become known to him/her in their capacity as an attorney. Such professional secrecy is safe-guarded by various statutory provisions.<sup>26</sup>

Differences in the scope of legal privilege depend on the type of proceedings.

Under criminal procedure an attorney-at-law is entitled to refuse to give evidence (*Aussageverweigerung*). This right may not be circumvented by the confiscation of any documents or data medium or by the examination of the attorney's employees or sub-contractors. A verdict based on such evidence is null and void.<sup>27</sup>

Also, civil procedure provides for the right to refuse to give evidence in civil proceedings. However, any evidence gained by violating this right can be used in these proceedings without any further consequences.<sup>28</sup>

However, an attorney's privilege may be pierced by certain reporting obligations to the Federal Criminal Police Office (*Bundeskriminalamt*) regarding potential cases of money laundering or terrorist financing.

26 E.g. Art. 321 para 1 no. 4 Act of Civil Procedure (*Zivilprozessordnung*, ZPO); Art. 157 para 1 no. 2 StPO; Art. 171 para 2 Federal Fiscal Code (*Bundesabgabenordnung*, BAO).

27 Art. 157 StPO.

28 Art. 321 para 1 no. 4 ZPO.

**? Does legal privilege extend to documents created by attorneys after they are handed over to the client?**

In criminal proceedings, legal privilege extends to documents and information in the possession of the suspect or the attorney, which were produced for advising or defending the client (e.g. transcripts of interviews of employees, memos, internal investigation reports etc.).

**? Does legal privilege apply to in-house lawyers?**

No. Generally, in-house lawyers do not fall within the scope of legal privilege.

**? Does legal privilege apply to other types of service providers?  
Can legal privilege be extended to them if they are subcontracted by attorneys?**

Within the scope of the above-mentioned privilege are also patent lawyers, notaries and auditors as well as their employees and subcontractors. Legal privilege, as applicable for attorneys in criminal proceedings, extends to subcontractors if they are commissioned by the attorney (e.g. legal experts, forensic experts, etc).

## **COLLECTING AND PROCESSING DATA AND DATA PRIVACY PROTECTION**

**? How should the company ensure that evidence is properly collected?**

The company must determine what data is needed for the internal investigation and where they are located. Relevant questions are, for example: what means of communication are used (emails, apps, phones)? What devices do employees use to communicate? Is there any cloud or local share-drive? Is the cooperation of a local IT expert needed? Is there any information solely in the form of a hard copy document?

It is then essential to determine whether and to what extent the company can legally access and review the data. Particularly problematic are situations where the private use of the company's infrastructure is allowed or tolerated. In such case, it will be necessary to distinguish between private data and business-related data. Thus, to facilitate possible future internal investigation it is recommended to have comprehensive and clear internal directives providing the complete rules on communication, archiving and the use of company devices by employees (in particular whether private use is allowed or not) on the one hand, and explicit information on how the company can review and collect these data on the other hand.

The company should also issue a preservation notice to employees to ensure that potential evidence (and all data relevant for the matter investigated) is preserved and not destroyed. The employees in question should sign or give a confirmation that they are complying with the preservation notice, and this should be kept on the record.

**? What conditions must be met to allow investigators access to employees' emails/other records which potentially contain private information?  
Is the consent of the custodian necessary before data collection begins?**

Under data protection law, the copying, storage, filtering, review and analysis of emails and files of suspected employees located on the employer's IT infrastructure for inspection purposes or in the case of reasonable suspicion of criminal actions may be justified based on the employer's legitimate interest to investigate and/or prosecute the possible crimes.<sup>29</sup>

---

29 Art. 6 para 1 lit f GDPR.

The review must be performed in such a way that these interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (e.g. using filtering techniques to only search for the relevant parts, etc.). In general, only the review of business-related emails and files is justified without obtaining the employee's consent. The review of private personal data usually requires the employee's consent from a data protection law perspective. Employee consent is however seen critically by courts and authorities as the criteria of "freely given" might be questionable.

However, under specific circumstances the processing of private emails containing relevant information may be legitimate if it *inter alia* complies with the principle of proportionality and limitation of the privacy intrusion according to the scope of the investigation (as mentioned above).

Furthermore, the respective employees shall be informed about e.g. the inspection of their mailbox and files, the purpose of and legal grounds for the data processing, the recipients, and the employees' data subject rights. The information must be provided to the employee within specified timeframes (at the latest within 1 month of having obtained the data). It is still debated whether this information provided to the employee about the inspection might be deferred to a slightly later point in time in order to not jeopardise the investigation.

If third parties who act as data processors for the company (e.g. providing forensic services) are engaged, the conclusion of a written data processing agreement is necessary.<sup>30</sup>

Finally, it must be reviewed internally whether the processing in this context (considering the nature, scope and purposes of the processing) is likely to result in a high risk to the rights and freedoms of natural persons. If this is the case, prior to the processing, a privacy impact assessment (impact of the envisaged processing operations on the protection of personal data) must be carried out.

### **? Are there any restrictions in relation to cross-border transfers of data collected during an investigation?**

In the case of an envisaged transfer of data to countries outside of the EU/EEA, for which an adequate level of data protection has not been determined (e.g. USA), additional guarantees are required, e.g. the conclusion of the EU Standard Contractual Clauses and possible additional measures.<sup>31</sup>

### **? What should the company do once the internal investigation is finished?**

Once the internal investigation is finished, the data gathered and processed during the internal investigation must be erased, with only the most important findings stored for the purpose of confronting the employee with the findings or for potential court or administrative proceedings.

## **INTERVIEWING EMPLOYEES**

### **? Does an employee have an obligation to actively participate in interviews organised by the counsel of the employer? Is an employee required to participate and cooperate in interviews?**

Employees are generally bound by their employer's instructions, which can include the participation in interviews organised and conducted by an attorney. Members of the management board of a limited liability company can be specifically instructed by the company's shareholders, by way of a shareholder resolution, to participate in such interviews. Furthermore, a board member's general duty of care (see b. above) can lead to the obligation of board members to participate in such interviews.

<sup>30</sup> Art. 28 GDPR.

<sup>31</sup> Art. 44 et seqq. GDPR.

**? Do employees have the right to receive minutes from the interview?**

In general, no. However, under certain circumstances producing minutes that are provided to the employee could be beneficial in order to create an objective undisputable result of the outcome of an interview.

**? Do employees have the right to be informed of the outcome of the investigation?**

No.

## **WHISTLEBLOWING**

**? Is there any specific regulation relating to whistleblowers?  
If so, is there any obligation to react to whistleblowing/to have a system in place for reacting to whistleblowing?**

Specific companies, such as credit institutions, investment firms or investment services firms, are required to implement appropriate procedures for their employees allowing them to confidentially report internal breaches of certain laws, regulations or rulings and to further conduct investigations based on such reports.<sup>32</sup>

In addition, there is a general obligation pursuant to the duty of care to reasonably react to information provided by a whistleblower, which can include the initiation of further internal investigations, if appropriate and necessary.

By 17 December 2021, EU Directive Nr. 2019/1937 on the protection of persons who report breaches of Union law ("Whistleblowing Directive") must be transposed into Austrian statutory law.<sup>33</sup> The purpose of this Directive is to enhance the enforcement of Union law and policies in specific areas by laying down common minimum standards providing for a high level of protection of persons reporting breaches of Union law.

## **CRIMINAL PROCEEDINGS AGAINST THE COMPANY**

**? Is there corporate criminal liability in the country?**

Under the Austrian Corporate Criminal Liability Act,<sup>34</sup> companies can be criminally liable for the criminal acts committed by individuals: a decision-maker (Entscheidungsträger) or an employee, if the criminal act has been committed either (i) for the advantage of the company or (ii) in breach of the company's duties.<sup>35</sup>

The duties of a company<sup>36</sup> are stipulated throughout the legal system, predominantly in civil and administrative law provisions. Therefore, a compliance system might not only be necessary to prevent/mitigate corporate criminal liability, but the lack of a compliance system might even lead to criminal liability of a company in the first place.

Any corporate entity qualifies as a company,<sup>37</sup> but any official acts (hoheitliches Handeln), such as acts of the state, the federal states or any corporate entities are excluded as long as they are acting in the execution of the laws.

---

32 Art. 99g para 1 Austrian Banking Act, Art. 95 Austrian Stock Exchange Act.

33 The Whistleblowing Directive provides for different stages of transposition (cf Art 26).

34 *Verbandsverantwortlichkeitsgesetz, VbVG*.

35 Art. 3 para 1 VbVG.

36 According to Art. 3 para 1 No. 2 VbVG.

37 Art. 1 para 2 VbVG.

**? Can individuals and companies both be prosecuted for the same misconduct (parallel prosecution)?**

Yes, both individuals and companies can be criminally liable for the same misconduct. A company can only be liable for the criminal acts of an individual.<sup>38</sup> However, the corporate liability for a criminal act and the individual liability of a person for the same act do not exclude each other.<sup>39</sup>

**? Can corporate criminal liability be avoided or mitigated?**

According to section 18 of the VbVG, the prosecutor can decide to not (further) prosecute a company under certain circumstances. Such decision depends on the seriousness of the offence, the weight of the breach of duty, consequences of the criminal conduct, the possible amount of a fine and the conduct of the entity after the offence.

In relation to the last criterion (i.e. conduct of the entity after the offence), the prosecutor may take into account inter alia the company's cooperation with regard to the investigation of the offence. Conducting thorough internal investigations to dissolve criminal behaviour within the company may therefore result in the avoidance of the initiation of criminal proceedings in the first place. Furthermore, reference is made to the leniency programme (cf above).

**? Can criminal proceedings be settled with the enforcement authorities, or through leniency programmes?**

Cf the chapter concerning the leniency programme above.

## UPCOMING DEVELOPMENTS

Since the Corporate Criminal Liability Act became effective on 1 January 2006, the prosecution and indictment of companies has grown. When in the years from 2006 until 2010 the cases of prosecution including companies pursuant to the VbVG more than tripled (from approximately 50 per year to more than 160), the significance has grown even more in the past ten years. From 2013 to 2019 the cases regarding proceedings pursuant to the VbVG settled by the prosecutor grew from approximately 200 to 300 per year. In addition, between 2013 and 2019, between 20 and 25 cases were brought to court each year. Based on our experience, the prosecutors tend to assess and apply the VbVG on an increasing basis.

---

38 Art. 1 VbVG.

39 Art. 3 para 4 VbVG.

*This chapter was written by Valerie Hohenberg and Markus Taufner.*



**VALERIE HOHENBERG**  
Partner

**Wolf Theiss, Austria**

T. +43 1 51510 1021  
[valerie.hohenberg@wolftheiss.com](mailto:valerie.hohenberg@wolftheiss.com)



**MARKUS TAUFNER**  
Senior Associate

**Wolf Theiss, Austria**

T. +43 1 51510 1862  
[markus.taufner@wolftheiss.com](mailto:markus.taufner@wolftheiss.com)





WOLF THEISS

# BOSNIA AND HERZEGOVINA

Bosnia and Herzegovina (**BiH**) is a country consisting of two separate entities, i.e. the Federation of Bosnia and Herzegovina (**FBiH**) and the Republic of Srpska (**RS**), and one special autonomous district under the direct sovereignty of the state, i.e. the Brčko District of Bosnia and Herzegovina (**BD**). In addition, FBiH is divided into 10 cantons.

In each of these parts essentially different legal regimes apply; however, certain legal matters are regulated by laws enacted at the state level and as such are applicable in all parts of the country. Furthermore, in many cases the relevant legislation of the entities regulating a particular matter is harmonized, but differences may occur in terms of the application and interpretation by different entities' courts.

Certain topics in this overview are regulated at the entity/district level and others are regulated at the state level. If not specifically indicated, the regulation of certain matters is harmonised, and where applicable, a separate overview of the regimes applicable in BiH is provided.

## KEY TAKEAWAYS

- **Companies may be criminally liable for the misconduct of their employees and board members.**
- **Investigating misconduct is included in management's fiduciary duties and is a sign of a sound compliance management system.**
- **The investigation of misconduct itself is a cornerstone of a proper corporate investigation.**
- **The concept of legal privilege is limited to the obligation of registered attorneys to preserve the confidentiality of information received from their clients.**
- **Self-reporting or cooperation with prosecuting authorities does not have any automatic benefit for the company.**

## OBLIGATION TO INVESTIGATE CRIMINAL MISCONDUCT INTERNALLY

### ? **Are companies obliged to investigate misconduct internally?**

Any such obligation is not explicitly stipulated by law, however, management members are obliged to carry out their business conscientiously, with the due care expected of a prudent businessman and in the reasonable belief of acting in the best interests of the company. Shareholders and other competent bodies (if any) in the company are entitled and encouraged to investigate any failure of management to act in accordance with their duties and obligations or if they act in a way that is contrary to the applicable law and internal regulations.

Furthermore, employers are obliged to conduct disciplinary proceedings following any violation of employment obligations by the company's employees, whereas the disciplinary procedure often also involves an internal investigation.

In that regard, diligent investigation of any (potential) misbehaviour is a fundamental part of any effective compliance management system if the company wants to be released from its civil and/or criminal liability.

**? In which situations will a decision to internally investigate be necessary to prevent the civil or criminal liability of board members?**

The criminal sentence for a company may be mitigated if the managerial or supervisory body voluntarily reports a perpetrator after he/she commits a criminal offence. This means that the board members must not only set appropriate procedures to prevent misconduct, but also investigate any misbehaviour detected, which often includes an internal investigation.

Failing to conduct an internal investigation may breach the fiduciary duties of the board members, which would make him/her liable for any damage to the company (e.g. penal or administrative fines, damages to third persons, loss of further profits, etc.) which might have been prevented.

An internal investigation should be conducted to determine the employee's liability for violation of duties of their workplace, as well as if any board member should violate its obligations; causes damages to the company by failing to act with due care expected of a prudent businessman and in the reasonable belief of acting in the best interests of the company, etc.

**? Is there a duty to report the outcome of the internal investigation or any information obtained during the internal investigation to enforcement authorities?  
If so, who is subject to the reporting duty and who is exempt?  
Are companies obliged to self-report?**

Individuals and companies should generally report (i) a crime or its perpetrator or (ii) the preparation of an intended crime; after becoming aware of it report it further to applicable Criminal Codes in BiH. In certain legally prescribed cases, failure to act in the above-mentioned manner(s) is also considered a criminal offence.

This often means that the company should be able to investigate the matter to the extent necessary to report the crime(s), but that it should report it immediately once the suspicion is confirmed. Though at the same time by reporting the crime, the company could be exposing itself to criminal prosecution for it. It could be argued that individuals who represent the company (i.e. members of its executive body) should not be forced to report or testify against the company as this would represent a circumvention of its right to not self-incriminate.

However, further to applicable Criminal Codes officials (authorised employees of public service in competent authorities) or other responsible persons (authorised persons in other legal entities, e.g. managing directors) have a special responsibility to report any discovery in the course of their duties of a committed crime for which a punishment of five years imprisonment or more may be imposed, i.e. possibly sentenced to the same extent as the perpetrator of the crime itself.

**? Would cooperation and voluntary self-disclosure be taken into account by the law enforcement authorities in relation to both individual and corporate liability?**

Generally, cooperation and voluntary self-disclosure will be taken into consideration by the law enforcement authorities, especially when deciding on sanctions. However, there is no automatic benefit for self-disclosure or cooperation, and companies are not incentivized by the law to decide to self-report and cooperate with prosecuting authorities, nor can they be certain of any benefits should they decide to cooperate, share information or report misconduct.

Criminal sentences for a company whose managerial or supervisory body voluntarily reports a perpetrator after he/she commits a criminal offence can be mitigated, whereby in some cases the company may also be exonerated.

Under the applicable Criminal Codes, a perpetrator who attempts to commit a criminal offence, but voluntarily forsakes the completion of a punishable attempt, may be exonerated. However, he/she shall still be punished for any actions which constitute a separate criminal offence (e.g. in case of forgery of documents through which the

perpetrator tried to commit fraud or embezzlement but voluntarily forsake its completion, the court and relevant authority will still consider his/her liability for the actual forgery itself).

### PLANNING AND STRUCTURING INTERNAL INVESTIGATIONS

- ? **How should internal investigations be structured?**  
**When should an internal investigation be conducted by an attorney?**

The company should have an internal regulation in place that governs the process of dealing with (or even the suspicion of) misconduct, including internal investigation procedures as part of the compliance management system. It should specify the persons responsible for dealing with internal investigations (which is usually an independent compliance function) and how the structure of the internal investigation should be decided, including a process for independent reporting.

Whenever there is a risk that a reporting duty has arisen, or will arise during the investigation, or if there is a risk of a police dawn raid, an attorney should be engaged as an external counsel to lead and conduct the investigation to minimize the risk of exposure to the reporting duty, and to maintain legal privilege over investigation products.

### CONFIDENTIALITY AND LEGAL PRIVILEGE

- ? **Who can be protected by attorney-client privilege ("legal privilege")?**  
**Which information/data is and is not protected by legal privilege, and what (if any) are the exceptions from legal privilege?**

Under the relevant FBiH and RS laws, including the Law on Advocacy and Code of Ethics for Attorneys, legal privilege is reserved only for attorneys, i.e. lawyers registered before the competent bar association. Any such information an attorney obtains during a mandate from the client or otherwise, including all documentation, written submissions, as well as audio or video records, constitutes a legal privilege. Even if an attorney does not accept a mandate, such an obligation exists in relation to information which was provided to the attorney by the potential client.

Legal privilege extends to all attorneys in a joint lawyers' office, and to a law firm and all its employees, and is not time-limited. Even after the authorization to represent a client in a certain matter is revoked, or the relevant proceeding is finalized, the obligation still exists because of information becoming known to the attorney in the course of the relevant mandate and/or proceedings.

Under FBiH law, an attorney may disclose facts and circumstances which represent a legal privilege only in certain types of court proceedings (i) upon the written approval of the person who disclosed such information to the attorney; or (ii) if the disclosure of the information is indispensable in criminal proceedings or disciplinary proceedings in order for the attorney to prove his/her innocence. On the other hand, under RS law, the disclosure of such information is possible if it is relevant to the client's defence or necessary to justify a decision on denial of defence in a certain matter.

In addition, in both cases, the obligation of attorneys (to the client) to preserve the confidentiality of all information received when providing legal services is protected by the state in various procedural situations, e.g. an attorney can refuse to testify if this would lead to a breach of the confidentiality obligation.

However, if any attorney-client communications, documents or other forms of information media are seized, intercepted or obtained from the company directly or through third parties, they are not covered by attorney client privilege.

**? Does legal privilege extend to documents created by attorneys after they are handed over to the client?**

No, the confidentiality obligation is tied to the person of the attorney (and his or her employees and subcontractors), rather than to the information or document itself. Therefore, any information or document that is protected when in the possession of the attorney is not protected when it is in the hands of the client or an unrelated third person. Prosecuting authorities often use this to order the company to hand over all documents they have received from the attorney, including reports from the internal investigation and protocols from interviews. Best practice is to structure the investigation with the attorney who is leading the investigation and who subcontracts other third parties who participate in the investigation, should such a participation be necessary.

It is essential that the investigation and its reporting lines/forms are structured so as to minimize the risk that the investigation report is taken by the authorities e.g. during the dawn raid, and then used as evidence in a court proceeding.

**? Does legal privilege apply to in-house lawyers?**

No. In-house lawyers do not enjoy the protection of legal privilege.

These may be obliged to protect a business secret; however, information regarding a breach of law or other legislation cannot be determined as a business secret.

**? Does legal privilege apply to other types of service providers?  
Can legal privilege be extended to them if they are subcontracted by attorneys?**

Legal privilege is extended only in cases stipulated by the applicable Code of Ethics for Attorneys, as indicated above, and it is not extended to service providers. It could be argued that service providers are entitled to the privilege that falls within the client-provider relationship, whereas the special protection of premises (as is the case with legal privilege) does not apply to them. Therefore, all relevant documents should be kept on the premises of the attorney.

There are other types of privileges, but these also fall within the client-provider relationship and do not apply in corporate investigations (e.g. tax advisors' privilege does not prevent tax advisors, upon a written request from the court, from providing any information they have about a company if necessary in an investigation or criminal procedures).

## **COLLECTING AND PROCESSING DATA AND DATA PRIVACY PROTECTION**

**? How should the company ensure that evidence is properly collected?**

The company must determine what data is needed for the internal investigation and where they are. What means of communication are used (emails, apps, phones)? What devices do employees use to communicate? Is there any cloud or local share-drive? Is the cooperation of a local IT expert needed? Is there any paper-only information? It is then essential to determine whether and to what extent the company can legally access and review the data. It is not unusual for employees to use apps that are encrypted or do not save content, and it is then extremely difficult to distinguish between the personal content of their communication from work content. A comprehensive and clear internal directive providing the complete rules on communication, archiving and the use of company devices by employees on the one hand, and explicit information on how the company can review and collect this data on the other, is a cornerstone of any proper internal investigation.

The company should also issue a preservation notice to employees to ensure that potential evidence (and all data relevant to the matter investigated) is preserved and not destroyed. The employees in question should sign for or give confirmation that they are complying with the preservation notice, and this should be kept on the record.

**? What conditions must be met to allow investigators access to employees' emails/other records which potentially contain private information?  
Is the consent of the custodian necessary before data collection begins?**

GDPR is not directly applicable in BiH, with the exception of Article 3 para 2, based on which GDPR could also apply to non-EU companies if certain requirements set out in GDPR are met. It is due to be implemented into BiH legislation via amendments to the BiH Personal Data Protection Law, but it is not certain when such amendments will be adopted and come into force. Until that date, all personal data processing of companies in BiH must be carried out in compliance with the currently-applicable BiH Personal Data Protection Law. The BiH Personal Data Protection Law does not specifically regulate investigations involving employee emails or other records potentially containing private information. Thus, the general rules apply to such matters.

In general, the processing of personal data is considered legal if performed on a valid legal basis, which includes consent, legitimate interest of the controller, public interest requirements, etc. Due to the specific imbalance of power in an employment relationship (especially in terms of obligation to obtain freely-given consent), it may be argued that performing an internal investigation based solely on consent, without another more reliable legal basis, might be problematic.

In that regard, internal investigations must be conducted in such a way that the risks of breaching privacy laws are minimised. This must be assessed on a case-by-case basis since, generally, the greater the harm faced by the employer (e.g. a large-scale corruption scheme), the more intrusive investigative instruments might be considered proportionate.

Thus, when performing corporate investigations, the legitimate interests of the controller should also be considered. In such cases, the investigation and supervision needs to be conducted only when necessary, to the extent and in a way strictly stipulated by the controller's internal actions, as well as in a way that protects the controller's legitimate interests but does not compromise or jeopardize the private and personal life of the data subject, i.e. the employee, which shall be assessed taking into account the circumstances of each particular case. The controller is obliged to carefully review the relevant data during the investigation, but in a way that does not involve any private information about the employee, i.e. to delicately balance its own interests against the interests or fundamental rights of the employees (e.g. the right to a private life and secrecy of communication).

One-off targeted searches of emails/documents using selected key words should not be considered disproportionate if the employer is aiming to protect itself, its property and its reputation by helping to determine if employees might be in breach of their responsibilities. However, only work-related data is allowed to be processed. No private personal data can be subject to review and any processing of private personal data must be immediately stopped.

On the other hand, as part of the obligation towards transparency, the controller should ensure that the respective employees (or potentially other relevant persons, as the case may be) are duly informed about the processing as part of the investigation. Any such informing should be conducted in writing and should include, among other things, the legal basis and purposes of the data processing and the corresponding rights of the employee. If employees had never been informed that their data might be processed for the purposes of harm prevention, for instance, the company would be in breach of this obligation.

**? Are there any restrictions in relation to cross-border transfers of data collected during an investigation?**

Cross-border transfer of data from BiH is, in general, allowed if the third-country or the international organization to which the personal data is being transferred implements adequate safeguards for personal data as set out in

the BiH Personal Data Protection Law. The transfer of personal data to another country that does not provide adequate safeguards as stipulated by the BiH Personal Data Protection Law, may exceptionally be allowed in specific cases stipulated by the law; for example, if the transfer is necessary in the public interest, the disclosure of personal data is necessary to fulfil the contract between the data subject and the controller or the fulfilment of pre-contractual obligations undertaken at the request of the person whose data is being processed, etc. In any case, if there are no valid grounds for transferring personal data to a third country, the controller may request approval from the BiH Agency for Personal Data Protection.

**? What should the company do once the internal investigation is finished?**

Once the internal investigation is finished, the data gathered and processed during the internal investigation must be erased, with only the most important findings stored for the purpose of confronting the employee with the findings or for potential court or administrative proceedings. Employees whose data was processed must be informed of such processing.

## INTERVIEWING EMPLOYEES

**? Does an employee have an obligation to actively participate in interviews organised by the counsel of the employer?  
Is an employee required to participate and cooperate in interviews?**

Any employee instructed by the employer to cooperate during internal investigations could be obliged to do so in accordance with the general obligations arising out of their employment duties. To ensure their legality, interviews should take place within the working hours of employees and should be strictly connected to their work. Refusal to cooperate may be considered a breach of their employment duties, if anticipated as such in an employment agreement or the company's internal acts.

Employees under the suspicion of committing a breach of work duties shall be allowed by the employer to present his/her defence in case of a disciplinary procedure. However, if absent, the employee will miss the opportunity to defend himself/herself before the employer's representatives. Therefore, such an employee does not have an obligation but rather a right to participate in any interviews organised by the employer, especially during a disciplinary procedure, but he/she may decide not to exercise such a right.

**? Do employees have the right to receive minutes from the interview?**

Not specifically regulated. However, as minutes usually do not constitute a decision by which it is decided regarding employee's rights and obligations, it could be argued that employees in principle should not receive minutes from the interview.

**? Do employees have the right to be informed of the outcome of the investigation?**

No, employees do not have to be informed of the outcome of interviews or the investigation, unless they are the subject of such an investigation for breaching work duties and found liable as an outcome of the investigation.



## WHISTLEBLOWING

**? Is there any specific regulation relating to whistleblowers?  
If so, is there any obligation to react to whistleblowing/to have a system in place for reacting to whistleblowing?**

The following laws primarily regulate whistleblowing in BiH:

- BiH Law on Protection of Persons Reporting Corruption in BiH Institutions;
- RS Law on Protection of Persons Reporting Corruption;
- BD Law on Protection of Persons Reporting Corruption.

There are no specific whistleblowing laws adopted in FBiH; however, the draft of the FBiH Law on Protection of Persons Reporting Corruption in FBiH has been prepared by the Government of FBiH in March 2018, but has not yet been adopted.

The BiH Law on Protection of Whistleblowers regulates the protection of whistleblowers in BiH government institutions and companies established by such institutions. It regulates the status of whistleblowers, corruption reporting procedures, obligations of the institutions in relation to reporting of corruption, protection of whistleblowers, and sanctions for breaching the statutory provisions. However, the application of this law is limited, as stated above, and is in general not applicable to companies (unless they are established by BiH institutions). Under the BiH Law on Protection of Whistleblowers, the reporting of corruption may be conducted internally and externally, whereby internal reporting should be regulated by the internal bylaws of the relevant BiH institution or company established by a BiH institution, which are published on the premises and on the website of the institution. A whistleblower may opt to report corruption externally if: (i) the duration of the internal procedure exceeds 15 days; (ii) the whistleblower considers that the internal procedure was not properly conducted; or (iii) the whistleblower believes that the person authorized for collecting reports on corruption, or the head of the institution, may be directly or indirectly involved in the corruption.

The RS Law on Protection of Whistleblowers, *inter alia*, stipulates that all persons can report (in good faith) any kind of corruption in the public or private sector, of which he/she has direct knowledge. In that regard, the RS Law on Protection of Whistleblowers is also applicable to privately-owned companies. The law further provides for (i) the obligation to act upon a report of corruption as a general principle – stipulating that the responsible person is obliged to undertake measures for detection, prevention, suppression and punishment of all kinds of corruption as well as measures for the protection of whistleblowers; and (ii) the urgency principle (*ekonomičnost*) – stipulating that the procedure for the protection of whistleblowers is urgent and should be conducted without delay, in the shortest period necessary to determine all relevant facts. The RS Law on Protection of Whistleblowers provides that a whistleblower may initiate an internal protection procedure if they suffer any harmful effects from reporting corruption. Responsible persons are obliged to decide on such request within 30 days of the day the request is submitted. The law also provides the following obligations of the responsible person to:

- enable the reporting of corruption;
- receive the report on corruption;
- return the report to the whistleblower for amendments if the report does not contain all statutory elements;
- ensure data protection and the anonymity of the whistleblower;
- act upon the report, i.e. work on the detection, prevention, suppression and punishment of corruption, within seven days of the date of receipt of the report;

- without delay undertake activities to eliminate harmful effects to the whistleblower and ensure the protection and rights of the whistleblower;
- undertake measures for the determination of the disciplinary and material liability of persons involved in the corruption;
- notify the whistleblower of the measures and activities undertaken on the basis of his/her report within 15 days of the day of submitting a request for delivery of the subject notification;
- deliver the decision or the notification of the outcome of the procedure to the whistleblower within eight days of the day of conclusion of the procedure;
- forward the report without delay to the competent authorities if there are grounds for criminal liability;
- deliver the report to the RS Ministry of Justice in accordance with the law.

Any person who manages 15 or more employees shall adopt a whistleblowing policy (*uputstvo*), which shall include regulations on the procedure itself, on the whistleblowers' rights, obligations of the responsible person and especially the protection of the whistleblower's anonymity.

The BD Law on Protection of Whistleblowers is harmonized with the BiH Law, but in comparison to the BiH Law on Protection of Whistleblowers, the BD Law is applicable to both public institutions and privately owned companies.

## CRIMINAL PROCEEDINGS AGAINST THE COMPANY

### ? Is there corporate criminal liability in the country?

Yes, a company shall be responsible for any criminal offence committed in the name of, on account of or in favour of the company, (i) when the criminal offence occurs on the conclusion, order or approval of the managerial or supervisory bodies of the company; or (ii) when the managerial or supervisory body has influenced the perpetrator or enabled him/her to commit the criminal offence; or (iii) when the company has been disposing of the illicitly-acquired monetary gain or has been using the items originating from the criminal offence; or (iv) when the managerial or supervisory body failed to act with due care in supervising the legality of its employees' work.

### ? Can individuals and companies both be prosecuted for the same misconduct (parallel prosecution)?

Both the perpetrator and the company can be prosecuted independently. The liability of a company shall not exclude the liability of individuals, i.e. the responsible persons who committed the criminal offence.

### ? Can corporate criminal liability be avoided or mitigated?

There are no applicable regulations that stipulate the possibility for a company to release itself from criminal liability.

A criminal sentence for a company may be mitigated if the managerial or supervisory body voluntarily reports a perpetrator after he/she commits a criminal offence; whereas the company may be exonerated from criminal sentence if (i) its managerial or supervisory body returns the wrongfully acquired monetary gain, or (ii) remedies any adverse consequences of the wrongdoing, or (iii) provides information on other companies' liability.

For criminal offences committed out of negligence, a company may be liable if managerial or supervisory bodies of a legal person fail to carry out due supervision over the legality of employees' work, in which case the criminal sentence for company may be mitigated.

**? Can criminal proceedings be settled with the enforcement authorities, or through leniency programmes?**

There is no practice of out-of-court settlements, particularly if compared to the US settlement practice. Some instruments exist, but only a fraction of cases are resolved out of court. The out-of-court settlement system has essentially been constructed for prosecuting individuals and does not allow for prosecution to be settled without the admission of guilt.

A guilt and sanctions agreement made between the perpetrator and the public prosecutor is the only out-of-court settlement that has been used in practice. The offender must admit to his or her guilt and agree to sanctions that will then have to be confirmed by a court.

## UPCOMING DEVELOPMENTS

Current court practice in terms of prosecuting companies is scarce and mostly based on imposing monetary fines, rarely on seizure of property, or termination of the company. The practice of out-of-court settlements for companies in BiH is existent to none, especially as prosecuting authorities are hesitant to initiate highly complex corporate cases. This especially taking into account that current legislation makes cooperation almost impossible between prosecuting authorities and companies that would wish to cooperate, and with the practical non-existence of settlements.

It should be noted that BiH was identified as a potential candidate for EU membership in June 2003; however, further to the Opinion of the European Commission to the EU Council on the membership application of BiH, one of the key priorities that BiH needs to fulfil in order to be recommended for the opening of EU accession negotiations, is stepping up the process of aligning with EU *acquis* and implementing and enforcing relevant legislation. It can be expected that in the future we will witness the harmonization of BiH legislation with the EU *acquis*, whereas it remains to be seen in which direction shall such harmonization goes, and if and how companies will benefit from it.

*This chapter was written by Lana Sarajlic and Lamis Kulenovic, independent attorneys-at-law in cooperation with Wolf Theiss.*



**LANA SARAJLIC**  
Counsel

**Wolf Theiss**  
**Bosnia & Herzegovina**

T. +387 33 953 452  
[iana.sarajlic@wolftheiss.com](mailto:iana.sarajlic@wolftheiss.com)



**LAMIS KULENOVIC**  
Associate

**Wolf Theiss,**  
**Bosnia & Herzegovina**

T. +387 33 953 459  
[lamis.kulenovic@wolftheiss.com](mailto:lamis.kulenovic@wolftheiss.com)



WOLF THEISS

**BULGARIA**

## KEY TAKEAWAYS

- There is no corporate criminal liability in Bulgaria, but companies may incur administrative liability (i.e. pecuniary sanctions) for the misconduct of their employees, managers, directors and board members.
- Investigating misconduct is included in management's duties towards the company and is a sign of a sound compliance management system.
- The effect of legal privilege is limited to the correspondence between the client and the lawyer.
- Suspicion of bribery may trigger the duty to report information to the authorities.
- Self-reporting or cooperation with prosecuting authorities does not have any automatic benefit for the company.

## OBLIGATION TO INVESTIGATE CRIMINAL MISCONDUCT INTERNALLY

### ? Are companies obliged to investigate misconduct internally?

Under Bulgarian law there is no explicit obligation for companies to investigate internally detected misconduct.

However, some of the largest companies have dedicated internal security structures tasked with such prerogatives, and internal investigations are used as a compliance tool and a tool to limit potential liability of the company (civil and administrative) and of its managers/directors (civil, criminal and administrative).

### ? In which situations will a decision to internally investigate be necessary to prevent the civil or criminal liability of board members?

As to civil liability, the Bulgarian Commercial Act provides that the manager/director of a company may be liable for damages, both for active actions and for omission of oversight. Therefore, an internal investigation may be required in case of reasonable suspicions of a possible wrongdoing in the company, as it could prevent further damages to the company (i.e. represent a mitigation measure) and potential liability for the manager/director. Also, if a manager/director has or receives information of a possible wrongdoing and does not take appropriate mitigation measures (such as an internal investigation), his or her actions could be considered as negligence and may be sufficient grounds for the company to claim civil liability.

Certain types of misconduct may give rise to criminal prosecution against the manager/director of a company and may trigger fines and/or custody. For example, in case of negligence in the exercise of management or supervisory activity, entering into disadvantageous transactions, bribery, bankruptcy, money laundering, tax fraud etc. If a corporate director has a suspicion of criminal wrongdoing but takes no action to stop it, he or she may be held liable for "non-hindering criminal wrongdoing". More complex constructions of co-liability in the form of aiding and abetting also cannot be excluded. In this respect, internal investigations may mitigate the potential liability of the managers/directors to some extent.

Managers/directors may also bear criminal liability if they have not conducted their business with the "*care of a good trader*" and for that reason the company enters insolvency causing harm to creditors. This obligation includes also the obligation to control and manage the employees in the company and to be aware of their actions.

- ? Is there a duty to report the outcome of the internal investigation or any information obtained during the internal investigation to enforcement authorities?  
If so, who is subject to the reporting duty and who is exempt?  
Are companies obliged to self-report?**

There are no general obligations for companies to report the outcome of internal investigations or information obtained during the investigation. Such obligation would be triggered only if there is sufficient evidence that a crime has been committed.

All individuals, and according to legal doctrine – all companies – have a legal obligation to immediately report most of the crimes listed in the Bulgarian Criminal Code. In such a case, the obligation to report applies both to the company and to the individuals which have knowledge of the crime – investigators, managers/directors, employees, etc. This general obligation, however, is rarely sanctioned in practice.

A more subtle aspect is that the knowledge for a potential crime, arising out of an internal investigation, if not reported, could potentially result in suspicions for concealment or complicity with the crime. In practice few such examples have been identified, but in the context of complex business-related crimes, involving multiple individuals, such risk should be considered in each specific case.

- ? Would cooperation and voluntary self-disclosure be taken into account by the law enforcement authorities in relation to both individual and corporate liability?**

Under Bulgarian criminal law, in case of cooperation and voluntary self-disclosure, the punishment of the liable person shall be reduced. Although there are no specific provisions under criminal law providing the possible reductions, in practice prosecutors and courts tend to weigh them significantly in the course of the proceedings. This principle is applicable also in respect of administrative breaches (i.e. not criminal) in case of cooperation by the company. However, there are no guidelines or determining methodology that could be relied upon.

## PLANNING AND STRUCTURING INTERNAL INVESTIGATIONS

- ? How should internal investigations be structured?  
When should an internal investigation be conducted by an attorney?**

As a matter of practicality, it is recommended that the company has in place an internal regulation that governs the process of dealing with (suspicion of) misconduct including internal investigation procedures as part of the compliance management system. It should specify the persons responsible for dealing with internal investigations (usually an independent compliance function) and how the structure of the internal investigation should be decided, including a process for independent reporting.

Whenever there is a risk that a reporting duty may arise during the investigation, or if there is a risk of a police dawn raid, an attorney registered in Bulgaria should be engaged as an external counsel to lead and conduct the investigation to minimize the risk of exposure to the reporting duty, and to maintain legal privilege over investigation products.

## CONFIDENTIALITY AND LEGAL PRIVILEGE

- ? Who can be protected by attorney-client privilege (“legal privilege”)?  
Which information/data is and is not protected by legal privilege, and what (if any) are the exceptions from legal privilege?**

The concept of legal or attorney-client privilege does not exist in the same way as in the US. Legal privilege provided under the Bulgarian Bar’s Act applies to attorney-at-law, attorney-at-law from the European Union, junior

attorney-at-law or attorney-at-law assistant within the meaning of the Bar Act, who has been admitted to the Bar Association.

Irrespective of any investigation, dispute, litigation, inspection etc. lawyers are covered also when they are providing advice not related or arising out of investigations or litigations. This has been consistently applied by civil and criminal courts. However, some administrative authorities (such as the Bulgarian Competition Protection Commission) are more reluctant to apply this provision during their investigations.

Under the legal privilege, any papers, files, electronic documents, and computer equipment held by an attorney-at-law may not be subject to violation, inspection, copying, verification or seizure. Similarly, correspondence between an attorney-at-law and a client may not be subject to inspection, verification or seizure and may not be used as evidence. Meetings and calls between an attorney-at-law and his or her client may not be intercepted and recorded. Any recordings, where available, shall not be used as means of evidence and shall be subject to immediate destruction.

Attorneys-at-law cannot be questioned on their procedural capacity, about meetings, calls and correspondence with clients or other attorneys-at-law as well as with regard to any facts and circumstances of which they become aware in relation to their capacity. When a client is held in custody or deprived of liberty, his or her attorney-at-law has the right to meet him or her privately and their conversation during meetings may not be intercepted or recorded, although meetings may be subject to observation. Moreover, during meetings the attorneys-at-law have the right to hand over and receive written material in relation to the case. According to the Bar Act the contents of such documents may not be subject to inspection; which leads to the conclusion that legal privilege extends to documents created by attorneys after they are handed over to the client, but only in this hypothesis.

### **? Does legal privilege extend to documents created by attorneys after they are handed over to the client?**

No, in principle the confidentiality obligation is tied to the person of the attorney (and his or her employees and subcontractors), rather than to the information or document itself. Therefore, any information or document that is protected when in the possession of the attorney is not protected when it is in the hands of the client or an unrelated third person.

The legal privilege would extend to the correspondence, including electronic correspondence, between the client and the lawyer. The question of whether "correspondence" implies all documents exchanged (e.g. such as an internal investigation reports) and other lawyer's products, if included in the correspondence, is yet untested. However, documents which are a product of the lawyer's work and have been sent to the client should fall within the term "correspondence" and thus be included in the scope of legal privilege.

### **? Does legal privilege apply to in-house lawyers?**

No. In general, in-house counsel have the status of regular employees and don't enjoy legal privilege.

It is possible for an attorney to work as an in-house lawyer, but he/she must have been admitted to the Bar Association for the legal privilege provisions to apply to him or her. In-house lawyers which are not admitted to the Bar are not covered by the provisions in respect of legal privilege.

### **? Does legal privilege apply to other types of service providers? Can legal privilege be extended to them if they are subcontracted by attorneys?**

Legal privilege does not apply to other persons or entities. Even if works are subcontracted to them by lawyers, legal privilege cannot be extended.



## COLLECTING AND PROCESSING DATA AND DATA PRIVACY PROTECTION

### ? How should the company ensure that evidence is properly collected?

The company must determine what data are needed for the internal investigation and where they are. What means of communication are used (emails, apps, phones)? What devices do employees use to communicate? Is there any cloud or local share-drive? Is the cooperation of a local IT expert needed? Is there any solely-paper information? It is then essential to determine whether and to what extent the company can legally access and review the data. It is not unusual for employees to use apps that are encrypted or do not save content, and it is then very difficult to distinguish between the personal content of their communication from work content. A comprehensive and clear internal regulations providing the complete rules on communication, archiving and the use of company devices by employees on the one hand, and explicit information on how the company can review and collect these data on the other, is a cornerstone of any proper internal investigation.

The company should also issue a preservation notice to employees to ensure that potential evidence (and all data relevant for the matter investigated) is preserved and not destroyed. The employees in question should sign or give confirmation that they are complying with the preservation notice, and this should be kept on the record.

### ? What conditions must be met to allow investigators access to employees' emails/other records which potentially contain private information? Is the consent of the custodian necessary before data collection begins?

Personal data processing in Bulgaria is subject to the GDPR. The law implementing the GDPR in Bulgaria explicitly regulates certain matters relating to the processing of personal data in the context of employment relationships. Among others, employers should adopt rules and procedures where systems are in place to report breaches and restrict use of internal company resources (e.g. emails, laptops, etc.). These rules must be communicated to the employees.

Employees have clear and specific rights to privacy in the workplace, recognized under Bulgarian law, but these rights are balanced with certain entitlements of the employer in the course of its business operations. Without the explicit consent of the employee the employer only has the right to review the business-related correspondence, messages, etc. of the employee. The employer has no right to check the personal emails of the employee. Any private correspondence is protected under the Bulgarian Constitution and any access or disclosure without the explicit consent of the employee, could be subject to criminal liability. As an exception to this rule, the protection of private correspondence may be waived only by court order for the purposes of detection and prevention of serious crimes.

The employer should make clear in the internal company rules whether employees are entitled to use the company's email for personal use.

- if yes, the employer needs the explicit consent of the employee for access, processing and disclosure of their correspondence (as the employer would not be able to differentiate between professional and personal correspondence before accessing the email);
- if no, i.e. if all use for personal purposes is strictly forbidden and only professional correspondence is allowed, then the employer may process such correspondence without the consent of the employee, if employees have been informed that personal use is prohibited, and as long as the extent of the review is proportionate.

**? Are there any restrictions in relation to cross-border transfers of data collected during an investigation?**

In case of an envisaged transfer of data to countries outside the EU/EEA, for which an adequate level of data protection has not been determined (e.g. USA), additional guarantees are required, e.g. the conclusion of the EU Standard Contractual Clauses.

**? What should the company do once the internal investigation is finished?**

Once the internal investigation is finished, the data gathered and processed during the internal investigation must be erased, with only the most important findings stored for the purpose of confronting the employee with the findings or for potential court or administrative proceedings. Employees whose data were processed must be informed of such processing.

## **INTERVIEWING EMPLOYEES**

**? Does an employee have an obligation to actively participate in interviews organised by the counsel of the employer?  
Is an employee required to participate and cooperate in interviews?**

An employee has an obligation to actively participate in the interviews organised by the counsel of the employer if this obligation exists in his or her employment agreement as part of the job description or if it is included as part of the internal rules or the interior labour regulations adopted in the enterprise. Otherwise, the employee is required to participate in such interviews only in case of a lawful instruction issued by the employer.

**? Do employees have the right to receive minutes from the interview?**

No.

**? Do employees have the right to be informed of the outcome of the investigation?**

No.

## **WHISTLEBLOWING**

**? Is there any specific regulation relating to whistleblowers?  
If so, is there any obligation to react to whistleblowing/to have a system in place for reacting to whistleblowing?**

Currently, no. There is no specific regulation related to whistleblowing in Bulgaria, nor any formal legal definition of whistleblowing. Bulgarian courts do not acknowledge specific rights of whistle blowers.

Current legislation provides for few specific examples where the rights of an employee are protected. For example, the Bulgarian Labour Code provides that submitting a report to the Financial Supervision Commission for breaches by an employer of certain financial services laws, the social security code and others, shall not constitute a breach of work discipline in the form of abuse of the confidence and damage of the reputation of the business, nor a disclosure of confidential information, unless the employee deliberately communicates false information.

The Bulgarian Anticorruption Act (Counter-Corruption and Unlawfully Acquired Assets Forfeiture Act) provides that any citizen who has any evidence of corruption or conflict of interest regarding defined public officer may report this to the Anticorruption Commission. The Commission has an obligation to undertake specific measures to keep the identity of the citizen confidential, including measures to prevent any psychological or physical pressure over him or her. Specific measures to preserve a witness are also provided in criminal proceedings but not in civil or commercial proceedings.

However, a whistleblower protection bill, implementing the EU Directive in the same matter, is being prepared by the Bulgarian Ministry of Justice and should come into effect in December 2021. We do not expect the bill to vary from the EU Directive, which expresses a preference for employers to maintain whistleblowing hotlines (either through a designated employee or a third party), with it proposed that all employers with more than 50 employees should be required to set up such a hotline. The hotline must be easily accessible and the procedure clear and understandable. All reports must be confidential, protected, and diligently and impartially analysed, and the whistleblower must be notified that its report is being processed and informed of its outcome.

## **CRIMINAL PROCEEDINGS AGAINST THE COMPANY**

### **? Is there corporate criminal liability in the country?**

There is no corporate criminal liability in Bulgaria. Only natural persons may be held criminally liable. Companies may be subject to administrative sanctions for some types of breaches, but not criminal liability.

### **? Can individuals and companies both be prosecuted for the same misconduct (parallel prosecution)?**

No, only individuals may be prosecuted.

### **? Can corporate criminal liability be avoided or mitigated?**

N/A.

### **? Can criminal proceedings be settled with the enforcement authorities, or through leniency programmes?**

The settlement of criminal proceedings under Bulgarian law is significantly different, compared to the US settlement practice.

In the course of criminal proceedings against individuals, voluntarily settlements may be achieved either at the investigation stage (i.e. prior to the initiation of the court case), or during the initial phase of the court procedure. In both cases, the law does not allow for prosecution to be settled without the admission of guilt. The offender must admit to his or her guilt and agree to sanctions that will then have to be confirmed by a court.

Leniency programs do not exist under Bulgarian Criminal law, but only in the context of competition proceedings.

## **UPCOMING DEVELOPMENTS**

Notwithstanding that criminal liability for companies does not exist under Bulgarian law, corporate investigations remain an essential tool for companies to ensure prompt compliance and to mitigate potential damages. Respectively, managers/directors may benefit from internal investigation to promptly react and limit potential criminal liability.

With the adoption of the whistleblowers legislation, expected for December 2021, we would expect a gradual increase in situations prompting or requiring an internal investigation in Bulgarian companies.

*This chapter was written by Anna Rizova-Clegg and Oleg Temnikov.*



**ANNA RIZOVA-CLEGG**  
Partner

**Wolf Theiss, Bulgaria**

T. +359 2 8613 703  
[anna.rizova@wolftheiss.com](mailto:anna.rizova@wolftheiss.com)



**OLEG TEMNIKOV**  
Counsel

**Wolf Theiss, Bulgaria**

T. +359 2 8613 732  
[oleg.temnikov@wolftheiss.com](mailto:oleg.temnikov@wolftheiss.com)



# CROATIA

## KEY TAKEAWAYS

- Criminal liability for misconduct of employees and board members could be extended to companies.
- Management's fiduciary duties are to implement a compliance management system and if required to conduct internal investigations.
- Processing employees' data requires prior authorisation and is crucial for a lawful and proper internal investigation.
- Legal privilege is limited to attorneys but can be effectively utilised for a broad range of service providers in internal investigations.
- Self-reporting and cooperation with prosecuting authorities may be beneficial for the company.

## OBLIGATION TO INVESTIGATE CRIMINAL MISCONDUCT INTERNALLY

### ? Are companies obliged to investigate misconduct internally?

There is no express obligation imposed on companies to investigate detected misconduct. However, diligently investigating misconduct as part of a compliance management system could help the company to be released from its criminal liability, if detected and reported.

### ? In which situations will a decision to internally investigate be necessary to prevent the civil or criminal liability of board members?

With regard to civil liability, corporate directors have an obligation to ensure that the corporation behaves in compliance with all relevant regulations as a part of corporate director's general fiduciary duty. Whenever a corporate director has a reasonable suspicion of a possible wrongdoing in the corporation, he or she must initiate appropriate steps to confirm (or dissipate) it, and to prevent further damage and wrongdoing with the appropriate actions. An internal investigation will often be such an appropriate step. In such cases, failure to conduct an internal investigation would represent a breach of the corporate director's fiduciary duties and he or she could thus be liable for any prejudice to the corporation (e.g. penal or administrative fines, damages to be paid to third persons, loss of further profits etc.) that could have been prevented, had the wrongdoing been discovered in time.

Furthermore, under the Whistleblowing Act, the board has a strict obligation to set up a system for reporting wrongdoings. The board's failure to do so, let alone any board's interference with an internal investigation, may lead to a fine up to EUR 7,000 for the company and EUR 4,000 for the directors.

On the other hand, with regard to the criminal liability of directors, failure to investigate any potential wrongdoing should not automatically result in criminal liability. This particularly relates to offences which could not be affected or prevented by the management board's action. However, should the omission to investigate a wrongdoing be intentional and potentially aimed towards assisting the perpetrator, board members could be found criminally liable in certain circumstances. More generally, if a director has a firm suspicion of a serious criminal wrongdoing (e.g. corruption, money laundering, serious fraud) and does nothing about it, he or she may themselves be held liable for "non-hindering criminal wrongdoing".

- ? Is there a duty to report the outcome of the internal investigation or any information obtained during the internal investigation to enforcement authorities?  
If so, who is subject to the reporting duty and who is exempt?  
Are companies obliged to self-report?**

There is a general obligation under the Criminal Code to report a crime. The obligation is also imposed on companies. Only attorneys, who learn about this information when providing legal services (i.e. conducting investigations), are exempted from this reporting duty.

However, companies should not be scrutinized by the reporting duty, as the right not to self-incriminate should apply to companies as well. Furthermore, individuals who can represent the company (i.e. corporate directors) should not be forced to report or testify against the company as this would represent evasion of the right to not self-incriminate. Nevertheless, company employees who would be obliged to report crimes or have been conducting the investigation most likely would not be covered by the said right and might be obliged to report the crime.

- ? Would cooperation and voluntary self-disclosure be taken into account by the law enforcement authorities in relation to both individual and corporate liability?**

Cooperation and voluntary self-disclosure should always be considered at least as a mitigating circumstance (i.e. leading to a smaller sanction). In some cases, voluntary self-disclosure may lead to a substantial reduction or even immunity from sanctions. Companies which disclose the criminal offense before the criminal offense is identified by the authority, may be granted immunity from the fine.

## PLANNING AND STRUCTURING INTERNAL INVESTIGATIONS

- ? How should internal investigations be structured?  
When should an internal investigation be conducted by an attorney?**

Internal rules that govern the process of dealing with wrongdoing and the subsequent internal investigation are highly recommended. The rules should envisage the persons in charge of the internal investigation and the framework of their work, spanning from the suspicion of wrongdoing to independent reporting. Furthermore, the rules should foresee an early involvement of attorneys (if there is a possibility that a reporting obligation may arise) and potential service providers, such as forensic or accounting professionals. In practice the attorney usually subcontracts forensic or accounting professionals so that the risk of exposure is minimized, and legal privilege is maintained inside the company.

## CONFIDENTIALITY AND LEGAL PRIVILEGE

- ? Who can be protected by attorney-client privilege ("legal privilege")?  
Which information/data is and is not protected by legal privilege, and  
what (if any) are the exceptions from legal privilege?**

"Legal privilege" under Croatian law is construed as being the attorneys' obligation (to the client) to preserve confidentiality of all information received when providing legal services. This is respected by the State in various procedural situations: e.g. if an attorney is interviewed by an authority or invited to testify, the testimony can be refused if this would lead to a breach of the confidentiality obligation.

The same principle is applied to the obligation of delivery of documents or their seizure. To ensure it, a special proceeding is applied when attorneys' premises are searched: a Bar representative must be present and documents can only be seized if this representative attests that they are not covered by legal privilege. "Legal privilege" covers, therefore, any information/data received when providing a legal service, regardless of whether



this is received from the client or from third persons. A stronger privilege covers legal services provided within the frame of defence in criminal proceedings: in those cases even any communication between the attorney and the client is protected.

**? Does legal privilege extend to documents created by attorneys after they are handed over to the client?**

The privilege is associated with the attorney, who is registered with the Bar, as an individual (including attorney's employees and subcontractors) and not to the information or document itself. Therefore, the information or document which is protected by legal privilege when kept by the attorney is not protected by the privilege if found in the hands of the client or an unrelated third person.

**? Does legal privilege apply to in-house lawyers?**

In-house lawyers do not enjoy any privilege under Croatian law. Legal privilege applies to professional attorneys and therefore cannot be applied to in-house lawyers or counsels.

**? Does legal privilege apply to other types of service providers?  
Can legal privilege be extended to them if they are subcontracted by attorneys?**

Although other types of privileges exist (e.g. tax advisors' privilege), they do not have the same reach and effect as the attorneys' privilege. All such privileges fall within the client-provider relationship when providing regulated services. However, corporate investigations cannot be fully subsumed by any other type of regulated services other than legal services. As noted above, "legal privilege" covers not only the attorney personally, but also any other person used by the attorney for providing various type of services during the investigation. This means that if other service providers (such as forensic or accountancy experts) are sub-contracted by the attorney in direct connection with a specific legal service, they should be covered by legal privilege to the same extent as the attorney. However, the special protection of premises does not apply to them. In practice, all relevant documents are usually kept in the attorney's premises.

## **COLLECTING AND PROCESSING DATA AND DATA PRIVACY PROTECTION**

**? How should the company ensure that evidence is properly collected?**

The company should establish which data is required for the internal investigation, and once the data is recognized it must be located. The location of the needed data may be on printed paper or stored on various communication tools (emails, apps, phones), devices employees use, cloud or local share-drives (which may all require IT-related knowledge). Employees may use encrypted apps and it is very difficult to distinguish between the personal data from their work content. For a lawful and proper internal investigation, companies' rules should include a directive that regulates the employees' communication, archiving thereof and the use of company devices, and conditions under which the company can review and collect these data if required. In addition, a preservation notice should be signed (or confirmed) by the employees, which would ensure that potential evidence is preserved and not destroyed if required.

**? What conditions must be met to allow investigators access to employees' emails/other records which potentially contain private information?  
Is the consent of the custodian necessary before data collection begins?**

Any personal data processing may only take place on one of the lawful grounds specified by the GDPR. In particular, processing of employees' personal data within an internal investigation may only be based on the

legitimate interests of the controller. However, the controller must perform a delicate balancing of legitimate interests against the interests or fundamental rights of the employees (e.g. the right to private life and secrecy of communication). This balancing exercise should be well-documented. Furthermore, the extent of the processing must be strictly necessary to achieve the aim of the investigation and there should be no less invasive measures available. Data included in the investigation should be carefully selected prior to their review and no private information should be accessed within the investigation. The set-up of the correct key words and adequate training of the reviewers is essential here.

Employees should also be informed that their personal data may be processed within the investigation. The privacy notice must include, among others, the legal basis for the data processing, its purpose and the employees' corresponding rights. Reliance on employees' consent during an investigation might be problematic. The GDPR requires that consent is freely given. According to the EU Data Protection Working Party, employees are almost never in a position to freely give consent, given their dependent position. Also, processing of employees' personal data by using applications or tracking systems is subject to the data protection impact assessment and under the eye of the Croatian data protection regulator AZOP.

**? Are there any restrictions in relation to cross-border transfers of data collected during an investigation?**

Cross-border transfer of data collected during an investigation outside the EU is subject to strict requirements. In particular, companies must ensure that the data will be adequately protected even after their transfer to a third country. Available instruments include binding corporate rules and standard data protection clauses adopted by the Commission.

**? What should the company do once the internal investigation is finished?**

Under the GDPR all the internal investigation collected data must be erased when the internal investigation is finished. Only the most important findings can be stored for eventual internal, court or administrative proceedings. Employees whose data were processed must be informed of such processing.

## INTERVIEWING EMPLOYEES

**? Does an employee have an obligation to actively participate in interviews organised by the counsel of the employer?  
Is an employee required to participate and cooperate in interviews?**

An employee should participate and cooperate in interviews. This obligation can be inferred from the general obligation of all employees to prevent damage and, in the case of managing employees, also from their obligation to "ensure compliance with legal and internal regulations".

**? Do employees have the right to receive minutes from the interview?**

There is no obligation to provide the employees with the minutes from the interview.

**? Do employees have the right to be informed of the outcome of the investigation?**

There is no obligation to inform the employees of the outcome of interviews or the investigation.

## **WHISTLEBLOWING**

- ? Is there any specific regulation relating to whistleblowers?  
If so, is there any obligation to react to whistleblowing/to have a system in place for reacting to whistleblowing?**

The Whistleblowing Act came into force on 1 July 2019. The Act regulates that corporations and employers (with a certain number of employees) in general have an obligation to establish a procedure for reporting a potential wrongdoing and to appoint an internal officer responsible for receiving such reports. If confronted with plausible information from a whistleblower, the responsible officer has an obligation to initiate appropriate analysis – and eventually investigation – of the situation as part of his or her duties.

## **CRIMINAL PROCEEDINGS AGAINST THE COMPANY**

- ? Is there corporate criminal liability in the country?**

Yes, there is a strict corporate criminal liability in Croatia. Companies may be held criminally liable for actions of the company's officers entrusted with business responsibilities. As a part of mitigating circumstances, a company may avoid criminal liability if it has implemented and applied adequate procedures for the early detection and reporting of such a crime committed by persons whose actions are attributed to the company.

- ? Can individuals and companies both be prosecuted for the same misconduct (parallel prosecution)?**

Yes. Both the company and the individual perpetrator may be prosecuted for the same misconduct.

- ? Can corporate criminal liability be avoided or mitigated?**

In accordance with the Act on Criminal Liability of Legal Entities, companies which disclose the criminal offense but before the criminal offense is identified by the public, may be granted immunity from the fine. Furthermore, possible liability could be mitigated if adequate measures that could have prevented a crime from being committed (in practice referred to as the "compliance management system") were in place.

- ? Can criminal proceedings be settled with the enforcement authorities, or through leniency programmes?**

There is no available case law on out-of-court settlements regarding companies' criminal liability. In general, the out-of-court settlement has been designed for natural persons and it must include the admission of guilt. Some leniency policies exist that are not directly connected to criminal liability but rather orientated to certain other offences, such as competition offences.

The instrument of the out of court settlement would be an agreement on guilt and sanctions made between the perpetrator and the public prosecutor. However, it is not widely used. Besides the criminal fine, there are other sanctions that may be imposed by the court, like measures banning the company of certain commercial activities, participating in public tenders or from receiving subsidies.

## UPCOMING DEVELOPMENTS

There is a major increase of activities taken by the Croatian authorities in the past few years relating to the investigations of the corporate criminal liability. A number of criminal procedures were initiated regarding the internal corporate wrongdoings (such as false accounting representation) or regarding the bribe allegations (usually in public tenders for the purpose of various privileges through the abuse of official position and power). Such cases usually come with an extreme reputational risk for the companies as the cases often have political implications and therefore are widely covered in media. The establishment of internal corporate investigation policies and procedures have never been in the focus of the companies on the Croatian market, but a change in the approach is imminent as it becomes more and more obvious that the compliance and good internal practices will become one of the most important future aspects in terms of liability and reputation.

*This chapter was written by Dalibor Valincic, Josip Martinic and Benjamin Sadric in cooperation with Wolf Theiss.*



**DALIBOR VALINCIC**  
Partner

**Wolf Theiss, Croatia**

+385 1 4925 460  
[dalibor.valincic@wolftheiss.com](mailto:dalibor.valincic@wolftheiss.com)



**JOSIP MARTINIC**  
Senior Associate

**Wolf Theiss, Croatia**

+385 1 4925 439  
[josip.martinic@wolftheiss.com](mailto:josip.martinic@wolftheiss.com)



**BENJAMIN SADRIC**  
Associate

**Wolf Theiss, Croatia**

+385 1 4925 469  
[benjamin.sadric@wolftheiss.com](mailto:benjamin.sadric@wolftheiss.com)



# CZECH REPUBLIC

## KEY TAKEAWAYS

- Companies may be criminally liable for the misconduct of their employees and board members.
- Investigating misconduct is included in management's fiduciary duties and is a sign of a sound compliance management system.
- Internal directives regulating the processing of employee data and the investigation of misconduct are cornerstones of a proper investigation.
- The concept of legal privilege is limited to the obligation of registered attorneys to preserve the confidentiality of information received from their clients.
- Suspicion of bribery may trigger the duty to report information to the authorities.
- Self-reporting or cooperation with prosecuting authorities does not have any automatic benefit for the company.

## OBLIGATION TO INVESTIGATE CRIMINAL MISCONDUCT INTERNALLY

### ? Are companies obliged to investigate misconduct internally?

The law does not explicitly require this. However, diligently investigating misconduct is a fundamental part of any effective compliance management system if the company strives to avoid criminal liability. Even if the misconduct did not relate to the crime actually committed, the prosecuting authorities will nevertheless assess the company's compliance management system in terms of its general approach to dealing with misconduct. Since 2016, companies can avoid criminal liability if they can demonstrate that they have implemented adequate measures which were able to prevent the crime from being committed – but unfortunately did not work this one time ("compliance defence").

### ? In which situations will a decision to internally investigate be necessary to prevent the civil or criminal liability of board members?

The fiduciary duties of corporate board members include ensuring and monitoring that the company acts in compliance with all relevant regulations and that they exercise their duties with ordinary care. This means that the board members must not only implement appropriate procedures to prevent misconduct, but also investigate any detected misconduct, which often includes an internal investigation. If a board member who is under strong suspicion of misconduct does not ensure that the suspicion is diligently investigated and that any confirmed misconduct is properly handled, then he or she risks liability for an intentional "breach of fiduciary duties". Moreover, if the suspicion of misconduct entails criminal wrongdoing, then he or she may be held liable for "failing to hinder criminal wrongdoing" or may even be held liable for aiding and abetting the crime as well.

In such cases, failing to conduct an internal investigation would mean a breach of the fiduciary duties of the board members, which would make them liable for any damage to the company (e.g. penal or administrative fines, damages to third persons, loss of further profits, etc.) that could have been prevented.

- ? **Is there a duty to report the outcome of the internal investigation or any information obtained during the internal investigation to enforcement authorities?  
If so, who is subject to the reporting duty and who is exempt?  
Are companies obliged to self-report?**

All individuals and companies have a legal obligation to immediately report (or stop from happening) a number of crimes listed in the Czech Criminal Code. Aside from the most serious crimes, the reporting duty also applies to crimes for which there is a strong public interest in tackling, such as crimes relating to bribery. Attorneys are exempted.

Any person who credibly acquires knowledge that such a crime has been committed or is being committed and fails to report or stop it without delay is committing a crime him/herself. However, the knowledge must be acquired in a credible manner. How this is assessed will depend on the situation: the credibility of the source, the circumstances and conditions, and the form and content of the information. This often means that the company can investigate the matter to the extent necessary before reporting the crime(s) to the authorities, but it should report it immediately *once the suspicion is confirmed*. By reporting the crime however, the company could be exposing itself to criminal prosecution for the crime itself. The company can claim that it is not subject to the reporting duty because, by reporting the crime, it would be incriminating itself. Similarly, individuals who can represent the company (i.e. members of its executive body) should not be forced to report or testify against the company, as this would represent a circumvention of the right to not self-incriminate.

However, the right to not self-incriminate will most likely not apply to company employees who would be personally obliged to report crimes even in situations where they would be the ones investigating them internally. Companies should therefore consider this carefully when planning the structure of their internal investigations.

- ? **Would cooperation and voluntary self-disclosure be taken into account by the law enforcement authorities in relation to both individual and corporate liability?**

The public prosecutor can decide that a company has released itself from criminal liability because it implemented adequate measures which were able to prevent the crime from being committed (compliance management system), and its willingness to cooperate with the prosecuting authorities is a sign that this is in place. Also, a judge can consider self-disclosure and cooperation as mitigating circumstances during court proceedings. However, there is no automatic benefit for self-disclosure or cooperation, and companies are not incentivised by the law to self-report and cooperate with prosecuting authorities, nor can they be certain about any benefits should they decide to cooperate, share information or report misconduct.

## PLANNING AND STRUCTURING INTERNAL INVESTIGATIONS

- ? **How should internal investigations be structured?  
When should an internal investigation be conducted by an attorney?**

The company should have an internal regulation in place that governs the process of dealing with (the suspicion of) misconduct, including internal investigation procedures as part of the compliance management system. It should specify the persons responsible for dealing with internal investigations (usually an independent compliance function) and how the structure of the internal investigation should be decided, including a process for independent reporting.

Whenever there is a risk that a reporting duty has arisen, or will arise during the investigation, or if there is a risk of a policies dawn raid, an attorney should be appointed as an external counsel to lead and conduct the investigation to minimise the risk of exposure to the reporting duty, and to maintain legal privilege over products of the investigation. If further advice is needed from specific service providers such as forensic or accounting professionals, they should be subcontracted directly by the attorney and report directly to him or her, so that the risk of exposure is minimised, and legal privilege is maintained.



## **CONFIDENTIALITY AND LEGAL PRIVILEGE**

- ? Who can be protected by attorney-client privilege ("legal privilege")? Which information/data is and is not protected by legal privilege, and what (if any) are the exceptions from legal privilege?**

The concept of legal or attorney-client privilege does not exist in the same way as in the US. Instead, attorneys have a confidentiality obligation based upon the constitutional rights to a fair trial. "Attorney" means a lawyer registered with the Czech Bar Association in accordance with Czech law or a European attorney in accordance with EU Law. This obligation requires attorneys to preserve all information received from their client when providing legal services. This not only includes information known by the attorney, but also information in material format (paper documents, data files or data disks) which the attorney received in relation to his or her mandate. All material information is protected if located on the premises of the attorney (interpreted by courts as all places where the attorney works, including his or her home or car, and the law firm's data clouds).

- ? Does legal privilege extend to documents created by attorneys after they are handed over to the client?**

No. The confidentiality obligation is tied to the attorney (and his or her employees and subcontractors), rather than to the information or document itself. Therefore, any information or document that is protected when in the possession of the attorney is not protected when it is in the hands of the client or an unrelated third person. Prosecuting authorities often use this to order the company to handover all documents they have received from the attorney including reports from the internal investigation and protocols from interviews. Best practice is to structure the investigation with the attorney who is leading the investigation and who subcontracts other third parties who participate in the investigation if such participation is necessary.

It is essential that the investigation and its reporting lines/forms are structured so as to minimise the risk that the investigation report is taken by the authorities e.g. during a dawn raid, and then used as evidence in court proceedings.

- ? Does legal privilege apply to in-house lawyers?**

No. In-house counsel are not regarded as attorneys under Czech law. They have the status of regular employees and do not enjoy legal privilege.

- ? Does legal privilege apply to other types of service providers? Can legal privilege be extended to them if they are subcontracted by attorneys?**

Service providers (such as forensic or accounting professionals) can invoke legal privilege to the same extent as the attorney but only if they are subcontracted by the attorney in direct connection with provision of the legal services. However, the special protection of premises does not apply to them. Therefore, all relevant documents should be kept on the premises of the attorney. .

## **COLLECTING AND PROCESSING DATA AND DATA PRIVACY PROTECTION**

- ? How should the company ensure that evidence is properly collected?**

The company must determine what data are needed for the internal investigation and where they are located. Which means of communication are used (email, apps, phones)? What devices do employees use to communicate? Is there any cloud or local share-drive? Is the cooperation of a local IT expert needed? Is there any information that is only located on hard copies, i.e. paper documents? It is then essential to determine whether and to what extent the company can legally access and review the data. It is not unusual for employees to use apps that

are encrypted or do not save content, and it is then highly difficult to distinguish between the personal content of their communication and work content. A comprehensive and clear internal directive providing the complete rules on communication, archiving and the use of company devices by employees on the one hand, and explicit information on how the company can review and collect these data on the other, is a cornerstone of any proper internal investigation.

The company should also issue a preservation notice to employees to ensure that potential evidence (and all data relevant for the matter investigated) is preserved and not destroyed. The employees in question should sign or give confirmation that they are complying with the preservation notice, and this should be kept on the record.

**? What conditions must be met to allow investigators access to employees' emails/other records which potentially contain private information?  
Is the consent of the custodian necessary before data collection begins?**

Employee privacy is protected both by Czech labour law and by EU law (in particular GDPR).

Internal investigations must be conducted in such a way that the risks of breaching privacy laws are minimised. This must be assessed on a case-by-case basis since, generally, the greater the harm faced by the employer (e.g. large-scale corruption scheme), the more that intrusive investigative methods might be considered proportional.

One-off targeted searches of emails/documents using carefully selected key words are unlikely to be considered disproportionate if the employer is aiming to protect itself, its property and its reputation by helping to determine if employees may be in breach of their responsibilities. However, only work-related data may be processed. No private personal data can be subject to review, and any processing of private personal data must be immediately stopped if it has begun.

The processing of employee data can only take place on one of the lawful grounds specified by the GDPR. In internal investigations, the most frequently used legal ground is the legitimate interest of the employer. However, the employer must delicately balance its own interests against the interests or the fundamental rights of employees (e.g. the right to a private life and the privacy of communication) as part of a legitimate interest assessment – "LIA"). This balancing exercise should be properly documented in the form of a balancing test. Every balancing test should include at least the information regarding the purpose of the data processing, the necessity of the data processing, potential consequences of the data processing – impact on data subjects, protective measures adopted, and the outcome of the assessment.

A privacy impact assessment (PIA) is explicitly required under the GDPR if the type of processing is likely to pose a high risk to the privacy of natural persons (such as employees). A PIA must be performed in particular if the processing involves processing sensitive information, the merging or combining of data which was gathered by various processes, or occurs systematically over a longer time-period and may cause decisions about data subjects which have a significant effect on their lives (such as legal decisions). It must always be assessed whether a PIA must be executed for purposes of the internal investigation.

The extent of the processing must be as strictly necessary to achieve the aim of the investigation, and there must not be less invasive measures available. The information included in the investigation should be carefully selected prior to review and no private information should be accessed as part of the investigation. It is essential that the right key words are selected, and the reviewers are sufficiently trained.

An internal directive should inform employees that their data may be processed as part of any investigation. This must include, among other things, the legal basis and purposes of the data processing and the corresponding rights of the employee. If employees were never informed that their data might be processed for the purposes of harm prevention, for instance, the company would be in breach of this obligation. Requiring the consent of employees for their data processing during an investigation is not recommended, as the consent must be freely given and can be withdrawn at any time.

**? Are there any restrictions in relation to cross-border transfers of data collected during an investigation?**

Strict conditions apply to cross-border transfers of data collected during investigations to locations outside of the EU. In particular, companies must ensure that the data will be adequately protected even after their transfer to a third country. Available instruments include binding corporate rules and standard data protection clauses adopted by the European Commission. In addition, where the data are transferred within the group companies, the relevant intra-group policies should also be in place.

**? What should the company do once the internal investigation is finished?**

Once the internal investigation is finished, the data gathered and processed during the internal investigation must be erased, with only the most important findings stored for the purpose of confronting the employee with the findings or for potential court or administrative proceedings. Employees whose data were processed must be informed of such processing.

## **INTERVIEWING EMPLOYEES**

**? Does an employee have an obligation to actively participate in interviews organised by the counsel of the employer?  
Is an employee required to participate and cooperate in interviews?**

Employees instructed by the employer to cooperate during internal investigations must do so in accordance with their general obligations arising out of their employment duties (general obligation to prevent damage to their employer and loyalty obligation). To ensure their legality, interviews should take place within the working hours of employees and should be strictly connected to their work. Refusal to cooperate may be considered a breach of their employment duties.

**? Do employees have the right to receive minutes from the interview?**

No.

**? Do employees have the right to be informed of the outcome of the investigation?**

No, employees do not have to be informed of the outcome of interviews or the investigation.

## **WHISTLEBLOWING**

**? Is there any specific regulation relating to whistleblowers?  
If so, is there any obligation to react to whistleblowing/to have a system in place for reacting to whistleblowing?**

Currently, no. There is no comprehensive law on whistleblowing and the courts do not acknowledge the rights of whistleblowers as such. However, if confronted with plausible information from a "whistleblower", any member of an executive or supervisory board of a corporation) has the obligation to initiate an appropriate analysis – and investigation where appropriate - of the situation as part of his or her general fiduciary duties as described above under "Obligations".

A whistleblower protection bill, implementing the EU Directive in the same matter, is being prepared by the Czech Ministry of Justice and should come into effect in December 2021. Heated debate currently surrounds the specific

provisions of this bill. Nevertheless, we do not expect the bill to vary from the EU Directive, which expresses a preference for employers to maintain whistleblowing hotlines (either through a designated employee or a third party), with it proposed that all employers with more than 50 employees should be required to set up such a hotline. The hotline must be easily accessible and the procedure clear and understandable. All reports must be confidential, protected, and diligently and impartially analysed, and the whistleblower must be notified that its report is being processed and informed of its outcome.

## CRIMINAL PROCEEDINGS AGAINST THE COMPANY

### ? Is there corporate criminal liability in the country?

Yes. A company is liable for a crime if the crime was committed by any of a broad range of personnel listed in the (managers, employees, board members, shadow directors, etc.) in the company's interest or in the course of the company's commercial operation. Strict corporate criminal liability exists, which means that a company's criminal liability depends solely on the actions and intention of the perpetrator, all the while remaining independent from and concurrent with the criminal liability of the perpetrator.

### ? Can individuals and companies both be prosecuted for the same misconduct (parallel prosecution)?

Both the perpetrator and the company can be prosecuted independently, and the company may be prosecuted (albeit rarely) even if the perpetrator is acquitted. Criminal liability of the company passes to any successor or successors.

### ? Can corporate criminal liability be avoided or mitigated?

In accordance with the Act on Criminal Liability of Legal Persons and Proceedings Against Them<sup>1</sup>, a company can release itself from criminal liability if it has implemented adequate measures that could have prevented a crime from being committed (in practice referred to as the compliance management system). In September 2018, the Prosecutor General's Office issued non-binding internal guidelines for public prosecutors, which explain in some detail how companies' compliance management systems should be evaluated during criminal proceedings.

In particular, each compliance management system should be evaluated with respect to the proportionality principle, which is to say that compliance management systems should be evaluated in proportion to the organisational size, regulatory density, the nature of business activities and how international they are, the risk profile and market environment of any given legal person. Most importantly, the system should have viable core elements: it should be preventive (able to dissuade and impede misconduct), capable of detecting any such misconduct and reactive to misconduct (disciplinary consequences or legal action, or it must learn from the misconduct). Finally, the system needs to be able to be continuously improved.

### ? Can criminal proceedings be settled with the enforcement authorities, or through leniency programmes?

There is no practice of out-of-court settlements, particularly if compared to the US settlement practice. Some instruments exist, but only a fraction of cases are resolved out of court. The out-of-court settlement system has essentially been constructed for prosecuting individuals and does not allow for prosecution to be settled without the admission of guilt. Some leniency policies exist, but these are primarily limited to tax or antitrust offences.

---

1 Act No. 418/2011 Sb, On the Criminal Liability of Legal Persons and Proceedings Against Them.

A guilt and sanctions agreement made between the perpetrator and the public prosecutor is the only out-of-court settlement that has been used in practice. However, this instrument has only been used in 1.5% of cases since its implementation. The offender must admit to his or her guilt and agree to sanctions that will then have to be confirmed by a court. Not only must the company admit guilt, but the majority of guilt and sanctions agreements are refused by courts.

Companies sanctioned with a ban on commercial activity, a ban on participating or working in public tenders or a ban on subsidies can, after half of the term of their penalty has passed, ask the court to be paroled and for the rest of their sanction to be dropped, on the condition that the company proves that it has implemented effective measures capable of preventing criminal activity.

## UPCOMING DEVELOPMENTS

Since companies became liable for criminal prosecution eight years ago, prosecuting authorities have acted hesitantly, limiting themselves to contemplating how best to approach their investigations into companies, and cautiously or clumsily testing the waters. However, steady improvements in the proficiency and technological development of the prosecuting authorities have led to an increase of highly complex cases. This is unfortunately at odds both with the current legislation that makes cooperation almost impossible between prosecuting authorities and companies that would wish to cooperate, and with the practical non-existence of settlements. At present, the OECD and the International Bar Association are in the process of attempting to convince national legislators to establish a predictable system and procedure for out-of-court settlements for companies, which currently have few incentives (if any) to cooperate and self-report.

*This chapter was written by Jitka Logesova and Jaromir Pumr.*



**JITKA LOGESOVA**

Partner

**Wolf Theiss, Czech Republic**

T. +420 234 765 223

[jitka.logesova@wolftheiss.com](mailto:jitka.logesova@wolftheiss.com)



**JAROMIR PUMR**

Associate

**Wolf Theiss, Czech Republic**

T. +420 234 765 216

[jaromir.pumr@wolftheiss.com](mailto:jaromir.pumr@wolftheiss.com)



WOLF THEISS

HUNGARY

## KEY TAKEAWAYS

- Companies may be criminally liable for the misconduct of their employees and board members.
- Investigating misconduct is included in management's fiduciary duties.
- Internal policies regulating the processing of employees' data and the investigation of misconduct are cornerstones of a proper investigation.
- The concept of legal privilege is limited to the obligation of registered attorneys to preserve the confidentiality of information received from their clients.
- Self-reporting or cooperation with prosecuting authorities does not have any automatic benefit for the company.

## OBLIGATION TO INVESTIGATE CRIMINAL MISCONDUCT INTERNALLY

### ? Are companies obliged to investigate misconduct internally?

Hungarian law does not explicitly lay down any such obligation. From the general fiduciary duty owed by the company's management to ensure compliant operations and business conduct from which the company it derives, however, that any suspected misbehaviour should be diligently investigated even if such misbehaviour does not directly relate to any criminal offence.

### ? In which situations will a decision to internally investigate be necessary to prevent the civil or criminal liability of board members?

Corporate statutory representatives (directors) owe a general fiduciary duty to ensure that they as well as the company managed by them follow all relevant laws as well as the company's articles of association or any resolutions of the company's supreme decision-making body.

Accordingly, in case of any reasonable suspicion of any possible wrongdoing, management is legally expected to take all appropriate steps to review (and legitimately rectify, if necessary) the situation. Unless an internal investigation is conducted, the directors risk being found in breach of their fiduciary duties and could therefore become liable for any prejudice (including damages) to the company that could have been prevented, had the wrongdoing been discovered in time.

The general threshold to trigger any criminal liability under the Hungarian Criminal Code is set at damage caused in excess of HUF 50,000 (approx. EUR 150). But obviously there are situations when criminal liability can be triggered without any monetary damage arising.

Furthermore, if a corporate director has a firm suspicion of a still ongoing criminal wrongdoing (e.g. corruption, money laundering, antitrust behaviour in public procurement or concession, etc.), he or she may per se be held liable for "non-hindering criminal wrongdoing".



- ? Is there a duty to report the outcome of the internal investigation or any information obtained during the internal investigation to enforcement authorities?  
If so, who is subject to the reporting duty and who is exempt?  
Are companies obliged to self-report?**

Under the Hungarian Criminal Code, in case of certain serious crimes (e.g. offences against the state or corruption involving officials) there is a reporting obligation (or obligation to stop them from even happening) by individuals having credible knowledge about the case, the failure to comply with which could constitute a criminal offence in itself. Hungarian legislation does not contain explicit rules on the reporting person, however, or about any straightforward exemptions.

The Hungarian Criminal Procedural Act confirms, nevertheless, that no one may be compelled to make a self-incriminating testimony or to produce self-incriminating evidence. In general, it can be established that the companies are not obliged to self-report.

- ? Would cooperation and voluntary self-disclosure be taken into account by the law enforcement authorities in relation to both individual and corporate liability?**

Voluntary self-disclosure and then engaging of good faith cooperation will customarily be considered by the acting judge as mitigating circumstance (i.e. leading to a lower sanction) during court proceedings. In some instances (e.g. antitrust behaviour in public procurement or concession) such cooperation can lead to a substantial reduction of or even immunity from criminal sanctions. Any such self-disclosure and subsequent cooperative conduct by the company cannot, however, lead automatically to preferential treatment or other benefits from the procedural or substantive law perspective becoming available to the company in Hungary.

## PLANNING AND STRUCTURING INTERNAL INVESTIGATIONS

- ? How should internal investigations be structured?  
When should an internal investigation be conducted by an attorney?**

The company should have an internal regulation in place that governs the process of dealing with (or even suspicion of) misconduct including internal investigation procedures as part of the compliance management system. It should specify the persons responsible for dealing with internal investigations and how the structure of the internal investigation should be decided, including a process for independent reporting.

Whenever there is a risk that a reporting duty has arisen, or will arise during the investigation, or if there is a risk of a police dawn raid, an attorney should be engaged as an external counsel to lead and conduct the investigation as well as to minimize the risk of exposure to the reporting duty, and to maintain legal privilege over investigation products.

Involving any external investigator should be considered on a case-by-case basis. If any further advice is needed from specific service providers and professionals such as forensic or accounting professionals, they should be subcontracted directly by the attorney and report directly to him or her. In such cases to conclude a confidentiality agreement is highly recommended.

## **CONFIDENTIALITY AND LEGAL PRIVILEGE**

- ? Who can be protected by attorney-client privilege ("legal privilege")?  
Which information/data is and is not protected by legal privilege, and  
what (if any) are the exceptions from legal privilege?**

"Legal privilege" under Hungarian law is awarded to the communication created between an attorney and their clients in the course of, in the interest of or within the framework of defence during any proceedings, i.e. not just during regulatory or criminal investigations, but all administrative authority procedures as well as all court procedures launched by Hungarian authorities or before Hungarian courts, such as, in particular, competition, data protection and tax related proceedings, and regulatory proceedings relating to the financial services, energy, food, gambling, insurance, pharmaceuticals and other sectors.

Such "legal privilege" will then prevent Hungarian authorities from reviewing or using as evidence any communication containing legal advice relating to defence in regulatory proceedings, so long as it is apparent from the communication and related documents that those were created by or related to exchange with external counsel.

- ? Does legal privilege extend to documents created by attorneys after they are handed over to the client?**

According to Hungarian law, all documents created by attorneys also have a legal privilege after those have been handed over to the clients. This means that Hungarian authorities shall not be allowed to use those documents as evidence in proceedings, that contains legal advice irrespective of whether they are available from the clients. They are only allowed to inspect only to the extent necessary to determine whether the lawyer has unreasonably refused access on the grounds of legal privilege. Legal advice in Hungary is defined broadly, so it is not limited to the advice itself, but to all information that the client and the attorney communicates between themselves (including documents both from attorney and client). Therefore it remains very important to structure an investigation, including the imbedded reporting channels, in a way that is sufficient to exclude the risk of any access by the investigatory authorities.

- ? Does legal privilege apply to in-house lawyers?**

Pursuant to a recent change in law, "legal privilege" applies to communication between the company and its in-house counsel to the extent that such an in-house counsel concerned is registered with the Hungarian Bar Association to perform attorney activities.

- ? Does legal privilege apply to other types of service providers?  
Can legal privilege be extended to them if they are subcontracted by attorneys?**

"Legal privilege" in Hungary is exclusively reserved for attorneys (including in-house counsel in certain instances, as discussed above). Although other regulated professions in Hungary (such as auditors, notaries, forensic or accountancy experts etc.) are also bound by certain professional secrecy obligations, their client-provider relationship will not benefit from the legal privilege provisions in Hungary. So long as their work products are bundled together and channelled through the external lawyer, however, the client will be able to benefit from the same legal privilege exemption.

## COLLECTING AND PROCESSING DATA AND DATA PRIVACY PROTECTION

### ? How should the company ensure that evidence is properly collected?

The company must determine what data are needed for the internal investigation. The company should keep in mind the following questions:

- What forms of communication are used? (e.g. emails, apps, phones etc.)
- How does the company handle the business and private contents? Is it allowed to keep private contents on any company device?
- What contains the internal policies concerning data protection?
- What devices do employees use to communicate?
- On what devices does the employer store data? (e.g. cloud, local servers etc.)
- Is the cooperation of a local IT expert needed?

It is then essential to determine whether and to what extent the company can legally access and review the data. A comprehensive and clear internal policy or guide providing the complete rules on communication, archiving and the use of company devices by employees on the one hand, and explicit information on how the company can review and collect these data on the other, is a cornerstone of any proper internal investigation.

Destroying any potential evidence during the investigation may be considered a breach of their employment duties by the side of the employees.

### ? What conditions must be met to allow investigators access to employees' emails/other records which potentially contain private information? Is the consent of the custodian necessary before data collection begins?

Any personal data processing may take place only on one of the lawful grounds specified by GDPR. The consent of the employee cannot serve as a lawful basis, however, as – based on the EU Data Protection Working Party's opinion – the precondition of "freely given nature" is almost never satisfied in case of employment relationships. Having regard to the rules of Grand Chamber of European Court of Human Rights set out in *Barbulescu vs. Romania*, and the Hungarian data protection authority's ("NAIH") related recommendation, in case of reviewing the employees' business emails the legal basis could be in the employer's legitimate interest, which requires previous legitimate interest assessment.

Based on NAIH recommendations it is of the utmost importance to create an internal policy related to the reviewing of business email correspondence. In this policy the employer should lay down conditions for review of emails.

The process of internal investigation requires compliance with further obligations as well. Accordingly, the affected employees must be informed in advance of – among others – the legal basis of data processing, the purpose of processing and (possible) technical means used for reviewing (in accordance with the GDPR and the applicable Hungarian law). Email review can affect exclusively the business communication.

Email review is allowed only to the extent strictly necessary to achieve its aim, e.g. based on the related practice of the headline or subject field of the email being sufficient to state the infringement the employer cannot process further data and open the email, the investigation shall refer only to a certain limited period in time, etc. If a software is used to find the relevant emails with the appropriate keywords, after sorting these emails, private email correspondence cannot be the subject to further investigation. As a general rule, the presence of the affected employee should be also ensured. Provided, however, that effectiveness of the investigation is compromised by the presence of the affected employee, it is in the employer's legitimate interest that the employee is not present at the investigation, subject to appropriate safeguards.

As such an email review may imply a high risk for the data subjects where a large amount of data is processed – despite the fact that the “black list” of mandatory data protection impact assessment issued by NAIH does not contain the review of business emails – the email review may require a data protection impact assessment (Article 35 of GDPR), and, where appropriate, the evidence related to the consultation with the data subjects (employees and their representatives).

**? Are there any restrictions in relation to cross-border transfers of data collected during an investigation?**

Cross-border transfer of data collected during an investigation to a third country is subject to strict requirements. In particular, companies must ensure adequate protection of the data even after their transfer. “Available and adequate means” includes binding corporate rules and standard data protection clauses adopted by the Commission.

**? What should the company do once the internal investigation is finished?**

Once the internal investigation is finished, the data gathered and processed during the internal investigation must be erased, with only the most important findings stored for the purpose of confronting the employee with the findings or for potential court or administrative proceedings. Employees whose data were processed must be informed of such processing.

## **INTERVIEWING EMPLOYEES**

**? Does an employee have an obligation to actively participate in interviews organised by the counsel of the employer?  
Is an employee required to participate and cooperate in interviews?**

Yes, which obligation can be inferred from the general obligation of cooperation set out in the Hungarian Labour Code, but the employee cannot be obliged to testify against himself/herself. However, refusal to cooperate may be considered a breach of their employment duties

**? Do employees have the right to receive minutes from the interview?**

No.

**? Do employees have the right to be informed of the outcome of the investigation?**

No, employees do not have to be informed of the outcome of interviews or the investigation.

## WHISTLEBLOWING

### ? Is there any specific regulation relating to whistleblowers?

**If so, is there any obligation to react to whistleblowing/to have a system in place for reacting to whistleblowing?**

Yes, there is special regulation for employers operating a whistleblowing system. However, it is only an option for private companies to set up any such whistleblowing system, not an obligation.

If a whistleblowing system has been set up for a private company, the employer becomes obliged to investigate the report and the whistleblower shall be notified about its result and the steps which are to be taken. However, the reports defined by the relevant Act (e.g. those made anonymously or by an unidentifiable whistleblower) might be ignored.

The regulations do not specify any obligations or requirements related to the whistleblowing system apart from the one that – if there is such a one – the whistleblowing system shall be created in a manner ensuring that the name of the whistleblower shall not be known by any person other than the examiner.

We note that the employer is subject to certain notification obligations under the relevant law. Primarily, the whistleblower should be informed/notified of the result of the investigation and of the measures taken.

## CRIMINAL PROCEEDINGS AGAINST THE COMPANY

### ? Is there corporate criminal liability in the country?

Yes, there is a strict corporate criminal liability in Hungary. A Hungarian company may be held criminally liable if its managing directors, employees with supervisory/leading functions and/or shareholder have committed crimes through or by way of using the company (within the company's field of business) or the company otherwise benefitted from those crimes.

### ? Can individuals and companies both be prosecuted for the same misconduct (parallel prosecution)?

Yes. Both the company and the individual perpetrator may be prosecuted for the same misconduct, though they would face different criminal sanctions.

### ? Can corporate criminal liability be avoided or mitigated?

A company cannot automatically avoid criminal prosecution by, for example, cooperating with authorities. However, cooperation and voluntary self-disclosure will always be considered at least as a mitigating circumstance (i.e. leading to lower sanctions).

### ? Can criminal proceedings be settled with the enforcement authorities, or through leniency programmes?

Under the relevant provisions of the Criminal Procedural Act and the Act on Criminal Measures Applicable to Legal Entities it is possible to conclude a settlement with the enforcement authorities during criminal proceedings, though a criminal measure ultimately becoming applicable to the company may not be the subject of any such settlement. A concluded settlement makes the investigation much easier and mitigates the penalty to a greater extent.

*This chapter was written by Janos Toth and Bela Madarasz.*



**JANOS TOTH**  
Partner

**Wolf Theiss, Hungary**

T +36 1 4848 810  
[janos.toth@wolftheiss.com](mailto:janos.toth@wolftheiss.com)



**BELA MADARASZ**  
Associate

**Wolf Theiss, Hungary**

T +36 1 4848 851  
[bela.madarasz@wolftheiss.com](mailto:bela.madarasz@wolftheiss.com)



POLAND

WOLF THEISS



## KEY TAKEAWAYS

- Companies may be criminally liable for the misconduct of their employees and board members.
- Investigating misconduct is included in management's fiduciary duties and is a sign of a sound compliance management system.
- Internal directives regulating the processing of employees' data and the investigation of misconduct are the cornerstone of a proper investigation.
- The concept of legal privilege is limited to the obligation of registered attorneys to preserve the confidentiality of information received from their clients.
- Self-reporting or cooperation with prosecuting authorities does not have any automatic benefit for the company in general criminal proceedings but does have a benefit in criminal fiscal proceedings.

## OBLIGATION TO INVESTIGATE CRIMINAL MISCONDUCT INTERNALLY

### ? Are companies obliged to investigate misconduct internally?

There is currently no such regulation requiring companies to conduct internal investigations in connection with reported misconduct. Nevertheless, the Polish Company Code introduces the liability of board members for the obligations of a limited liability company, in case the enforcement against the company proves unsuccessful. Although no obligation to carry out internal investigation is set forth by this provision, board members may still be very much interested in conducting such an investigation, given the risk of being held jointly and severally liable with the company for its obligations in the above-mentioned circumstances.

### ? In which situations will a decision to internally investigate be necessary to prevent the civil or criminal liability of board members?

Members of the board, when "not investigating suspicion of misconduct" might still be liable for "passivity" or "ignorance", because of the duty of care/fiduciary duties in investigation of misconduct.

In Poland, like several other countries, such passivity could most often result in a breach of duty of care or breach of fiduciary duties. It is conceivable that in such situations, the passivity (e.g. the CEO of a company ignoring signs that one of his subordinates steals from the company) causes damage to the company (monetary in relation to fraudulent behaviour, or reputational if criminal prosecution is later triggered). The corresponding liability could then be either criminal, or civil – as the company can sue the CEO and/or other board members for damages that his/her passivity caused, or bring a criminal referral against the CEO and/or other board members

However, unlike in certain other countries, such passivity cannot be recognized as participation in the crime, even in situations where the member of the board, again, ignores obvious signs of a crime (e.g. bribery) committed by one of his subordinates, and the intensity of his/her ignorance cannot result in criminal liability for participation in the said crime, or aiding its committal.

**? Is there a duty to report the outcome of the internal investigation or any information obtained during the internal investigation to enforcement authorities?  
If so, who is subject to the reporting duty and who is exempt?  
Are companies obliged to self-report?**

The Polish criminal law provides for two kinds of reporting duties. Firstly, the Polish Criminal Code recognises the failure to report specifically listed criminal offenses – most serious crimes, including also offences of a terrorist nature, murder, grievous bodily harm, bringing general danger, piracy, unlawful detention, rape, sexual abuse of a minor, hostage-taking. Failure to report such crimes constitutes a criminal offence.

Secondly, the Code on Criminal Procedure introduces a general obligation for anyone, who has learned about the perpetration of a criminal offence prosecuted ex officio, to report it to the prosecutor or the police, e.g. fraud, money laundering, bribery and others. This is however merely a social duty and failure to comply with this obligation does not imply any negative legal consequences.

With regard to the obligation of a company to self-report, under Polish law a suspect has no obligation to provide evidence against himself.

**? Would cooperation and voluntary self-disclosure be taken into account by the law enforcement authorities in relation to both individual and corporate liability?**

There is a legal obligation both for individuals and entities to provide assistance to authorities conducting criminal proceedings, whenever requested by the authorities and in the required time period.

Otherwise, cooperation and voluntary self-disclosure must be taken into account by the law enforcement authorities (in relation to both individual and corporate liability) in criminal fiscal cases.

An offender who, after committing a prohibited act, notified authorities appointed for the prosecution thereof, disclosing the material circumstances of the act, in particular the persons cooperating in its perpetration, shall not be subject to punishment for a fiscal offence or fiscal misdemeanour. Also, a person who submits a legally effective correction of a tax return and pays in full, immediately or by the deadline set by the fiscal authorities, the public due that has been depleted or threatened to be depleted, is not subject to a penalty for a fiscal crime or fiscal misdemeanour. For clarity, a criminal fiscal case is a case related to a fiscal offence, whereas a fiscal offence is an offence directed against the financial interests of the Polish State, which threatens the State Treasury with financial detriment.

The benefits of the cooperation/self-reporting are limited to fiscal crimes, not to crimes against property. The benefits of cooperation/self-reporting shall also apply to the perpetrator of giving a bribe, but not to the recipient of the bribe. A perpetrator of giving a bribe shall not be subject to punishment if a material or personal benefit or a promise thereof has been accepted, and the perpetrator has notified a body established for the prosecution of offences and disclosed all material circumstances of the offence before the body learned about it.

Should the Bill amending the Act on the liability of corporate bodies for criminal offences be adopted, companies would gain a fundamental incentive to cooperate with authorities. Pursuant to the provisions of the Bill, a company would not be held liable in case the committed crime, which cannot be a crime punishable by imprisonment of over 5 years, was reported by the company to the law enforcement authorities, including disclosure of relevant circumstances of committing the crime, as well as individuals and other collective entities taking part in it.

## PLANNING AND STRUCTURING INTERNAL INVESTIGATIONS

### ? **How should internal investigations be structured?** **When should an internal investigation be conducted by an attorney?**

Because of the lack of an express legislation regarding internal investigations, a company would be well advised to keep an internal regulation in place that governs the process of dealing with (suspicion of) misconduct including internal investigation procedures as part of the compliance management system. It should specify the persons responsible for dealing with internal investigations (usually an independent compliance function) and how the structure of the internal investigation should be decided, including a process for independent reporting.

Whenever there is a risk that a reporting duty has arisen, or will arise during the investigation, or if there is a risk of a police dawn raid, an attorney should be engaged as an external counsel to lead and conduct the investigation to minimize the risk of exposure to the reporting duty, and to maintain legal privilege over investigation products. If further advice is needed from specific service providers such as forensic or accounting professionals, they should be subcontracted directly by the attorney and report directly to him or her, so that the risk of exposure is minimized, and legal privilege is maintained.

## CONFIDENTIALITY AND LEGAL PRIVILEGE

### ? **Who can be protected by attorney-client privilege ("legal privilege")?** **Which information/data is and is not protected by legal privilege, and what (if any) are the exceptions from legal privilege?**

Under Polish law there are two types of confidentiality privileges: defence counsel privilege and attorney-client privilege. The defence counsel privilege is absolute and unlimited in time. Nobody can release the defence counsel from his/her privilege. Persons bound by the obligation of professional confidentiality: notaries, attorneys-at-law, tax advisers, doctors, journalists, or statisticians, and persons obliged to protect the secrets of *Prokuratoria Generalna Rzeczypospolitej Polskiej* (the General Solicitor's Office of the Republic of Poland) may be questioned about the facts covered by such secrecy only where this is necessary for the sake of justice and the circumstances cannot be determined on the basis of other evidence. In an investigation, the decision as to questioning or permitting questioning shall be taken by the court, at a session without the participation of the parties, within a period not longer than 7 days from the date of service of the motion by the public prosecutor. The court's decision may be contested.

The scope of legal privilege under Polish law is set forth in statutes with regard to the legal professions that can be carried out in Poland: the attorney-at-law (*adwokat*) and the legal adviser (*radca prawny*). In both cases, the attorney has to be registered with the respective Bar Association. The following rules apply also to foreign EU attorneys, registered with one of the Bar Associations, as well as legal trainees. EU attorneys, not registered in Poland, are generally (with a few exceptions) subject to the provisions on legal privilege in accordance with the law of the country of origin. The confidentiality obligation requires attorneys to preserve the confidentiality of everything learned in connection with the provision of legal advice, regardless of by which means of communication the lawyer acquired the information. Legal privilege covers any information regardless of whether it is on paper, in a computer, in a cloud, and irrespective of where it is located. This obligation cannot be limited in time. Information, which is not covered by legal privilege, includes information acquired by an attorney in the circumstances justifying suspicion of money laundering or terrorism financing. Neither is the information covered by tax mandatory disclosure rules (MDR) considered privileged.

**? Does legal privilege extend to documents created by attorneys after they are handed over to the client?**

Based on an internal regulation (the Code of Ethics of Attorneys-at-law), legal privilege does also apply to messages, notes and documents, in relation to the case, received from the client or other parties, irrespective of their location. Further, a similar internal regulation – the Code of Ethics of Legal Advisors, states that the confidentiality obligation should be extended to all documents created by the legal advisor and to the legal advisors' correspondence with the client and persons involved in the case, all which are created for the purpose of providing legal advice. Attorney-client privilege does not apply to documents if the holder is a person suspected of a crime (as opposed to a suspect, i.e. a person to whom criminal charges have been formally presented)

As a rule, these regulations are upheld by courts and prosecutors. Their violation happens exceptionally. However, noteworthy, both public prosecutors and courts attempt to use legally available means to obtain testimonies of attorneys and/or access to documents in the legal proceedings of various types.

**? Does legal privilege apply to in-house lawyers?**

Only in-house lawyers registered at a Bar Association enjoy legal privilege. In-house lawyers, not registered at a Bar Association, have the status of regular employees and don't enjoy legal privilege, unless they are a defence counsel in disciplinary proceedings, in which case in-house lawyers not registered at a Bar Association enjoy legal privilege, too.

**? Does legal privilege apply to other types of service providers?  
Can legal privilege be extended to them if they are subcontracted by attorneys?**

Besides attorneys, various other professions do enjoy legal privilege within a scope in accordance with the respective legal regulation of the given profession. Such professions include tax advisors, auditors and auditing firms. However, the confidentiality obligation does not extend to accountants. Attorneys-at-law and legal advisors are required to ensure that those who are working with them in the scope of their professional activity maintain confidentiality with regard to the scope of the legal privilege for attorneys.

It is worthy of note that a consequence of the absolute nature of defence counsel privilege is the prohibition of reading documents containing information covered by this privilege.

The course of action with respect to a letter or document depends on who made the statement that contains information covered by defence counsel privilege – a defence counsel or another person.

In a situation when such a statement is made by a defence counsel or a person who is not a defence counsel, e.g. a secretary of a lawyer's office, but it does not raise any doubts, the authority performing the activity shall leave the documents to the said person without becoming acquainted with their content or appearance. The statement by a defence counsel has an absolute character, as it is deemed credible and cannot be questioned.

Only when the statement of a person who is not a defence counsel does raise doubts, the authority carrying out the search shall, without reading the letter or document, wrap and seal it and hand it over to the court, regardless of who ordered the seizure of property or the search. The public prosecutor, even if he himself conducts the search, is not entitled to acquaint himself with the seized documents and to assess whether they are messages covered by the defence counsel privilege.

The court shall decide on the further handling of the retained letters or documents. It analyses the submitted letters and other documents from the point of view of whether they cover circumstances connected with performing the function of defence counsel. Only those documents are subject to retention for the purposes of the proceedings which are not related to the performance of the function of a defence counsel.

## **COLLECTING AND PROCESSING DATA AND DATA PRIVACY PROTECTION**

### **? How should the company ensure that evidence is properly collected?**

In the preparatory stage of the internal investigation the company should define what data must be obtained, identify the people who are in possession of the data as well as determine in what form (digital or paper form) it takes and where it is kept.

A good starting point for internal investigations is clearly defined internal policies which outline the rules of the use of the IT and communications systems and networks of the company, the use of company's devices, the methods of monitoring as well as gathering and processing data obtained by the company.

### **? What conditions must be met to allow investigators access to employees' emails/other records which potentially contain private information? Is the consent of the custodian necessary before data collection begins?**

Regulations protecting employees' privacy are in particular GDPR as well as the Labour Code and the Act on Personal Data Protection.

Before starting the internal investigation the internal privacy policy or privacy notice used by the company should be checked in order to determine whether employees have been properly informed about the purpose and legal basis for processing their personal data in relation to internal investigation as well as their rights in this respect.

Employee's data can only be processed on one of the lawful grounds determined in Article 6 GDPR. Given that the employee's consent to the data processing must be freely given and can be withdrawn at any time, the processing should rely on a legal basis other than consent. In internal investigations, the most common legal basis is the company's legitimate interest. Should the company rely on its legitimate interest it must run a balancing test and carefully consider whether the aim of the processing is a legitimate interest and whether the legitimate interest is not overridden by the employee's interests or fundamental rights and freedoms. In accordance with the principle of data minimisation the data processing must be necessary and proportionate for the purpose. The company must ensure that the least intrusive methods of data collecting and processing as regards the employee's privacy and data protection rights are selected.

In the course of the internal investigation the employee's personal rights, in particular the secrecy of correspondence, must be respected. Employees' emails/other records identified as private (e.g. from the subject header) cannot be accessed. A recommended solution allowing the preservation of privacy is filtering emails/documents by running keyword searches which display only emails containing one of the chosen keywords. In any case, if when reading emails or records it turns out that they are of a private nature the review must be immediately stopped. No private data should be processed.

### **? Are there any restrictions in relation to cross-border transfers of data collected during an investigation?**

If data collected during the internal investigations is transferred to outside the EU, there must be a legal basis for such a transfer under GDPR. An adequate level of data protection must be ensured by the company also after the data transfer to a third country. Based on adequacy decisions of the European Commission, data can be transferred, in particular, to Switzerland, Canada, Japan, Israel and New Zealand. If the transfer based on adequacy decisions is not possible, the most common arrangements are standard data protection clauses adopted by the European Commission or binding corporate rules.

### ? What should the company do once the internal investigation is finished?

Once the internal investigation is closed it must be evaluated as to what findings should be retained for possible disciplinary actions or a potential court or administrative proceeding. In accordance with the storage limitation principle determined in GDPR all other data collected and processed during the internal investigation must be deleted since the purpose of data processing has already been achieved. The transparency principle requires that employees whose personal data are processed in connection with the investigation must be informed as to how that data is used.

## INTERVIEWING EMPLOYEES

### ? Does an employee have an obligation to actively participate in interviews organised by the counsel of the employer?

**Is an employee required to participate and cooperate in interviews?**

Yes, it is the employee's duty to participate in internal investigations when instructed to do so by the employer. This obligation results from the obligation to take care of the best interests of the employer (loyalty obligation). Employees must follow the employer's orders which are related to work and lawful. Therefore, an employee, who potentially may have information about any irregularities which occurred in the company, instructed by the employer to actively participate in interviews must follow such an instruction. Refusal to cooperate can result in disciplinary sanctions.

Former employees are not obliged to cooperate in internal investigations. However, such an obligation can be imposed in a settlement agreement. This is usually the case if the irregularities have been reported before the employee left the company and the employer grants the employee in the settlement agreement an additional voluntary severance pay.

### ? Do employees have the right to receive minutes from the interview?

No, because these are documents prepared for the employer's internal purposes.

### ? Do employees have the right to be informed of the outcome of the investigation?

Currently, no, but if the interviewed employee is the reporting person (whistleblower) who triggered the internal investigation, he/she will need to be informed of the investigation's progress and outcome under the EU Directive on the protection of whistleblowers which must be implemented by the EU member states until December 2021.

## WHISTLEBLOWING

### ? Is there any specific regulation relating to whistleblowers?

**If so, is there any obligation to react to whistleblowing/to have a system in place for reacting to whistleblowing?**

As of now, there is no comprehensive law which would provide for general rules on whistleblowing. Industry-specific laws introduce certain provisions on the rights and obligations of whistleblowers; however, due to the nature of these regulations, their scope of application is very limited. This applies to, for example, the Act on Banking Law, Anti-Money Laundering Act and the Regulation on technical and organisational requirements for investment firms.

A possible source of a regulation for whistleblowers could be the Bill on Liability of Corporate Bodies. The law, which has yet to be adopted, could potentially introduce provisions e.g. on the obligations of corporate bodies

regarding the notification of the whistleblower, the scope of protection and the right of the whistleblower under certain circumstances to claim damages. The Bill also proposes a fine for corporate bodies in the event of non-compliance with obligations concerning whistleblowing that is two times higher than the maximum fine for collective entity for the relevant crime or misconduct.

Nevertheless, we can expect the implementation into Polish law of the EU Directive 2019/1937 on the protection of whistleblowers to be the key-regulation in this field. Based on available information, the Minister of Development, Labour and Technology was appointed in December 2020 to carry out various legislative works with the goal of the implementation of the EU Directive. Currently, no information on the contents of the Bill has been made available. It can be expected that the Bill will follow previous implementations of EU law and opt for a literal transposition. However, uncertainties on a number of issues remain, such as the admissibility of anonymous reporting, penalties and their amounts as well as a detailed scope of application.

## **CRIMINAL PROCEEDINGS AGAINST THE COMPANY**

### **? Is there corporate criminal liability in the country?**

Yes. A corporate body (company) shall be held liable for an offence involving the conduct of an individual:

- who acts for or on behalf of the company within the framework of his/her right or obligation to represent the entity, make decisions on behalf of the entity or perform internal audits, or violating that right or obligation,
- who is in a position to act because of violation by the person referred above of his/her rights or obligations,
- who is acting for or on behalf of the company with the consent or acquiescence of the person referred above,
- who being an entrepreneur collaborates with the company on a permanent basis to achieve a legal purpose,
- if the company benefitted or could have benefitted from that conduct, even non-financially. However, the company will not be held accountable if it can prove to have made the decision on the employment of the individual with due diligence or to have exercised due supervision over such person.

Strict corporate criminal liability exists which means that a company's criminal liability depends solely on the actions and intentions of the perpetrator. At the same time, it does remain, though dependent on the criminal liability of the perpetrator.

### **? Can individuals and companies both be prosecuted for the same misconduct (parallel prosecution)?**

There must be two independent criminal proceedings, one against the individual and the second against the company. According to the planned provisions of the bill, as opposed to the current wording, a company could be held liable without prior conviction for a criminal offence of an individual.

According to the current regulations, the company shall be prosecuted and held liable if the fact that the individual has committed an offence is confirmed by a final and non-appealable judgement convicting that person, a judgement conditionally discontinuing the criminal proceedings or criminal fiscal proceedings against that person, a ruling granting that person a right to voluntarily surrender to liability, or a court ruling to terminate the proceedings against that person due to the circumstances preventing him/her from being punished.

Both the perpetrator and the company can be prosecuted in the same proceedings with respect to fiscal offenses and fiscal misdemeanours.

### ? Can corporate criminal liability be avoided or mitigated?

A company can deflect its liability, if it can be proven that a corporate body or a representative of the company, acting with adequate diligence required under the given circumstances, provided for the organisational arrangements of the entity's activity that ensured the prevention of committing a criminal offence by the individual.

If, in a given case, conducting an internal investigation were to be seen as part of such organisational arrangements aimed at preventing a criminal offence, then the company will have to prove that carrying out such an investigation is in order to avoid liability. In fact, proving that the company acted without due diligence or supervision may be difficult considering internal compliance systems and other monitoring instruments, introduced nowadays by companies.

Corporate criminal liability can be avoided by cooperation and voluntary self-disclosure, which must be taken into account by the law enforcement authorities in criminal fiscal cases.

An offender who, after committing a prohibited act, notified authorities appointed for prosecution thereof, disclosing the material circumstances of the act, in particular the persons cooperating in its perpetration, shall not be subject to punishment for a fiscal offence or fiscal misdemeanour. Also, a person who submits a legally effective correction of a tax return and pays in full, immediately or by the deadline set by the fiscal authorities, the public due that has been depleted or threatened to be depleted, is not subject to a penalty for a fiscal crime or fiscal misdemeanour.

### ? Can criminal proceedings be settled with the enforcement authorities, or through leniency programmes?

A court settlement between the Company and the prosecutor is conceivable whereby they agree on a sentence and file a motion for conviction. The court may grant the motion for conviction when the circumstances of the crime and guilt are not in doubt and the objectives of the proceedings will be achieved despite not holding a full trial.

## UPCOMING DEVELOPMENTS

The Act on Liability of Corporate Bodies, currently in force, has been fairly inefficient. Only 88 companies were convicted, and the penalties were extremely low. The Bill amending the act on liability of Corporate Bodies is intended to change the philosophy of punishing companies that would be convicted without a prior conviction of an individual.

The Bill amending the Act on Liability of Corporate Bodies provides for the liability of companies for crimes committed by their employees although it only applies to larger companies, with more than 250 employees. The potential fines could reach PLN 50 million.

Under the Bill, a company may be held liable if the perpetration of a prohibited act occurred as a result of a lack of due diligence in the selection of an individual, a lack of due supervision of that individual, or a failure to exercise due diligence required under the circumstances to prevent an employee from committing a prohibited act. The company will only be liable for the employee's crime if it is related to the company's business.



To protect itself from sanctions imposed by a court, the company will need to comply with the requirements of the new Act on Liability of Corporate Bodies and demonstrate ongoing due diligence aimed at preventing a sanctionable act from occurring. It can do this by way of establishing internal compliance service, conducting a regulatory compliance and whistleblowing risk analysis, implementing relevant policies and procedures, and channels for anonymous whistleblowing and conducting regular audits.

*This chapter was written by Lech Gilicinski, Arkadiusz Matusiak and Agnieszka Nowak-Blaszczyk.*



**LECH GILICINSKI**

Partner

**Wolf Theiss, Poland**

T. +48 22 3788 953

[lech.gilicinski@wolftheiss.com](mailto:lech.gilicinski@wolftheiss.com)



**ARKADIUSZ MATUSIAK**

Counsel

**Wolf Theiss, Poland**

T. +48 22 3788 934

[arkadiusz.matusiak@wolftheiss.com](mailto:arkadiusz.matusiak@wolftheiss.com)



**AGNIESZKA NOWAK-BLASZCZAK**

Senior Associate

**Wolf Theiss, Poland**

T. +48 22 3788 943

[agnieszka.nowak-blaszczak@wolftheiss.com](mailto:agnieszka.nowak-blaszczak@wolftheiss.com)



WOLF THEISS

ROMANIA

## KEY TAKEAWAYS

- Under Romanian law, companies face criminal exposure for misconduct of their employees and board members.
- Internal investigations and sound compliance programmes are key for complying with the Board obligation to prevent harm to the company.
- Data protection by design should enable safe and sound internal investigation processes. Remote internal investigations determined by work from home policies should be addressed specifically.
- Legal privilege covers external attorney – client communication and could be extended to subcontractors (inhouse lawyers' advice is not protected).
- For corruption or assimilated crimes, there is a duty to report to the prosecuting authorities.
- The national implementation law on the whistleblower is broader in scope than the EU Directive and likely to lead in practice to an intensification of reported cases.

## OBLIGATION TO INVESTIGATE CRIMINAL MISCONDUCT INTERNALLY

### ? Are companies obliged to investigate misconduct internally?

To date, local legislation did not expressly provide for the obligation to internally investigate misconduct. Internal investigations were often triggered by the board members, exercising their general duty to prevent damage to the company. Such duty includes also the efforts to ensure compliance culture within the organisation and also to investigate the cases where there are red flags for wrongdoings or even indications for the occurrence of damage, and ultimately address the identified issues by making informed and appropriate decisions to mitigate their negative consequences.

This perspective is likely to change given the legal obligations to be enforced under the local rules implementing the Whistleblower EU Directive, as private companies will be under a duty to follow up on whistleblowers' reporting and to keep a special register with the internal investigation measures taken. As per the draft law<sup>1</sup>, an internal reporting may be rejected/closed in limited circumstances where the alert does not satisfy the legal conditions (e.g. the whistleblower reporting is anonymous and includes the facts leading to a violation of the law and relevant evidence).

### ? In which situations will a decision to internally investigate be necessary to prevent the civil or criminal liability of board members?

There is a "warranty liability" to which the directors/members of the Board/General Manager are/is held. Namely, in their capacity of warrantors and controllers of the other officers and the personnel, if any of the latter would cause a damage for the company in the exercise of their activity, the directors/members of the Board/General

<sup>1</sup> The main aspects related to the draft law implementing the whistleblower mechanism is provided below under Whistleblowing.

Manager are held responsible if the loss would not have occurred had they properly pursued their monitoring and control tasks.

The directors/members of the Board/General Manager are subject to multiple types of statutory liability towards the company, third parties and the authorities. Directors can be personally accountable for: (i) civil law liability vis-à-vis the company (in particular, if they violate their duties), (ii) civil law liability vis-à-vis third parties (in particular towards the creditors if the company is insolvent, and the directors contributed to the insolvency of the company), and (iii) criminal law liability for misconduct set out in the Criminal Code. The most relevant criminal offences provided by the Romanian law are the offences of abuse of the assets or the credit of the company, of the powers granted by the office of director or deceptive accounting.

Diligent behaviour of the board members might deflect their civil responsibility, even though the legislation does not provide express rules related to this outcome of the internal investigations. In other terms, even if there is no legal requirement for performing an internal investigation (as a separate process), before claiming any civil responsibility from an employee or a board member in the court, the benefit of the internal investigation is unquestionable. If the board members perform such an internal investigation and they are not involved in the offence that created the civil damages to the firm, the board members may use in their defence the evidence that proves their innocence.

The Romanian Labour Law regulates the disciplinary procedure for all personnel – management and non-management which is applicable to both public and private sectors (being applicable for the board members/directors who are also contracted by the company on an individual labour contract basis). This is rather a right of the company/shareholders than an obligation of the company. Thus, if the employer/the company decides to take disciplinary measures, such a decision may be made in most of the cases as a result of an internal investigation performed under the disciplinary procedure regulated by the Romanian Labour Code. Within the disciplinary procedure, the company will manage the evidence for the potential misconduct of the employee and offer the employee the possibility to defend himself/herself and present his/her own evidence. As a board member, the evidence revealed by a preceding internal investigation may be useful to prove the fact that the general duty of protecting the company was fulfilled.

The company also has the possibility to perform an internal investigation as a process preceding the disciplinary procedure, and pursuing the findings of such investigation, to commence the procedure against the involved employees, which is mandatory to apply the majority of the disciplinary sanctions provided by the labour legislation (except for a warning). In any of these cases, the legal term for applying the disciplinary sanction shall be observed.

Also, the board members must not only set appropriate procedures to prevent misconduct, but also investigate any detected misconduct, which often includes an internal investigation. If the company and the board members contribute to the mitigation of the negative consequences of the criminal offence, the board members who made appropriate decisions, actively investigating the wrongdoing, and acting diligently in the manner they perform their activities on behalf of the company, may use this evidence to defend themselves and even to obtain a full deflection of the – criminal liability for the cases where they have not been directly involved in the criminal offence and prove that they do not tolerate such misconduct and cooperate with the law enforcement agencies.

- ? Is there a duty to report the outcome of the internal investigation or any information obtained during the internal investigation to enforcement authorities?  
If so, who is subject to the reporting duty and who is exempt?  
Are companies obliged to self-report?**

If the outcome of the investigation is related to public or private corruption<sup>2</sup> or other associated crimes, the representatives of the firm (with the power of control) have an obligation to report it to the authorities. The individuals with control tasks are obliged to notify the criminal investigation body or, other bodies empowered by

<sup>2</sup> The Romanian Criminal Code, Article 308, sanctions not only the acts of corruption committed by public servants, but also corruption in the private sector.

law, regarding any data from which results indications that an operation or an illicit act may have occurred which may attract criminal liability according to Law no. 78/2000 on preventing, discovering and sanctioning acts of corruption.

According to the Romanian Criminal Code, if a public servant (but also any person who supplies a public service, or who shall be subject to the public authorities' control or supervision) becomes aware of an offence criminalised by law in connection with the service but omits to immediately notify the criminal investigation body, shall be punished up to 3 years of imprisonment or a penal fine. A person employed in the private sector might also be subject to this obligation, if his/her activity falls under a public authority's control or supervision; e.g. employees working in banking, insurance or in other areas regulated and controlled by a public authority.

**? Would cooperation and voluntary self-disclosure be taken into account by the law enforcement authorities in relation to both individual and corporate liability?**

In Romania, cooperation and voluntary self-disclosure may be considered by the criminal authorities in relation to both an individual and a legal entity.

Based on the Romanian Criminal Code, a person (i.e. the perpetrator) will not be punished if, before the criminal authorities become aware of the illicit act, that person gave up on committing the respective act or informed the authorities of the illicit act in question so that the completion of the illicit act could be prevented, or if that person directly prevents the respective crime from being committed<sup>3</sup>. Any efforts made by an offender to eliminate or reduce the consequences of their offence or any circumstances relating to the committed offence, which reduce the seriousness of the offence or the threat posed by the offender, may count as mitigating circumstances and therefore the penalty prescribed by law is reduced by one-third.<sup>4</sup>

## **PLANNING AND STRUCTURING INTERNAL INVESTIGATIONS**

**? How should internal investigations be structured?  
When should an internal investigation be conducted by an attorney?**

Internal investigations are not specifically regulated by Romanian law. Therefore, the internal investigation procedures should be regulated by the company as part of its compliance management system. It should specify the persons responsible for dealing with internal investigations (usually an independent compliance function) and how the structure of the internal investigation should be decided, including a process for independent reporting.

An internal investigation should be conducted externally (i.e. by engaging an external lawyer to lead and conduct the investigation, in order to minimise the risk of exposure to the reporting duty, and to ensure legal privilege over investigation products) whenever there is a risk that a reporting duty has arisen, or will arise during the investigation, or if there is a risk of a police dawn raid.

---

<sup>3</sup> Article 34 of the Romanian Criminal Code.

<sup>4</sup> Articles 75 and 76 of the Romanian Criminal Code.

<sup>5</sup> Legal professional privilege is regulated by Law no. 51/1995 regarding the organisation and exercise of the attorney's profession and the Statute of the attorney profession, but also by the Romanian Civil Procedure Code, Romanian Criminal and Procedure Codes and by the Law no. 21/1996 regarding competition.

## CONFIDENTIALITY AND LEGAL PRIVILEGE

### ? **Who can be protected by attorney-client privilege ("legal privilege")? Which information/data is and is not protected by legal privilege, and what (if any) are the exceptions from legal privilege?**

Confidentiality and attorney-client privilege ("legal privilege") refers to the information/data/correspondence and communication between the attorney and his/her clients, and to the legal services provided by the attorney to his or her clients, in compliance with the deontological and ethical standards. It will not apply to any criminal activities carried out by the attorney in relation with the client activities, for the respective client.<sup>5</sup>

According to Romanian law, the attorney has the obligation to keep the professional secrecy regarding any aspect of a case entrusted to him/her, unless it is provided otherwise by the law. Professional documents and paperwork that are in the attorney's custody or in his/her law office are inviolable.

The search of the attorney, of his/her residence or law office, or the seizure of records and assets may be done only by a public prosecutor, based on a warrant issued under the terms of the applicable law. Documents containing communications between the attorney and his/her client or containing records made by an attorney on matters relating to the defence of a client are exempted from evidence seizure and confiscation. Also, the attorney's phone calls cannot be listened to or recorded by any technical means, nor the attorney's professional correspondence be intercepted and recorded, except under the conditions and by the procedure provided by the law.

The relationship between the attorney and the person he/she is assisting or representing cannot be the subject of technical supervision, except when there is evidence that the attorney is committing or preparing to commit a crime. If the technical supervision also covered the relationship between the attorney and the suspect or defendant, the evidence obtained cannot be used in any criminal proceedings and will be immediately destroyed by the prosecutor.

### ? **Does legal privilege extend to documents created by attorneys after they are handed over to the client?**

Legal privilege cannot be extended to documents created by attorneys after they are handed over to the client. Any information or document that is protected when in the possession of the attorney is not protected when it is in the hands of the client or an unrelated third person. The confidentiality obligation is strictly related to the person of the attorney (including his/her employees, subcontractors), rather than to the information or document itself.

### ? **Does legal privilege apply to in-house lawyers?**

In Romania, the law does not secure such privilege for the in-house legal advisors.<sup>6</sup>

### ? **Does legal privilege apply to other types of service providers? Can legal privilege be extended to them if they are subcontracted by attorneys?**

In Romania, there are no specific legal provisions related to third party providers' privileges. Nonetheless, as they are employed by the attorney to support the attorney in dealing with the investigation or for the purpose of clarification of certain aspects in order for the attorney to be able to advise his/her clients, in principal, we consider that the legal privilege should be extended over the communication and correspondence with the service providers, including, for instance, the client's electronical data sent by an attorney to a forensic accountant for an analysis, which shall further document the client's defence. This privilege should be expressly written in the contract signed between the attorney and the service providers.

<sup>6</sup> Law no. 514/2003 regarding legal advisors.

## **COLLECTING AND PROCESSING DATA AND DATA PRIVACY PROTECTION**

### **? How should the company ensure that evidence is properly collected?**

The company should have in place internal norms/procedures providing comprehensive and clear rules on communication, data storage, the use of company's devices by its employees, as well as the information on how the company may collect and review personal data within an internal investigation. In this regard, the company must assess and determine what data is needed for the internal investigation, and to what extent it can legally access and review the data, considering data protection legislation.

Moreover, before starting the data processing regarding the internal investigation, the company should issue a preservation notice to the employees in question to ensure that potential evidence related to the investigated matter is not destroyed, as well as to inform the employees about their data processing according to GDPR provisions.

### **? What conditions must be met to allow investigators access to employees' emails/other records which potentially contain private information? Is the consent of the custodian necessary before data collection begins?**

In Romania, the interception, storage, or any other operations in relation to electronic communications are allowed in certain cases, such as:

- the processing is regulated by the law;
- the user of the equipment consented to such processing;
- access is given to the competent authorities.

For the purpose of internal investigation, under the GDPR, access to the employees' business email accounts would be possible in our view only based on Article 6 (1) letter f), namely on a legitimate interest of the employer in ensuring the efficient running of the organisation, or for another similar legitimate interest, and following the conditions below mentioned:

- the employee was informed about this possibility before using the email account (i.e. when the person was employed by the company), and the internal policy of the firm provides that the email should be strictly used for business communication only;
- the balancing test provided by article 6 (1) letter f) of GDPR is in favour of the employer, meaning that the measure to monitor/access the employees' emails and other communication methods is proportionate to the specific aim pursued by the employer (e.g. the trigger is related to a very serious incident, such as indication for serious fraud cases, corruption, etc.);
- the employee was additionally informed in accordance to Article 13 of GDPR about this monitoring/ access of the business emails and the privacy note was sent to him/her in advance (before the email account has been accessed);
- if the data is copied/stored on a different media storage, this is made known to the employee;
- the private related emails are not accessed.

---

7 Article 35 of GDPR in conjunction to Article 5 of the Law no. 190/2018 regarding the implementation of GDPR and the Decision of the National Supervisory Authority for Personal Data Processing no. 174/2018 regarding the list of the personal data processing that are mandatory in the scope of the data protection impact assessment.



Under some circumstances the employer may need to perform a data protection impact assessment<sup>7</sup>, as well as to demonstrate that there is no other less intrusive means for achieving the legitimate interest of the employer or the evidence that the data subjects (employees and their representatives) have been consulted, especially if the legal entities decide to implement an internal investigation system process that may imply processing of personal data through access of the employee's emails or monitoring systems (such as data loss prevention tools or e-forensic tools).

Consequently, a thorough analysis on a case by case basis is recommended for establishing the framework in which such email access is allowed, depending on the case circumstances.

**? Are there any restrictions in relation to cross-border transfers of data collected during an investigation?**

Specific conditions apply to cross-border transfers of personal data collected during investigations, considering the provisions of GDPR. When personal data is transferred outside the European Economic Area, companies must ensure that the data will be adequately protected even after their transfer to a third country. In this respect, the international transfer of personal data must be carried out by the companies with the observance of special safeguards provided by the GDPR, such as: adequacy decisions, binding corporate rules, standard contractual clauses adopted by the European Commission, certification mechanism, codes of conduct, so-called "derogations", etc. In addition, where the data is transferred within the group companies, the relevant intra-group policies should be in place.

**? What should the company do once the internal investigation is finished?**

The data collected and processed during the internal investigation must be erased once the internal investigation is finished, except for those findings necessary for potential court or administrative proceedings.

## INTERVIEWING EMPLOYEES

**? Does an employee have an obligation to actively participate in interviews organised by the counsel of the employer?  
Is an employee required to participate and cooperate in interviews?**

The employee has the right to participate in the interviews performed as part of the disciplinary procedure (i.e. it is not an obligation, but in the case of absence, the employee will miss the opportunity to defend himself/herself in front of the employer's representatives).

In corporate investigations/internal audits, there is no express legal obligation for the employee to actively participate. Such an obligation may be regulated through the internal procedures of the company, and communicated transparently to the employees, being part of the loyalty obligation of the employees or of their general duty to act responsibly and cooperate with the company in protecting the integrity of the other employees or the assets of the firm. However, if the employee refuses to participate in such an interview, the employer cannot oblige him/her to participate. For the public authorities, the assessment of the legal obligation of the public clerks to participate in the internal investigations shall be assessed on a case by case basis.

**? Do employees have the right to receive minutes from the interview?**

No.

**? Do employees have the right to be informed of the outcome of the investigation?**

No, employees do not have to be informed of the outcome of interviews or the investigation.

## WHISTLEBLOWING

**? Is there any specific regulation relating to whistleblowers?  
If so, is there any obligation to react to whistleblowing/to have a system in place for reacting to whistleblowing?**

Romania will soon enforce the local rules implementing Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law<sup>8</sup>.

Such legislation will replace the existing mechanism limited to the public sector. Starting in 2004, taking into account the recommendations of GRECO and the UN Convention against Corruption, by Law no. 571/2004 protection of whistleblowers in the public sectors was introduced. Public institutions and state-owned companies (irrespective of the number of shares owned by the state) had an obligation to ensure that employees have the possibility to submit whistleblowing complaints in several areas<sup>9</sup>. Moreover, in the case of any suspicion of corruption (such as the misuse of EU funds), the employees' or entity's representatives had an obligation to report this to the criminal authorities.<sup>10</sup>

As per the new draft law, the element of novelty relates to the extension of the scope of the whistleblower mechanism and protection to the private sector. Thus, companies with more than 50 employees will have to identify or establish internal reporting channels, which they will make available for potential alerts<sup>11</sup>. The legislative solution chosen takes into account that, in the case of private entities, the obligation to establish reporting channels must be proportionate to the size of the entities and take into account the level of risk that their activities pose to the public interest. The exemption from the obligation to set up whistleblower compliance systems does not apply to undertakings which fall within the ambit of financial services, products and financial markets, money laundering and terrorism financing, transportation safety and environmental protection legislation. They will continue to have the obligation to identify or establish internal reporting channels, in accordance with the legal provisions in force.

The whistleblowers may be the companies' employees, but also any other person who, due to his/her professional activity, becomes aware of violations of the law at the company level, such as self-employed persons, shareholders, administrators, directors, suppliers of products or subcontractors of services, as well as paid and unpaid volunteers and trainees.

In addition, the scope of reporting is broader under the proposed national legislation than the exhaustive list of EU law violations provided under Directive (EU) 2019/1937. Under the local draft law, whistleblowers may report on any violations of the law, i.e. actions or omissions that constitute non-compliance with legal provisions, which represent disciplinary violations, contraventions or offences, or that contravene their object or purpose, including non-compliance with ethical and professional rules. Such provisions have been criticised by the business community in Romania as exceeding the public interest rationale and over-expanding the whistleblower mechanism with potential trivial alerts.

<sup>8</sup> In April 2021, the draft law was subject to public consultation, the expected adoption is by December 2021.

<sup>9</sup> Law no. 571/2004 on the protection of the whistleblowers in the public sector. Possibility to report must be ensured in areas such as corruption, conflicts of interest, discrimination, public procurement, gross negligence, non-compliance with transparency in relation to public information or decision-making processes in the public sector, etc.

<sup>10</sup> Art. 23 of Law no. 78/2000 on preventing, discovering and sanctioning acts of corruption.

<sup>11</sup> The draft law exempts private companies with less than 50 employees from the obligation to set up internal reporting channels. Employees of such undertakings may report externally, directly to the competent national authorities.

The draft law regulated the reporting and follow-up procedure to be implemented by private undertakings, including the following key steps to be designed in the internal procedures: (i) appointment of an internal or external independent person/entity to receive, register, examine, follow-up on and settle reports, who acts impartially and who enjoys independence in the performance of those duties, (ii) design, establishment and management of the manner in which reports are received in such a way as to protect the confidentiality of the identity of the whistleblower and of any third party mentioned in the report and to prevent access to it by unauthorised staff members, (iii) obligation to send to the whistleblower, within a maximum of 7 working days from the receipt of the report, the confirmation of its receipt and to inform the whistleblower about the status of subsequent actions, within a maximum of 3 months from the date of confirmation of receipt as well as, whenever there are subsequent actions, unless the information could jeopardise the inquiry. The designated person/entity, as well as the means of reporting must be brought to the attention of each employee, either by posting on the website of the institution or by posting at the headquarters, in a visible and accessible place. The employer must ensure that at least one means of reporting is accessible at all times.

## **CRIMINAL PROCEEDINGS AGAINST THE COMPANY**

### **? Is there corporate criminal liability in the country?**

Yes. Under the Romanian Criminal Code<sup>12</sup>, legal entities in the private sector are liable for criminal acts. The main sanction is a penal fine. Other penalties might consist of the dissolution of the legal entity, suspension of its activity, the closure of certain points of work, prohibition from participating in public procurement procedures, placement under judicial supervision or displaying or publishing the conviction decision.

A compliance system may prevent and mitigate corporate criminal liability if correctly implemented, enforced and monitored by the company's management.

### **? Can individuals and companies both be prosecuted for the same misconduct (parallel prosecution)?**

Both companies and individuals can be prosecuted for the same misconduct. The Romanian Criminal Code expressly stipulates that the criminal liability of a legal entity does not exclude the criminal liability of the individual participating in the committing of the same offence.

### **? Can corporate criminal liability be avoided or mitigated?**

The Romanian law provides no option how to avoid criminal liability. A compliance system may prevent and mitigate corporate criminal liability if correctly implemented, enforced and monitored by the company's management.

### **? Can criminal proceedings be settled with the enforcement authorities, or through leniency programmes?**

There is no established practice of out-of-court settlements, particularly if compared to the U.S. settlement practice. Settlement and leniency policies are regulated in relation to antitrust offences. A company may benefit from full or partial immunity from fines if it applies for leniency or recognises the competition law breach early in the investigation process.

---

12 Art. 135 et seq. of the Romanian Criminal Code.

## UPCOMING DEVELOPMENTS

Given the extension of the whistleblower mechanism to the private sector, increased focus in the media and prospects of granting rewards to the respective persons, one could expect an increase in the utilisation of such a tool for reporting information on law violations obtained in the context of work-related activities. Companies will not only have to allocate resources for setting up a functional whistleblower mechanism in strict compliance with the legal standards but also might need to shift the organisational mindset and culture in connection to conducting the internal investigation measures in response to credible whistleblowing reports. Such follow-on corporate investigation measures will need to be documented and kept in a specific register.

As regards the internal investigation process, given the work from home circumstances which might become permanent for some companies, the internal procedures will need to be adapted to make possible remote investigations. Particular operational and data protection issues as well as potential interim measures will need to be adapted to reflect the new realities of work from home policies.

*This chapter was written by Anca Jurcovan, Bryan Jardine and Nina Lazar.*



**ANCA JURCOVAN**

Partner

**Wolf Theiss, Romania**

T. +40 21 3088 107  
[anca.jurcovan@wolftheiss.com](mailto:anca.jurcovan@wolftheiss.com)



**BRYAN JARDINE**

Partner

**Wolf Theiss, Romania**

T. +40 21 3088 102  
[bryan.jardine@wolftheiss.com](mailto:bryan.jardine@wolftheiss.com)



**NINA LAZAR**

Associate

**Wolf Theiss, Romania**

T. +40 21 3088 184  
[nina.lazar@wolftheiss.com](mailto:nina.lazar@wolftheiss.com)



**SERBIA**

**WOLF THEISS**

## KEY TAKEAWAYS

- Companies may be criminally liable for the misconduct of their employees and management.
- Ensuring compliance with applicable laws and regulations is included in management's fiduciary duties and is a sign of adequate corporate governance.
- Internal directives regulating the processing of employees' data and the investigation of misconduct are the cornerstone of a proper corporate investigation.
- Self-reporting or cooperation with prosecuting authorities does not have any automatic benefit for the company.
- Attorney-client privilege is protected in various procedural laws, effectively preventing attorneys from being forced to reveal confidential information received from their clients.

## OBLIGATION TO INVESTIGATE CRIMINAL MISCONDUCT INTERNALLY

### ? Are companies obliged to investigate misconduct internally?

Although there is no explicit obligation for companies to conduct internal investigations aimed at identification of potential misconduct related to their business operations, companies are required to ensure compliance with applicable laws and regulations, which fact necessitates special care and diligence in the course of conducting business operations, from the company's perspective.

### ? In which situations will a decision to internally investigate be necessary to prevent the civil or criminal liability of board members?

To mitigate the risk of the liability for damages or criminal liability, a company's management needs to take appropriate steps in order to ensure the remediation of identified breaches, one of which steps could be the performance of an internal investigation.

Members of the management bodies (i.e. directors, supervisory board members, other representatives) have specific duties towards the company, including a general fiduciary duty. This duty means that all the above persons must act in accordance with their duties consciously, with the diligence of a "prudent businessman", and with a reasonable belief that they are acting in the best interests of the company. One of the obligations of directors of the company is reporting to the shareholders assembly, or the supervisory board, on the status of company's compliance with applicable laws and regulations.

Breaching the abovementioned duties may lead to liability for damages of the director towards the company and/or the shareholders. Further, if the action (or inaction) of the director caused damages to third parties under the general rules of tort, the company may also be liable for damages to such third parties.

Acting in accordance with fiduciary duties described above may also serve to exclude potential criminal liability (due to strict terms of criminal liability) of the company's management for potential breaches of laws and regulations within the company.

- ? Is there a duty to report the outcome of the internal investigation or any information obtained during the internal investigation to enforcement authorities?  
If so, who is subject to the reporting duty and who is exempt?  
Are companies obliged to self-report?**

There is no explicit self-reporting requirement under Serbian law with respect to the bribery-related criminal offences.

On the other hand, a separate criminal offence titled "Failure to Report a Criminal Offence" applies, *inter alia*, to an authorized person within a legal entity who knowingly fails to report a criminal offence of which he/she became aware in the course of his/her duties, if the identified criminal offence may be subject to imprisonment of at least five years.

Although the prosecution of the above criminal offence is not very common in practice, a general recommendation is that, once a suspicion of a potential misconduct arises, it should be properly investigated and evidenced, in order to reasonably determine all relevant facts surrounding the case. This especially since intentional false reporting of a criminal offence is also incriminating under Serbian law and there is no clear legal standard under Serbian law defining when a person "knows" that the criminal offence has been committed.

- ? Would cooperation and voluntary self-disclosure be taken into account by the law enforcement authorities in relation to both individual and corporate liability?**

Self-reporting does not guarantee exclusion of either individual or corporate criminal liability, although it may lead to such an outcome in certain cases. If the self-reporting does not exclude the existence of criminal liability, it should still be considered a beneficial occurrence while determining the punishment by the competent court.

Under the Corporate Criminal Liability Law, legal entity may (i.e. this is not a guarantee) be exempted from criminal punishment if it (i) reveals and reports a criminal offence before it finds out that criminal proceedings were instigated, and (ii) voluntarily and without delay remedies damaging consequences or returns unlawful benefits which it received.

In respect of the individual criminal liability, the court may release the defendant from criminal punishment for criminal offences subject to imprisonment of up to five years, if the perpetrator, after the execution of the criminal offence, and prior to him/her becoming aware that his/her criminal offence was revealed, remedies the consequences of the offence or reimburses the damages arising therefrom.

In addition, the public prosecutor may drop the criminal charges with respect to:

- criminal offences subject to a monetary fine or imprisonment of up to five years, if the defendant accepts one or several of specific obligations ordered by the public prosecutor (e.g. removing damaging consequences, donating money to a humanitarian cause, performing work in the public interest, etc.); or
- criminal offences subject to imprisonment of up to three years, if the defendant, due to obvious remorse, prevented the occurrence of damages or if he/she fully reimbursed such damages, and the public prosecutor deems that, based on the circumstances of the case, imposing a criminal punishment would not be righteous.



## PLANNING AND STRUCTURING INTERNAL INVESTIGATIONS

### ? **How should internal investigations be structured? When should an internal investigation be conducted by an attorney?**

The company should have effective internal policies established that deal with the prevention and revealing of potential misconduct.

Such policies should primarily be focused on educating the company's management and employees on acceptable behaviour and should clearly outline the actions and measures necessary for avoiding the occurrence of potentially detrimental situations. Training sessions should also be organized by compliance officers in order to acquaint the relevant persons within the company with applicable rules.

On the other hand, the internal policies should also include the possibility of performing a specific process, i.e. the internal investigation, aimed at revealing the existence of potential misconduct, with a preliminary outline of rights and obligations of (i) the company (e.g. to collect, process and control employee information, organize interviews, request return of business laptops and inspect employees' business emails, etc.), and (ii) its employees (e.g. to participate in the investigation process, to receive basic information on the reasons for the conduct of the investigation, to request their privacy to be respected where there is no prevailing legitimate interest of the company, etc.).

Whenever there is a risk that a criminal offence may have been committed or whenever the inspection of employees' communication needs to be performed, it is recommended that an external attorney specialized in the conduct of internal investigations be included in the process, as a legal counsel who will assist the company with the conduct of the internal investigation and, thereby, minimize the risk of violating the applicable legal procedures during the course of the investigation. If further advice is needed from specific service providers, such as forensic or accounting professionals, they may be recommended by the engaged external legal counsel and cooperate with him/her, so that the process is kept as efficient as possible.

## CONFIDENTIALITY AND LEGAL PRIVILEGE

### ? **Who can be protected by attorney-client privilege ("legal privilege")? Which information/data is and is not protected by legal privilege, and what (if any) are the exceptions from legal privilege?**

Legal privilege exists in Serbian law through the concept of an "attorney secret". The attorney is obliged, in accordance with Attorney Bar statutes and Codex on Professional Ethics, to keep as a professional secret all information that was conveyed to the attorney by the client, or which he/she became aware of in any other way during the course of the preparation, provision, or post-provision of legal services. The attorney needs to ensure that all persons employed in his/her office keep the secret as well. The attorney secret is unlimited timewise.

The above legal framework is protected in various procedural laws, e.g. civil, criminal, misdemeanour, administrative, etc. The exact mechanism of protection of the attorney secret and specific rights granted to attorneys in general, depend on each specific law; however, it is common for all these proceedings that the attorneys cannot be forced to reveal the facts which fall under the attorney secret.

The attorney secret encompasses not only information, but also the documents, case files and other written instruments, and the attorney's office as well. A search in an attorney's office may be ordered solely by the court regarding the exact case file, object or document, and must be done in the presence of an attorney appointed by the president of the Attorney Bar. Information and documents identified during the search, which are beyond the court's order, become inadmissible and cannot be used against the attorney's other clients.

**? Does legal privilege extend to documents created by attorneys after they are handed over to the client?**

No. The attorney secret is focused on protecting the attorney from being obliged to reveal information and/or findings that he/she came across in the course of his/her duties. Accordingly, such secrets do not encompass any documents and information handed over to the clients.

In light of the above, we note that engaging an external legal counsel who will assist the company with the conduct of the internal investigation is generally useful, since the report on identified findings arising from the internal investigation is provided to the company only once all the relevant facts and circumstance have been closely inspected and determined in the process.

**? Does legal privilege apply to in-house lawyers?**

No. Legal privilege does not extend to in-house lawyers (i.e. lawyers formally employed by a company).

**? Does legal privilege apply to other types of service providers?  
Can legal privilege be extended to them if they are subcontracted by attorneys?**

Other professions may also be subject to different confidentiality obligations, regulated under separate laws. However, this confidentiality framework is in principle more limited when compared to legal privilege, and generally does not allow for confidential information to be kept away from the competent authorities during criminal proceedings.

It is unlikely that the attorney secret protection rules may extend to persons sub-contracted by an attorney, unless these persons are formally employed by such an attorney. Still, the Codex on Professional Ethics adopted by the Serbian Attorney Bar requires that the attorney personally ensure that all the associates, officials, trainees and other persons engaged by the attorney during the representation of the client, are warned about the confidential nature of the attorney secret information.

## COLLECTING AND PROCESSING DATA AND DATA PRIVACY PROTECTION

**? How should the company ensure that evidence is properly collected?**

The company must determine what data is needed for the internal investigation and where it is. What means of communication are used (emails, apps, phones)? What devices do employees use to communicate? Is there any cloud or local share-drive? Is the cooperation of a local IT expert needed? Is there any solely-paper information? It is then essential to determine whether and to what extent the company can legally access and review the data. It is not unusual for employees to use apps that are encrypted or do not save content, and it is then very difficult to distinguish between the personal content of their communication from work content. A prior, comprehensive and clear internal directive providing the complete rules on communication, archiving and the use of company devices by employees on the one hand, and explicit information on how the company can review and collect these data on the other, is a cornerstone of any proper internal investigation.

The company should also issue a preservation notice to employees to ensure that potential evidence (and all data relevant for the matter being investigated) is preserved and not destroyed. The employees in question should sign or give confirmation that they are complying with the preservation notice, and this should be kept on the record.

**? What conditions must be met to allow investigators access to employees' emails/other records which potentially contain private information?  
Is the consent of the custodian necessary before data collection begins?**

Employee privacy is protected both by the Serbian Constitution and by the Serbian Personal Data Protection Law (modelled under GDPR).

Internal investigations must be conducted in such a way that the risks of breaching privacy laws are minimised. This must be assessed on a case-by-case basis since, generally, the greater the harm faced by the employer (e.g. a large-scale corruption scheme), the more intrusive investigative instruments might be considered proportional.

One-off targeted searches of emails/documents using selected key words should not be considered disproportionate if the employer is aiming to protect itself, its property and its reputation by helping to determine if employees may be in breach of their responsibilities. However, only work-related data is allowed to be processed. No private personal data can be subject to review and any processing of private personal data must be immediately stopped.

Employees' data processing can only take place on one of the lawful grounds specified by the Serbian Personal Data Protection Law. In the internal investigations, the most frequently used legal ground is a legitimate interest of the employer. However, the employer must delicately balance its own interests against the interests or fundamental rights of the employees (e.g. right to a private life and secrecy of communication) as a part of a legitimate interest assessment – LIA). This balancing exercise should be properly documented in the form of the balancing test. Every balancing test should include at least the information regarding the purpose of data processing, necessity of the data processing potential consequences of data processing – impact on data subjects, protective measures adopted; and outcome of the assessment.

A privacy impact assessment (PIA) is explicitly required under the Serbian Personal Data Protection Law if a type of processing is likely to pose a high risk to the privacy of natural persons (such as employees). PIA must be performed particularly if the processing involves the processing of sensitive information, the merging or combining of data which was gathered by various processes, or occurs systematically over a longer time-period and may affect decisions about data subjects which have a significant effect on their life (such as legal decisions). It must be always assessed whether PIA must be executed for purposes of the internal investigations.

The extent of the processing must be as strictly necessary to achieve the aim of the investigation, and there must be no less-invasive measures available. The information included in the investigation should be carefully selected prior to review and no private information should be accessed as part of the investigation. It is essential that the right key words are selected, and the reviewers are sufficiently trained.

An internal directive should inform employees that their data may be processed as part of any investigation. This must include, among other things, the legal basis and purposes of the data processing and the corresponding rights of the employee. Requiring consent of employees with their data processing during investigation cannot be recommended as the consent must be freely given (it is questionable if the criteria of "freely given" consent could be fulfilled in the employment relationship and can be withdrawn at any time.

**? Are there any restrictions in relation to cross-border transfers of data collected during an investigation?**

Any cross-border transfers of data collected during investigations to countries outside Serbia should be analysed, as such a transfer must be done in line with the Serbian Personal Data Protection Law. This further means that that this transfer will be permissible to a country, a part of territory or one or more sectors of determined activities within such a country and an international organization procuring an adequate level of protection of personal data (i.e. a country/part of territory/sector/organization that is included in the "List" maintained and published by the Serbian Government, or has entered into relevant bilateral agreement with Serbia). Otherwise, companies must ensure that the data will be adequately protected even after their transfer to a third country (i.e. country/part of territory/sector/organization that is not included in the above-stated "List"), by applying appropriate safeguards.

Available instruments include, for example, the standard data protection clauses adopted by the Serbian Data Protection Authority. In addition, where the data is transferred within the group companies, the relevant intra-group policies should be in place.

**? What should the company do once the internal investigation is finished?**

Once the internal investigation is finished, the data gathered and processed during the internal investigation must be erased, with only the most important findings stored for the purpose of confronting the employee with the findings or for potential court or administrative proceedings. Employees whose data were processed must be informed of such processing.

## INTERVIEWING EMPLOYEES

**? Does an employee have an obligation to actively participate in interviews organised by the counsel of the employer?  
Is an employee required to participate and cooperate in interviews?**

Yes. For an employee, this obligation may be inferred from the general obligation to prevent damages to the employer.

However, to ensure the legality of such interviews, these should take place within the working hours of employees and should be strictly connected to their work. Refusal to cooperate may be considered a breach of their employment duties.

**? Do employees have the right to receive minutes from the interview?**

Not by law, but such obligation may be imposed by the employer's internal enactment.

**? Do employees have the right to be informed of the outcome of the investigation?**

No, employees do not have to be informed of the outcome of interviews or the investigation.

## WHISTLEBLOWING

**? Is there any specific regulation relating to whistleblowers?  
If so, is there any obligation to react to whistleblowing/to have a system in place for reacting to whistleblowing?**

Yes, Serbia has had a Law on Protection of Whistleblowers in force since 2014.

Any employer with more than 10 employees must adopt a specific internal act, which regulates the whistleblowing procedure and must be available to all employees (e.g. via announcement boards, copies, intranet, etc.).

Moreover, the employer must inform all employees of their rights under the Law on Protection of Whistleblowers, and a specific person for receipt of whistleblowing reports must be appointed. Under the Whistleblowers Act, employers are obliged to act upon a whistleblower's report within 15 days and remedy the reported issue, in accordance with its authorizations.

The whistleblower must be protected from all harmful consequences and his/her identity must remain anonymous, if the whistleblower did not reveal it on his/her own initiative.

## CRIMINAL PROCEEDINGS AGAINST THE COMPANY

### ? Is there corporate criminal liability in the country?

Yes, Serbia has a Law on Liability of Legal Entities for Criminal Offences in force.

The liability of a company is based on the liability of its authorized person. An authorized person is broadly defined as a person within a legal entity that under a law, regulation or by other authorization performs management, supervision or other duties in the scope of the legal entity's business activity, as well as the person that actually performs such activities.

A legal entity shall be liable for (i) a criminal offence committed by its authorized person, within the scope of the activities and/or authorizations of the authorized person, with an intent to establish a gain for the legal entity; or (ii) a criminal offence carried out for the benefit of the legal entity, if the offence was committed by a natural person acting under the supervision and control of an authorized person within the company, if the offence resulted from the lack of required supervision or control by the authorized person.

While there is still no established case law confirming that having a compliance system would exculpate the company, it is obvious from the above provisions that the acts of supervisions and control of a company's authorized person(s) are crucial for evaluating the criminal liability of the company. Thus, the existence of such a compliance system serves an important role in the legal defence of the company.

In addition to the criminal liability, Serbian law also recognizes the liability of legal entities for misdemeanours (*prekršaji*) and commercial offences (*privredni prestupi*).

### ? Can individuals and companies both be prosecuted for the same misconduct (parallel prosecution)?

Yes, both the perpetrator and the company can be prosecuted.

### ? Can corporate criminal liability be avoided or mitigated?

As mentioned above, there is a possibility for the legal entity to be exempted from criminal punishment if it (i) reveals and reports a criminal offence before it finds out that criminal proceedings were instigated, and (ii) voluntarily and without delay remedies damaging consequences or returns unlawful benefits which it received.

On the other hand, since the existence of corporate criminal liability is closely related to the actions of a legal entity's authorized person(s), establishment of an effective compliance management system may also serve as an important element in the prevention of any potential misconduct by the legal entity's officers and/or employees. Further, existence of such compliance management system may potentially serve as a beneficial circumstance before the prosecution authorities.

### ? Can criminal proceedings be settled with the enforcement authorities, or through leniency programmes?

Public prosecution is authorized to execute settlement agreements with defendants focused on: (i) admission of guilt, (ii) testimony by an accomplice and (iii) testimony by a convicted person.

The common use of all the above settlement agreements is the possibility to negotiate with the public prosecution on the type, manner and scope of a criminal punishment. Admission of guilt is a necessary pre-condition for the execution of the above settlement agreements and these agreements cannot be offered to a person deemed to have been the instigator of an organized criminal group.

Moreover, all the above settlement agreements need to be confirmed by a competent court, before they are legally adopted.

On the other hand, we once again note that the public prosecutor may decide to drop the criminal charges with respect to, *inter alia*, criminal offences subject to a monetary fine or imprisonment of up to five years, if the defendant accepts one or several of specific obligations ordered by the public prosecutor, as well as with respect to criminal offences subject to imprisonment of up to three years, if the defendant, due to obvious remorse, prevented the occurrence of damages or if he/she fully reimbursed such damages, and the public prosecutor deems that, based on the circumstances of the case, imposing a criminal punishment would not be righteous.

## UPCOMING DEVELOPMENTS

Based on the latest reports of the Serbian Republic Public Prosecutor, prosecution of criminal offences against commerce, as well as prosecution of legal entities in Serbia in general, has still not reached the necessary levels of activity and specific remarks have been made to the end that this legal area needs to be further improved in practice.

Future education of acting public prosecutors, relevant personnel and other authorities (e.g. police departments, etc.) engaged in the prosecution of criminal offences related to the performance of commercial activities are expected in the forthcoming period, leading to an increased necessity for companies and other commercial entities to ensure their compliance with applicable regulations.

Moreover, there has recently been an increase in the instigation of misdemeanor and commercial offence proceedings against legal entities, before the competent courts, by various competent authorities in Serbia (e.g. Tax Authority, Customs Authority, Business Registers Agency, etc.) as a result of wrongful conduct by the management or employees, leading to potential significant fines and other legal consequences for the entities.

Accordingly, adoption of necessary internal policies, as well as the organization of proper education and internal trainings within companies is highly recommended, followed with performance of necessary internal investigations in situations in which potential issues need to be timely identified and remedied.

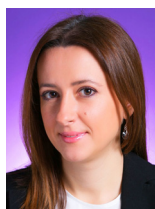
*This chapter was written by Aleksandar Ristic and Marijana Zejakovic in cooperation with Wolf Theiss.*



**ALEKSANDAR RISTIC**  
Senior Associate

**Wolf Theiss, Serbia**

T. +381 11 3302 926  
[aleksandar.ristic@wolftheiss.com](mailto:aleksandar.ristic@wolftheiss.com)



**MARIJANA ZEJAKOVIC**  
Senior Associate

**Wolf Theiss, Serbia**

T. +381 11 3302 945  
[marijana.zejakovic@wolftheiss.com](mailto:marijana.zejakovic@wolftheiss.com)



# SLOVAK REPUBLIC



## KEY TAKEAWAYS

- Companies may be held criminally liable for the misconduct of their employees and board members.
- Investigating misconduct is included in management's fiduciary duties and is a sign of a sound compliance management system which could help the company to release itself from corporate criminal liability.
- Internal directives regulating the processing of employees' data and investigation of misconduct are cornerstones of a diligent investigation.
- The concept of legal privilege is limited to the obligation of registered attorneys to preserve the confidentiality of information received from their clients.
- Suspicion of bribery may trigger the duty to report information to the authorities.
- Self-reporting or cooperation with prosecuting authorities does not have any automatic benefit for the company.

## OBLIGATION TO INVESTIGATE CRIMINAL MISCONDUCT INTERNALLY

### ? Are companies obliged to investigate misconduct internally?

The law does not explicitly lay down this obligation. However, diligently investigating misconduct is a fundamental part of any effective compliance management system and the prosecuting authorities will take into account how the company's compliance management system dealt with the misconduct, when determining criminal liability of the company.

The company may be released from criminal liability in relation to activities of its ordinary employees (however, not in relation to activities of members of statutory, supervisory or control bodies), which was attributed to the company because of failure to exercise due supervision and control over its employees. A criminal offence will not be attributed to a legal entity if the significance of not complying with these supervision and control obligations is minor when taking into account the business activities carried out by a legal entity, the form of committing the crime, its consequences and the circumstances under which the crime was committed.

### ? In which situations will a decision to internally investigate be necessary to prevent the civil or criminal liability of board members?

The fiduciary duties of corporate board members include ensuring and monitoring that the company behaves in compliance with all relevant regulations and that they exercise their duties with ordinary care. This means that the board members must not only set appropriate procedures to prevent misconduct, but also investigate any detected misconduct, which often includes an internal investigation. If a board member under a reasonable or founded suspicion of misconduct does not ensure that the suspicion is diligently investigated, and any revealed misconduct properly handled, then he or she risks being held liable for an intentional "breach of fiduciary duties". Moreover, if the suspicion of misconduct entails criminal wrongdoing, then he or she may be held liable for "failing to prevent a criminal wrongdoing" or may even be held co-liable for aiding and abetting the crime.

Failing to conduct an internal investigation could represent a breach of fiduciary duties of the board members, which could as a consequence make the board members liable for any damages to the company (e.g. penal or administrative fines, damages to third persons, loss of further profits, etc.) that may have been prevented.

- ? Is there a duty to report the outcome of the internal investigation or any information obtained during the internal investigation to enforcement authorities?  
If so, who is subject to the reporting duty and who is exempt?  
Are companies obliged to self-report?**

Generally, all individuals who obtain credible information that a specified crime<sup>1</sup> or one of the corruption criminal offences was committed or is being committed or prepared by another person have a legal obligation under the Slovak Criminal Code to report or prevent such crime. Failure to do so is a criminal offense. This does not apply to companies, which cannot be as legal entities held liable for failure to report or prevent these crimes under the Slovak Criminal Code and therefore do not have the associated duty to report or prevent the crimes. The question whether the members of statutory, supervisory or control bodies or regular employees can invoke the right against self-incrimination in relation to reporting or preventing crimes committed by the company has not yet been addressed by the courts and remains open.

- ? Would cooperation and voluntary self-disclosure be taken into account by the law enforcement authorities in relation to both individual and corporate liability?**

Both self-disclosure and cooperation are considered mitigating circumstances under the Criminal Code. Depending on the overall balance between mitigating and aggravating circumstances in a particular case, self-disclosure and cooperation may have an impact on the gravity of the sentence. This applies to both individual and corporate liability.

## PLANNING AND STRUCTURING INTERNAL INVESTIGATIONS

- ? How should internal investigations be structured?  
When should an internal investigation be conducted by an attorney?**

The company can implement an internal regulation that governs the process of dealing with (suspicion of) misconduct including internal investigation procedures as part of its compliance management system. The internal regulation should also specify the persons responsible for dealing with internal investigations (usually an independent compliance function) and also how the structure of the internal investigation should be decided, including a process for independent reporting.

Whenever there is a risk that reporting could be applicable, or will be applicable during the investigation, or if there is a risk of a police dawn raid, an attorney should be engaged as an external counsel to lead and conduct the investigation to minimise the risk of exposure to the reporting duty, and to maintain legal privilege over investigation outcomes. If specialised advice is needed from a particular specific service provider, for example, from forensic or accounting professionals, the provider should be subcontracted directly by the attorney and report directly to the attorney, so that the risk of exposure is minimised and legal privilege is maintained.

<sup>1</sup> Under Article 340 and 341 of the Slovak Criminal Code, the crimes that are to be reported or prevented include all crimes with a maximum prison sentence of at least ten years.

## CONFIDENTIALITY AND LEGAL PRIVILEGE

- ? Who can be protected by attorney-client privilege (“legal privilege”)?**  
**Which information/data is and is not protected by legal privilege, and what (if any) are the exceptions from legal privilege?**

The concept of legal or attorney-client privilege under Slovak law is not identical to the concept of attorney-client privilege in the US, where the attorneys have a confidentiality obligation based upon the constitutional rights to a fair trial. The “Attorney” legally defined as a lawyer registered with the Slovak Bar Association in accordance with Slovak law or a European attorney in accordance with EU law has a statutory duty of confidentiality. This duty requires attorneys to maintain as confidential all information acquired in connection with the provision of legal services. This does not only include the information known by the attorney, but also any information in material format (e.g. paper documents, data files or data disks), which the attorney received in relation to the performed mandate.

- ? Does legal privilege extend to documents created by attorneys after they are handed over to the client?**

No, the confidentiality obligation applies to the person of the attorney (including employees and subcontractors), rather than to the information or document itself. Therefore, any information or document that is protected when in the possession of the attorney might not be subject to the same level of protection when it is in the hands of the client or an unrelated third person. The prosecuting authorities often use this technique to order the company to hand over all documents they have received from the attorney including reports from the internal investigation and protocols from interviews. A recommended best practice is to structure the investigation together with the attorney, who is leading the investigation and who also subcontracts other third parties who participate in the investigation, if such participation is necessary.

It is essential that the investigation and its reporting lines/forms are structured so as to minimise the risk that the investigation report is taken by the authorities, e.g. during the dawn raid, and then used as an evidence in court proceedings.

- ? Does legal privilege apply to in-house lawyers?**

No. In-house counsels are not regarded as attorneys under Slovak law. They have the status of regular employees and are not bound by the statutory duty of confidentiality, and the communication is not protected by legal privilege.

- ? Does legal privilege apply to other types of service providers?**  
**Can legal privilege be extended to them if they are subcontracted by attorneys?**

Service providers (such as forensic or accounting professionals) can invoke legal privilege to the same extent as the attorney, only if they are subcontracted by the attorney in direct connection with the legal services provided by that specific attorney.

## COLLECTING AND PROCESSING DATA AND DATA PRIVACY PROTECTION

### ? How should the company ensure that evidence is properly collected?

The company must determine what data is needed for the purposes of the internal investigation and where the data is located. The following questions are fundamentally important for the effective execution of the data collection and processing: what means of communication are used (emails, apps, phones)? What devices do employees use to communicate? Is there any cloud or local share-drive? Is the cooperation of a local IT expert needed? Is there any solely-paper information?

It is then essential to determine whether and to what extent the company can legally access and review the data. It is not unusual for employees to use apps that are encrypted or do not save content, and it is then highly difficult to distinguish between the personal content of their communication from work content. The cornerstone of a diligent internal investigation is a comprehensive and clear internal directive, which provides complete rules on communication, archiving and the use of company devices by employees on the one hand, and explicit information on how the company can review and collect these data on the other hand.

The company should also issue a preservation notice to its employees, in order to ensure that potential evidence (and all data relevant for the matter investigated) is preserved and not destroyed. The employees in question should sign or give confirmation that they are complying with the preservation notice, and this should be kept on the record.

### ? What conditions must be met to allow investigators access to employees' emails/other records which potentially contain private information? Is the consent of the custodian necessary before data collection begins?

Employee privacy is protected both by Slovak labour law as well as under EU law (in particular GDPR).

Internal investigations must be conducted in such a way that the risks of breaching privacy laws are minimised. The aforementioned must be assessed on a case-by-case basis since, in general it applies that the greater the harm faced by the employer (e.g. large-scale corruption scheme), the more intrusive investigative instruments might be considered proportional.

For instance, one-off targeted searches of emails/documents using selected key words should not be considered disproportionately intrusive, if the employer is aiming to protect itself, its property and its reputation by helping to determine if employees may be in breach of their responsibilities. However, only work-related data may be processed for the purposes of the corporate investigation. No private personal data can be subject to the review and any processing of private personal data must be immediately ceased.

Employees' data processing can only be based on one of the lawful grounds specified by the GDPR. In the internal investigations, the most frequently used legal grounds for such processing is a legitimate interest of the employer. However, the employer must delicately balance its own interests against the interests or fundamental rights of the employees (e.g. right to a private life and secrecy of communication) as a part of legitimate interest assessment – LIA). This balancing exercise should be properly documented in the form of the balancing test. It shall be noted that every balancing test should include at least the information regarding the purpose of data processing, necessity of the data processing and the potential consequences of the data processing – impact on the data subjects, the protective measures adopted; and the outcome of the assessment.

A privacy impact assessment (PIA) is explicitly required under the GDPR, if a particular type of data processing is likely to pose a high risk to the privacy of natural persons (such as employees). In particular, the PIA must be performed if the data processing involves processing of sensitive information, merging or combining of data, which were gathered by various processes, or occurs systematically over a longer time-period and may lead to decisions that could have serious implication on the lives of the data subjects, (such as legal decisions). It must always be assessed whether the PIA shall be mandatorily executed for purposes of the internal investigations.

The extent of the data processing must be set only as necessary, in order to achieve the aim of the investigation. In addition, there must be no less-invasive measures available. The information included in the investigation should be carefully selected prior to the review and no private information should be accessed as a part of the investigation. It is essential that the right key words are selected, and the reviewers are sufficiently trained.

An internal directive should inform the employees that their data may be processed as part of any internal investigation. The said notification to the employees serves as the legal basis for the purposes of the data processing and the corresponding rights of the employee. If employees were never informed that their data might be processed for the purposes of harm prevention, for instance, the company would be in breach of this obligation. In addition, under Slovak labour law, the employer shall not intrude upon the privacy of an employee in the workplace by monitoring him/her or checking email sent from a work email address and delivered to such an address without giving notice in advance. An internal directive is not sufficient to cover this requirement and a notice needs to be served to the concerned employees.

**? Are there any restrictions in relation to cross-border transfers of data collected during an investigation?**

Strict conditions apply to cross-border transfers of data collected during investigations to outside of the EU. In particular, companies must ensure that the data will be adequately protected even after the transfer of the data to a third country. Suggested available instruments include binding corporate rules and standard data protection clauses adopted by the European Commission. In addition, where the data are transferred within the group companies, the relevant intra-group policies should be in place.

**? What should the company do once the internal investigation is finished?**

Once the internal investigation is finished, the data gathered and processed during the internal investigation must be erased, with only the most important findings stored for the purpose of confronting the employee with the findings or for potential court or administrative proceedings. Employees whose data was processed must be informed of such processing.

## **INTERVIEWING EMPLOYEES**

**? Does an employee have an obligation to actively participate in interviews organised by the counsel of the employer?  
Is an employee required to participate and cooperate in interviews?**

Employees instructed by the employer to cooperate during internal investigations must do so in accordance with their general obligations arising out of their employment duties (general obligation to prevent damage to their employer and loyalty obligation). To ensure their legality, interviews should take place within the working hours of employees and should be strictly connected to their work. Refusal to cooperate may be considered a breach of the employment duties.

**? Do employees have the right to receive minutes from the interview?**

No.

**? Do employees have the right to be informed of the outcome of the investigation?**

No, employees do not have to be informed of the outcome of interviews or the investigation.

## WHISTLEBLOWING

- ? Is there any specific regulation relating to whistleblowers?  
If so, is there any obligation to react to whistleblowing/to have a system in place for reacting to whistleblowing?**

The framework for whistleblowing in Slovakia is covered by the Whistleblowing Act, which regulates the conditions of provision of protection for the employees in regard to reporting of criminal actions and other forms of anti-social behaviour, and the rights and duties of the persons submitting the reports.

Employers with at least 50 employees are obliged to set up an internal system for handling reports of crimes and other anti-social activities (compliance hotline). This also includes the duty to maintain a registry of reports (for at least 3 years following the report). As part of the internal system, employers are obliged to appoint a responsible person (an employee or an external person), specifically to handle the reports. Accordingly, employees may report not only crimes, and administrative delicts but also other forms of unethical, discriminatory and anti-social behaviour.

Whistleblowers are protected during both the reporting and the investigation process. Employers cannot take any labour law related legal action against the whistleblowers without their prior consent, or without the approval of the Labour Inspectorate. Non-compliance with the Whistleblowing Act can result in fines of up to EUR 20,000 issued by the Labour Inspectorate.

## CRIMINAL PROCEEDINGS AGAINST THE COMPANY

- ? Is there corporate criminal liability in the country?**

Yes. A company is liable for a crime if it was committed by any of a broad range of personnel listed in the Act on Criminal Liability of Legal Persons<sup>2</sup> for the benefit of the company, on its behalf, as a part of its activities or through the company. Strict corporate criminal liability is applicable, which means that the criminal liability of a company depends solely on the actions and intention of the perpetrator, while remaining independent from and concurrent with the criminal liability of the perpetrator.

- ? Can individuals and companies both be prosecuted for the same misconduct (parallel prosecution)?**

Both the perpetrator and the company can be prosecuted independently, and the company may be prosecuted even if the perpetrator is acquitted. The criminal liability of a company passes to its legal successors.

- ? Can corporate criminal liability be avoided or mitigated?**

Under certain circumstances, a company can be released from criminal liability if it has implemented adequate measures that could have prevented a crime from being committed (in practice referred to as the compliance management system). This however applies only to cases where criminal offenses are attributed to the company due to activities of ordinary employees. In cases where criminal offenses are attributed to the company due to activities of members of statutory, supervisory or control bodies, the release from criminal liability based on compliance management system is not applicable. A criminal offence will not be attributed to a legal entity if the

2 Act No. 91/2016 Coll., On Criminal Liability of Legal Persons Section 4 (1) and 4 (2) of the Act on Criminal Liability of Legal Person includes the following: statutory bodies, members of the statutory bodies, persons in the controlling and supervisory functions, or other persons representing the legal persons or deciding on behalf of the legal person, and also ordinary employees in case of failure to exercise due supervision and control over such employees.

significance of not complying with the obligations to supervise and control the activities of ordinary employees is minor when taking into account the business activities carried out by a legal entity, the form of committing the crime, its consequences and the circumstances under which the crime was committed.

Each compliance management system should be evaluated in the light of the proportionality principle in relation to the organisational size, regulatory density, internationality and nature of business activities, risk profile and market environment of any given legal person. Most importantly, the compliance management system should have viable core elements: be preventive (able to dissuade and impede misconduct), capable of detecting any such misconduct and reactive to misconduct (disciplinary reactions or legal action, or it must learn from the misconduct). Finally, the compliance management system should be able to adopt the necessary adjustments and continuously be improved in according with the conducted investigations.

### **? Can criminal proceedings be settled with the enforcement authorities, or through leniency programmes?**

There is only a very limited practice of out-of-court settlements, particularly if compared to the U.S. settlement practice. Although some instruments are recognised by Slovak law, the out-of-court settlement system has essentially been based on prosecuting individuals.

An out-of-court settlement can be reached between the accused perpetrator and the aggrieved party. This settlement option is available only in the case of less severe offences<sup>3</sup> and cannot be concluded if the criminal offence resulted in death, in corruption offenses, and in cases of criminal prosecution of a public official or a foreign public official. The accused must (i) declare that he/she committed the act, for which he/she is being prosecuted, (ii) make compensation for the damages/injury caused, (iii) and deposit an adequate amount in a designated account for the purpose of protection and support of crime victims. The settlement must be approved by the prosecutor and lead to suspension of the criminal proceedings.

A plea agreement can be entered into between the perpetrator and the public prosecutor. The perpetrator must admit to his or her guilt and agree to sanctions. The plea agreement must be approved by the court.

Companies sentenced with a ban on commercial activity, a ban on participating in public tenders or a ban on subsidies can, after serving half of their sentence, ask the court to be paroled and ask for the rest of their sentence to be dropped if the company shows that serving the rest of the sentence is not necessary.

## **UPCOMING DEVELOPMENTS**

Initially, after the implementation of genuine corporate criminal liability in Slovakia in 2016, prosecuting authorities have acted hesitantly, and there have been only a very limited number of corporate criminal liability cases. However, the interest of authorities in this field has exponentially risen in recent years. What remains unresolved is a framework for out-of-court settlements, which is tailored to prosecuting individuals, and also the incentives for cooperation with the investigation. At present, the OECD and the International Bar Association are in the process of persuading national legislators to establish a predictable system and procedure of out-of-court settlements for companies, which currently have few incentives (if any) to cooperate and self-report.

---

3 Criminal offences for which a maximum term of imprisonment of five years is stipulated in the Criminal Code.

*This chapter was written by Jitka Logesova, Marko Ernek and Stanislav Bojnansky.*



**JITKA LOGESOVA**

Partner

**Wolf Theiss, Czech Republic**

T. +420 234 765 223

[jitka.logesova@wolftheiss.com](mailto:jitka.logesova@wolftheiss.com)



**MARKO ERNEK**

Senior Associate

**Wolf Theiss, Slovak Republic**

T. +421 2 591 012 38

[marko.erneka@wolftheiss.com](mailto:marko.erneka@wolftheiss.com)



**STANISLAV BOJNANSKY**

Associate

**Wolf Theiss, Slovak Republic**

T. +421 2 591 012 51

[stanislav.bojnansky@wolftheiss.com](mailto:stanislav.bojnansky@wolftheiss.com)





WOLF THEISS

**SLOVENIA**

## KEY TAKEAWAYS

- Companies can be held criminally liable for the misconduct of their employees and board members.
- Investigating misconduct is included in management's fiduciary duties and is a sign of a sound compliance management system.
- Internal policies regulating internal investigation processes and the processing of employees' data are the foundation of a proper investigation.
- Legal privilege is limited to registered attorneys.
- Reporting duties are restricted to the most serious offences.
- Self-reporting or cooperation with prosecuting authorities does not have any automatic benefit for the company but may impact the outcome of proceedings.

## OBLIGATION TO INVESTIGATE CRIMINAL MISCONDUCT INTERNALLY

### ? Are companies obliged to investigate misconduct internally?

Slovenian mandatory law does not expressly provide for the duty of companies to conduct internal investigations in relation to detected misconduct.

### ? In which situations will a decision to internally investigate be necessary to prevent the civil or criminal liability of board members?

In relation to civil liability, management and supervisory board members are ultimately responsible for the lawful conduct of the business of the company. They are bound to discharge their duties with the diligence of a conscientious and honest businessman. Failure to meet these obligations constitutes grounds for liability for damages of the management and supervisory board members.

Pursuant to the above general duties, management and supervisory board members are required to take proactive steps whenever they are informed or are otherwise aware of any (potential) illegalities or wrongdoings within the company that may result in any type of damages being incurred by the company. This duty is especially pronounced in cases where the illegalities or wrongdoings are or may be systemic in nature. In such cases, properly and demonstrably establishing all the relevant facts and underlying causes of the illegalities or wrongdoings may be essential in order to avoid civil liability for any damages incurred by the company. The conduct of an internal investigation (and subsequent steps taken pursuant with their findings) may thus in practice constitute an important or even decisive factor in the determination of whether or not management and supervisory board members have acted in compliance with the required standard of diligence.

In relation to criminal liability, white collar criminal offences (i.e. criminal offences against the economy or legal transactions pursuant to the Criminal Code) require that the criminal intent of the perpetrator be demonstrated. This means that any sort of negligence – including a negligent omission to investigate potential wrongdoings – should in principle not result in criminal liability for offences that have already been committed and where no action by the management board may influence or prevent the criminal offence.

Should however such an omission be intentional in relation to a specific criminal offence (i.e. the omission is intentionally aimed towards assisting the perpetrator), this may under certain circumstances constitute grounds for criminal liability of management and supervisory board members.

With regards to non-specific types of criminal offences, the liability of board members may be established when the conduct of an investigation and subsequent adoption of appropriate measures could have prevented the occurrence of a criminal offence (e.g. failure to investigate information regarding health and safety irregularities and adopt appropriate measures, resulting in death or injury).

**? Is there a duty to report the outcome of the internal investigation or any information obtained during the internal investigation to enforcement authorities?  
If so, who is subject to the reporting duty and who is exempt?  
Are companies obliged to self-report?**

Yes, in certain circumstances. There is a general requirement to report any criminal offence with a statutory minimum sentence of 15 years in prison. Failure to do so constitutes a criminal offence in itself. Spouses, common-law partners and close relatives are exempt from this duty, as well as defence counsels, doctors or priests of the perpetrator.

Additionally, there is a general requirement to report any criminal offence that is in progress and may be prevented if the offence in question carries a statutory minimum sentence of three years. Failure to do so also constitutes a criminal offence. Only spouses, common-law partners and close relatives are exempt from this duty.

Furthermore, there is an obligation in place for certain types of legal entities and natural persons (principally those involved in financial services, as well as attorneys and notaries) to report any suspicious transactions that raise money laundering concerns to the authorities.

**? Would cooperation and voluntary self-disclosure be taken into account by the law enforcement authorities in relation to both individual and corporate liability?**

With regard to corporate liability, cooperation and voluntary self-disclosure may constitute grounds for a remission or reduction in sentencing beyond mandatory minimums. Additionally, in such instances special discretion is awarded to the prosecutor who may choose not to prosecute when the sentence may be remitted entirely under the law. However, there are no publicly available data to determine whether this possibility is actually being used.

With regards to individual liability, the above discretion, as well as the possibility of remission or reduction of sentences beyond mandatory minimums, is more restricted, however it would probably be regarded as a mitigating circumstance at the very least.

## PLANNING AND STRUCTURING INTERNAL INVESTIGATIONS

**? How should internal investigations be structured?  
When should an internal investigation be conducted by an attorney?**

The company should have internal policies in place that govern the process of dealing with (even the suspicion of) misconduct, including internal investigation procedures as part of the compliance management system. It should specify the persons responsible for dealing with internal investigations (usually an independent compliance function) and how the structure of the internal investigation should be decided, including a process for independent reporting.

Whenever there is a risk that a reporting duty has arisen, or will arise during the investigation, or a dawn raid by the police is imminent, an attorney should be engaged as an external counsel to lead and conduct the investigation to minimize the risk of exposure to the reporting duty, and to maintain legal privilege over investigation products.

## **CONFIDENTIALITY AND LEGAL PRIVILEGE**

### **? Who can be protected by attorney-client privilege ("legal privilege")? Which information/data is and is not protected by legal privilege, and what (if any) are the exceptions from legal privilege?**

In general, attorneys-at-law, registered with the Bar, are bound by legal privilege pertaining to any facts that were made known to them in the course of the performance of their profession, if they are not obliged to reveal such information under applicable regulations. However, this is primarily an obligation of the attorneys, and is only partially reflected in legal protection or privileges in civil and criminal proceedings. Primarily, in both types of proceedings, attorneys may refuse testimony in relation to facts that they are obliged to keep as confidential.

In criminal proceedings, unless the attorney acts as a defence counsel, his/her premises may be searched for documents or information, but only in case it is not possible to obtain said documents or information through any other means. The search can only be conducted based on a court order, which needs to specify for which documents and information the search is to be conducted. A Bar representative must be present during the search. The Bar representative, as well as the attorney whose premises are the subject of a search, may file objections regarding documents seized, stating that they are not covered by the order. These documents are then immediately sealed and special procedures are in place for the examination of the objections by an independent judge.

If the attorney acts as a defence counsel in criminal proceedings, he/she cannot be called to testify in relation to the defendant, their premises cannot be searched for the purpose of obtaining documents or information and their client communications cannot be intercepted. This is an extension of the defendant's right to defence and privilege against self-incrimination and is absolute.

However, if any attorney-client communications, documents or other forms of information media are seized, intercepted or obtained from the company directly or through third parties, they are not covered by attorney client privilege.

### **? Does legal privilege extend to documents created by attorneys after they are handed over to the client?**

No, the confidentiality obligation is linked to the person of the attorney (and his or her employees and subcontractors), rather than to the information or document itself. Therefore, any information or documents that are protected when in the possession of the attorney is not protected when it is in the hands of the client or an unrelated third person.

It is therefore recommended that any sensitive information and documents be kept solely by the attorney engaged for the conduct of the internal investigation, and that the conduct of the investigation is itself structured so as to minimize the risk that large parts or the entirety of the materials, as well as the final product of the investigation, could be detected or seized without any advance warning by the authorities in case of any official proceedings.

### **? Does legal privilege apply to in-house lawyers?**

No. In-house counsel are not regarded as attorneys under Slovenian law. They have the status of regular employees and don't enjoy legal privilege.

**? Does legal privilege apply to other types of service providers?  
Can legal privilege be extended to them if they are subcontracted by attorneys?**

All service providers that have a statutory obligation to keep as confidential information they are provided with or come across in the performance of their profession (e.g. doctors, priests, bankers, psychologists, social workers, etc.) may refuse to testify in court or civil proceedings, unless statutory conditions for disclosure are met.

The legal privilege enjoyed by attorneys-at-law registered with the Bar is extended to any persons employed by these (i.e. employed in a law firm); however there is no precedence or direct statutory basis for the possibility of an extension of the attorney's legal privilege to third party service providers.

## COLLECTING AND PROCESSING DATA AND DATA PRIVACY PROTECTION

**? How should the company ensure that evidence is properly collected?**

The company should firstly establish what data may potentially be relevant in respect to the scope of a particular investigation, and all the places where such data may be stored (e.g. physical archives, company servers, employee work laptops or phones, external cloud services, etc.).

As a next step, the company should then determine if and to what extent each set of data may be gathered and accessed. Comprehensive and clear internal rules on communication, archiving, and the use of company devices by employees, as well as rules on access to such data may substantially facilitate any proper internal investigation.

The company should also issue a preservation notice to employees to ensure that potential evidence (and all data relevant for the matter investigated) is preserved and not destroyed, and obtain acknowledgement of such notification from the employees in question.

**? What conditions must be met to allow investigators access to employees' emails/other records which potentially contain private information?  
Is the consent of the custodian necessary before data collection begins?**

The review of employees' electronic communications and data stored or hosted on the employer's assets involves two separate legally-relevant facets:

- the processing of personal data of the employee and potential third parties (such as email addresses and traffic data) as regulated by the data protection laws, and
- the access and review of the substance of the communications as protected by the right to privacy and secrecy of communications.

While the relevant protections of privacy pursuant to both facets are very similar, they should nevertheless be considered separately in order to ensure that any such measures are deployed lawfully.

Principally, the employer cannot indiscriminately and routinely monitor and/or access employees' emails or other data. Such measures must be limited both in scope and to specific situations, where a clear aim of such measures to safeguard particular interests and rights of the employer (which enjoy a similar level of protection, as the rights of the employees) can be demonstrated. Further, such interests and rights of the employer must outweigh the interests and rights of the employees in each individual instance in order that such measures be deployed legally.

Such measures must be (i) appropriate, and (ii) necessary to achieve the aim, (iii) cannot be replaced by a less invasive measure, (iv) transparent, and (v) limited only to business/work related communications. The measure should affect only employees for which suspicion of a violation exists and the measure should cover only relevant

types of communication or data. The scope of the measures should be made transparent to employees prior to the start of the investigation. The most appropriate legal basis for the deployment of such measures is the legitimate interest of the employer. Such measures cannot be based on the consent of the employees.

The employer must delicately balance its own interests against the interests or fundamental rights of the employees. This balancing exercise should be properly documented in the form of the legitimate interest assessment (LIA). Every balancing test should include at least the information regarding the purpose of data processing, necessity of the data processing potential consequences of data processing - and impact on data subjects, protective measures adopted; and outcome of the assessment. Additionally, the employer should carry out a data protection impact assessment, which is explicitly required under the GDPR if a type of processing is likely to pose a high risk to the privacy of natural persons.

In the absence of (i) implemented clear and comprehensive policy regarding employee monitoring and (ii) determination of the investigation as a purpose of processing in the employee privacy policy, an internal directive should inform employees that their data may be processed as a part of any investigation. This must include, among other things, the legal basis and purposes of the data processing as well as the corresponding rights of the employee. If employees were never informed that their data might be processed for the purposes of harm prevention, for instance, the company would be in breach of this obligation.

**? Are there any restrictions in relation to cross-border transfers of data collected during an investigation?**

Strict conditions apply to cross-border transfers of data collected during investigations to the outside of the EU. In particular, companies must ensure that the data will be adequately protected even after their transfer to a third country. Available instruments include binding corporate rules and standard data protection clauses adopted by the European Commission. In addition, where the data is transferred within the group companies, intra-group policies should be in place.

**? What should the company do once the internal investigation is finished?**

Once the internal investigation is finished, the data gathered and processed during the internal investigation must be deleted as soon as the purpose for their collection has been fulfilled. In practice, this means that only key data and documents necessary for the safeguarding or exercise of the employer's rights may be retained, but only for the period necessary for this (e.g. for disciplinary measures against a particular employee, for potential court or administrative proceedings, etc.). Employees whose data was processed must be informed of this.

## **INTERVIEWING EMPLOYEES**

**? Does an employee have an obligation to actively participate in interviews organised by the counsel of the employer?  
Is an employee required to participate and cooperate in interviews?**

Employees may be ordered by the employer to cooperate during internal investigations (e.g. by attending an interview), pursuant to general provisions of employment law. Failure to comply with such an order may constitute a breach of their employment duties and may constitute grounds for disciplinary actions up to termination. To avoid unnecessary complications, interviews should preferably take place during the employees' normal working hours.

**? Do employees have the right to receive minutes from the interview?**

No.

**? Do employees have the right to be informed of the outcome of the investigation?**

No, employees do not have to be informed of the outcome of interviews or the investigation.

## WHISTLEBLOWING

**? Is there any specific regulation relating to whistleblowers?  
If so, is there any obligation to react to whistleblowing/to have a system in place for reacting to whistleblowing?**

There are specific regulations in place providing for a whistleblower's protection in cases of public sector corruption. A limited authority is vested in the Commission for the Prevention of Corruption – an independent body to which (public) corruption may be reported, investigates allegations of improprieties, and can provide assistance to whistleblowers – to enforce the protection of whistleblowers employed in private sector entities and to provide support to such whistleblowers towards their employers.

Apart from this, there is no comprehensive law that regulates the status, rights and protection of whistleblowers and corresponding obligations of private sector entities. Certain provisions of generally applicable legislation (e.g. the Criminal Code) contain specific provisions that offer legal protection for whistleblowing activities, while still other generally applicable provisions of mandatory law (i.e. the required diligence in the conduct of business pursuant to the Companies Act, the prohibition of retribution and discrimination and the corresponding duty to safeguard under the Employment Relationships Act) may trigger safeguarding obligations for management or supervisory bodies if they are confronted with or come across information on or from a whistleblower.

According to publicly available information, more comprehensive legislation regulating whistleblowers is in the early stages of preparation; however, none of its main points or contents have yet been disclosed to the public, and no timeline for its adoption and entry into force has been provided.

## CRIMINAL PROCEEDINGS AGAINST THE COMPANY

**? Is there corporate criminal liability in the country?**

Yes, companies may be held liable for criminal offences, committed in the name or for the benefit of a company, if one of the following conditions is fulfilled:

- the criminal offence constitutes the execution of an illegal corporate decision, order or approval of its management or supervisory bodies; or
- its management or supervisory bodies influenced the perpetrator or enabled the perpetrator to commit the criminal offence; or
- it is the recipient of illegal proceeds or objects created through a criminal offence; or
- if management or supervisory bodies failed in their duty to supervise the legality of the actions of their subordinate employees.



It should be noted (especially in relation to point (c) above) that pursuant to the Slovenian corporate criminal liability concept, corporate liability is not objective by nature, but requires some form of "participation", culpability or at the very least awareness on the part of the management or supervisory bodies. Merely having benefitted in some way from a criminal offence is by itself not enough to establish corporate criminal liability.

**? Can individuals and companies both be prosecuted for the same misconduct (parallel prosecution)?**

Yes, both the perpetrator and the company may be prosecuted for the same misconduct (both for criminal as well as administrative offences).

With regard to criminal offences, the law provides that proceedings against the company and perpetrator should be conducted jointly; however, the liability of the perpetrator and the company are severable, meaning that the company can be found liable even if the perpetrator is not liable or was coerced by the company.

**? Can corporate criminal liability be avoided or mitigated?**

The Liability of Legal Persons for Criminal Offences Act<sup>1</sup> does not provide for any mechanism pursuant to which a company implicated in a criminal offence can automatically avoid prosecution.

If the management or supervisory bodies of the company reports the perpetrator of the criminal offence before the criminal offence was detected by the authorities, the sentence for the company may be reduced. If simultaneously the company returns any undue benefits or repays any damages or reports or provides data on other implicated companies, the sentence may be remitted in its entirety. Additionally, according to general rules of criminal law, whenever the conditions for the remission of a sentence are met, state prosecutors may decide not to prosecute.

Separately, the state prosecutor may decide not to start proceedings against the legal entity, if the circumstances of the case indicate that this would not be prudent due to (i) the insignificant participation of the legal entity in the offence, (ii) the legal entity not having any assets or such assets would be insufficient to cover the costs of the proceedings, (iii) the legal entity being in bankruptcy proceedings or (iv) the perpetrator being the sole owner of the legal entity.

It should be noted, however, that all the above possibilities are at the discretion of the competent authorities, who are not obliged to reduce or remit sentences, or not to prosecute, even if all the required conditions are met by the company. Further, it is very difficult (if not impossible) for the management of supervisory bodies to be certain as to whether or not a particular criminal offence was detected by the authorities, since initial parts of criminal investigations are classified as confidential by law, and no information can be obtained in this respect from competent authorities.

**? Can criminal proceedings be settled with the enforcement authorities, or through leniency programmes?**

Criminal law in general provides the option to negotiate a plea agreement, whereby the company and the state prosecution conclude an agreement on the admission of guilt, and determine the sentence which is to be imposed. However, such an agreement must be confirmed by the court and can only be concluded when criminal court proceedings have been initiated.

---

1 Slo. *Zakon o odgovornosti pravnih oseb za kazniva dejanja (ZOPOKD)*, OG RS no. 98/04, as amended.

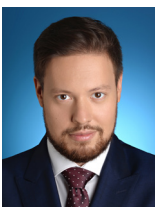
Criminal law generally also provides the state prosecution with the option to suspend or drop charges before formal court proceedings have been initiated in instances where the perpetrator is prepared to cooperate and perform certain actions or address the consequences of the criminal offence.

However, all the above possibilities are at the discretion of the prosecution, which is not obliged to deploy them in any particular instance.

## UPCOMING DEVELOPMENTS

More comprehensive legislation regulating whistleblowers may be expected at some point; it is likely that it will mostly follow established models in neighbouring countries and general provisions regarding whistleblowers of EU law. In light of the aforementioned, companies can and should start considering appropriate internal policies that can quickly be adapted to the minor particulars of upcoming local legislation.

*This chapter was written by Simon Tecco.*



**SIMON TECCO**  
Senior Associate

**Wolf Theiss, Slovenia**

T. +386 1 438 00 37  
[simon.tecco@wolftheiss.com](mailto:simon.tecco@wolftheiss.com)



UKRAINE

## KEY TAKEAWAYS

- Companies may be held criminally liable for the misconduct of their employees and board members.
- Investigating misconduct is included in management's fiduciary duties and is a sign of a sound compliance management system.
- Internal investigations are not well-regulated by the law, and the procedure for conducting them should be based primarily on the internal compliance management system of the company.
- Compliance with personal data protection laws is one of the foundations of a proper internal investigation.
- Internal directives regulating the processing of employees' data and the investigation of misconduct are cornerstones of a proper investigation.
- The concept of legal privilege is limited to the obligation of registered attorneys to preserve the confidentiality of information received from their clients, with whom the lawyers have formal client-attorney agreements.
- Self-reporting or cooperation with prosecuting authorities may have a benefit for the company.

## OBLIGATION TO INVESTIGATE CRIMINAL MISCONDUCT INTERNALLY

### ? Are companies obliged to investigate misconduct internally?

The law does not explicitly lay down this obligation and generally, a company failing to investigate misconduct would not be liable for it. On the other hand, if the company fails to report a criminal offence, particularly if the criminal offence is evident or obvious, the executives (and the company) of the company may be brought to criminal liability for such failure to act.

### ? In which situations will a decision to internally investigate be necessary to prevent the civil or criminal liability of board members?

Company executives (board members, directors, etc.) may be held liable in case their actions or inaction results in losses for the company. Therefore, if it is proven that in a specific situation it would have been reasonable and expedient to hold an internal investigation, but the company executives have not done so, they may be held liable for their passivity.

If there are clear indications of violations in a company and no investigation is conducted even though such an investigation is within the executive's competence, in a severe case (i.e. if the resulting harm amounts to ca. EUR 3,440 or more) the executive could be held criminally liable for "neglect of duty".

- ? Is there a duty to report the outcome of the internal investigation or any information obtained during the internal investigation to enforcement authorities?  
If so, who is subject to the reporting duty and who is exempt?  
Are companies obliged to self-report?**

There is a risk that if the executives of the company do not report a discovered crime, this may be qualified as covering up the crime. It is therefore recommended to carefully consider each case and get advice on the recommended course of action.

- ? Would cooperation and voluntary self-disclosure be taken into account by the law enforcement authorities in relation to both individual and corporate liability?**

Yes. Cooperation and voluntary self-disclosure are regarded by the Criminal Code as mitigating circumstances (possibly resulting in a less severe penalty or release from criminal liability). However, there is no standardized practice or guidelines in terms of fine amounts.

## PLANNING AND STRUCTURING INTERNAL INVESTIGATIONS

- ? How should internal investigations be structured?  
When should an internal investigation be conducted by an attorney?**

As internal investigations are not regulated by law, structuring of the investigation and involvement of external advisors should be decided on a case-by-case basis depending on the situation at hand. Usually, companies involve external advisors in case (i) they have no internal security departments or employees vested with the relevant authority, or (ii) there are reasons to believe that the internal security/compliance department (or official) have been involved in the misconduct.

## CONFIDENTIALITY AND LEGAL PRIVILEGE

- ? Who can be protected by attorney-client privilege ("legal privilege")?  
Which information/data is and is not protected by legal privilege, and  
what (if any) are the exceptions from legal privilege?**

Legal privilege extends to individual attorneys (lawyers admitted to the Ukrainian Bar), attorney's offices, persons employed by an attorney or attorney's office (assistants, trainees, etc.) and applies to:

- any information which has come to the attention of the attorney/attorney's office or persons employed by the attorney/attorney's office during the provision of legal services;
- communications, correspondence that passes between an attorney, assistant attorney or trainee and the client during the provision of legal services;
- the content of advice, consultations, explanations, documents, data, materials, belongings, information that was prepared, collected, received by an attorney, assistant attorney or trainee during the provision of legal services;

**? Does legal privilege extend to documents created by attorneys after they are handed over to the client?**

No. Legal privilege extends only to the documents that are kept by an attorney/attorney's offices, persons employed by an attorney or attorney's office. Thus, if a client intends for a document to be subject to attorney's privilege, such documents should be kept by the attorney (attorney's office).

**? Does legal privilege apply to in-house lawyers?**

There is no specific privilege for in-house lawyers. However, in-house lawyers are subject to general proprietary information protection mechanisms provided by Ukrainian law. As a matter of practice, in-house lawyers who are certified attorneys (advocates) may conclude an agreement based on which legal privilege will apply to their relationship with their employer.

**? Does legal privilege apply to other types of service providers?  
Can legal privilege be extended to them if they are subcontracted by attorneys?**

Legal privilege extends to attorney/attorney's offices, persons employed by an attorney or attorney's office (assistants, trainees, etc.).

## **COLLECTING AND PROCESSING DATA AND DATA PRIVACY PROTECTION**

**? How should the company ensure that evidence is properly collected?**

Ukrainian law does not provide for any specific requirements applicable to collection of evidence during an internal investigation or other private action. Thus, while collecting evidence the company should comply with general provisions of Ukrainian law on protection of personal data as well as privacy of information about an individual, companies' confidential information, etc.

This means, inter alia, that before collecting evidence the company should receive clear written consent from an employee to process his/her personal data. The employee should be informed about his/her lawful rights, the purpose and content of the collected data, potential transfers of data to third parties, etc. Further, the company should receive an employee's consent for (i) making video/audio footage featuring such an employee, (ii) access to his/her correspondence, etc. Because collecting such evidence is not allowed unless the company obtained the consent of the employee or the data used is not anonymized, it is highly recommended to either obtain such written consent when the employee commences his/her employment or anonymize the collected personal data to the extent possible.

Additionally, special rules apply to collecting information/documents that are regarded as containing banking or state secrets, etc.

**? What conditions must be met to allow investigators access to employees' emails/other records which potentially contain private information?  
Is the consent of the custodian necessary before data collection begins?**

Electronic messages sent via company email accounts are subject to the general privacy rights of correspondence of any individual. The correspondence can only be used with the consent of the message originator and its recipients. If the correspondence relates to the private life of an individual, its usage also requires the consent of such an individual.

Therefore, in practice, the use of corporate email accounts should be restricted to correspondence carried out in the employee's professional roles, or the employee should confirm and agree not to use corporate email for personal purposes, and thus the employer should not require consent for access to corporate email accounts used by employees.

The employer may also have access to email/communication of its employees based on internal policies (and/or relevant provisions in the employment agreement). The employees should be made familiar with any such policy and a record of this should be documented. Cross-border personal data transfer may require consent of the data subject (i.e. the relevant employee).

**? Are there any restrictions in relation to cross-border transfers of data collected during an investigation?**

Ukrainian legislation establishes limitations on cross-border transfer of personal data. Such transfers are possible only if the foreign state where the data recipient is located ensures a proper level of personal data protection.

Countries that belong to the European Economic Area and signatories to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data are considered to be states eligible for cross-border transfer. Additionally, the Government may approve the list of such qualifying states.

**? What should the company do once the internal investigation is finished?**

This is not clearly regulated by the law. Therefore, the course of action would depend on the circumstances of each individual case. The company may take internal remedial or punitive measures against employees involved in wrongful actions based on its internal policies – up to and including dismissal of the employees. The employees' misconduct may also be reported to law enforcement authorities as well as to relevant professional associations (if the employee is a member of a professional association).

## INTERVIEWING EMPLOYEES

**? Does an employee have an obligation to actively participate in interviews organised by the counsel of the employer?**

No, the employee does not generally have such an obligation, unless this obligation is provided for by internal regulations of the company.

**? Is an employee required to participate and cooperate in interviews?**

No. However, arguably, an employee may be required to participate in an interview if (i) an employment contract or internal regulation of the company provides for such duty of the employee, or (ii) if the employee is instructed by his/her superior to participate in the interview.

**? Do employees have the right to receive minutes from the interview?**

No. This is not regulated by the law.

**? Do employees have the right to be informed of the outcome of the investigation?**

No. This is not regulated by the law.



## **WHISTLEBLOWING**

- ? Is there any specific regulation relating to whistleblowers?  
If so, is there any obligation to react to whistleblowing/to have a system in place for reacting to whistleblowing?**

Yes, partially. Private companies are not per se required to have in place a system for reacting to whistleblowing. However, large state-owned companies and private companies participating in public procurement procedures with the value of ca. EUR 60k and more are required to develop and approve a separate internal anticorruption programme that should, inter alia, envisage the whistleblowing protection mechanism.

## **CRIMINAL PROCEEDINGS AGAINST THE COMPANY**

- ? Is there corporate criminal liability in the country?**

Corporate criminal liability does exist in Ukraine. The company may be held criminally liable when its executive or authorized representative (i) commits a crime on behalf and for the benefit of the company, (ii) fails to fulfil his/her obligations related to prevention of corruption, which resulted in the commission of a crime, etc. The Criminal Code of Ukraine defines the types of crimes that corporate entities (companies) may be held criminally liable for (e.g. money laundering, crimes that threaten national security and war crimes, violent crimes, etc.).

- ? Can individuals and companies both be prosecuted for the same misconduct (parallel prosecution)?**

Yes. Companies may be prosecuted in case of misconduct by their authorized representatives who are also held liable.

- ? Can corporate criminal liability be avoided or mitigated?**

Ukrainian law provides for a statutory exemption of companies from criminal liability due to expiration of the limitation period, which constitutes 3, 5, 10 and 15 years after the crime commission depending on the gravity of the criminal offence.

Additionally, since criminal liability of companies is closely related to criminal liability of its executives, any circumstance that works to decrease the official's liability (e.g. his/her actions aimed to mitigate harm, etc.) could also help mitigate liability for the company.

- ? Can criminal proceedings be settled with the enforcement authorities, or through leniency programmes?**

No. Criminal proceedings with respect to companies may not be settled with the authorities.

**UPCOMING DEVELOPMENTS**

Even though no specific legislation concerning internal investigations has been enacted in Ukraine yet, the number of internal investigations is increasing. For example, the dismissal of the Vice-President of the state-owned Ukrtransgaz in August 2017 was a result of an internal investigation. Reportedly, Privatbank, the largest Ukrainian bank, has also recently conducted an internal investigation related to inconsistencies in its audit and risk assessment results. Finally, investigations relating to FCPA violations have also been recently conducted at Ukrainian subsidiaries of global companies (Teva, IBM, etc.).

Given that, Ukrainian companies are now being encouraged and urged to establish their own internal rules and regulations on internal investigations aimed at tackling internal corruption and employee wrongdoing. This should help prevent any corruption-related and other charges against the company, its officials and employees.

*This chapter was written by Sergii Zheka and Iryna Orishko.*



**SERGII ZHEKA**  
Senior Associate

**Wolf Theiss, Ukraine**

T. +38 044 3 777559  
[sergii.zheka@wolftheiss.com](mailto:sergii.zheka@wolftheiss.com)



**IRYNA ORISHKO**  
Associate

**Wolf Theiss, Ukraine**

T. +38 044 3 777554  
[iryna.orishko@wolftheiss.com](mailto:iryna.orishko@wolftheiss.com)

## OUR OFFICES

**ALBANIA**

Murat Toptani Street  
AL - 1001 Tirana  
T. +355 4 227 45 21  
E. [tirana@wolftheiss.com](mailto:tirana@wolftheiss.com)

**AUSTRIA**

Schubertring 6  
A - 1010 Vienna  
T. +43 1 515 10  
E. [wien@wolftheiss.com](mailto:wien@wolftheiss.com)

**BOSNIA AND HERZEGOVINA**

Zmaja od Bosne 7  
BiH - 71 000 Sarajevo  
T. + 387 33 953 444  
E. [sarajevo@wolftheiss.com](mailto:sarajevo@wolftheiss.com)

**BULGARIA**

55 Nikola Vaptsarov Blvd.  
BG - 1407 Sofia  
T. +359 2 861 37 00  
E. [sofia@wolftheiss.com](mailto:sofia@wolftheiss.com)

**CROATIA**

Ivana Lučića 2a/19  
HR - 10 000 Zagreb  
T. +385 1 4925 400  
E. [zagreb@wolftheiss.com](mailto:zagreb@wolftheiss.com)

**CZECH REPUBLIC**

Pobřežní 12  
CZ - 186 00 Praha 8  
T. +420 234 765 111  
E. [praaha@wolftheiss.com](mailto:praha@wolftheiss.com)

**HUNGARY**

Kálvin tér 12-13  
H - 1085 Budapest  
T. +36 1 484 88 00  
E. [budapest@wolftheiss.com](mailto:budapest@wolftheiss.com)

**POLAND**

ul. Mokotowska 49  
PL - 00-542 Warszawa  
T. +48 22 3788 900  
E. [warszawa@wolftheiss.com](mailto:warszawa@wolftheiss.com)

**ROMANIA**

4 Vasile Alecsandri Street  
RO - 010639 Bucharest  
T. +40 21 3088 100  
E. [bucuresti@wolftheiss.com](mailto:bucuresti@wolftheiss.com)

**SERBIA**

Bulevar Mihajla Pupina 6/18  
SRB - 11000 Novi Beograd  
T. +381 11 330 29 00  
E. [beograd@wolftheiss.com](mailto:beograd@wolftheiss.com)

**SLOVAK REPUBLIC**

Aupark Tower, Einsteinova 24  
SK - 851 01 Bratislava  
T. +421 2 591 012 40  
E. [bratislava@wolftheiss.com](mailto:bratislava@wolftheiss.com)

**SLOVENIA**

Bleiweisova cesta 30  
SI - 1000 Ljubljana  
T. +386 1 438 00 00  
E. [ljublana@wolftheiss.com](mailto:ljubljana@wolftheiss.com)

**UKRAINE**

5A/10, Ihorivska Sk.  
UA - 04070 Kyiv  
T. +380 44 3777 500  
E. [kiev@wolftheiss.com](mailto:kiev@wolftheiss.com)

**WOLF THEISS** is one of the largest and most respected law firms in Central, Eastern and Southeastern Europe (CEE/SEE). We opened our first office in Vienna over 60 years ago. Our team now brings together over 340 lawyers from a diverse range of backgrounds, working in offices in 13 countries throughout the CEE/SEE region. During that time, we have worked on many cases that have broken new ground.

We concentrate our energies on a unique part of the world: the complex, fast-moving markets of the CEE/SEE region. This is a fascinating area, influenced by a variety of cultural, political and economic trends. We enjoy analysing and reflecting on those changes, drawing on our experiences, and working on a wide range of domestic and cross-border cases.