大成 DENTONS

Whistleblowing Insights

December 2019

Part 1
Designing an internal whistleblowing system

The issue of whistleblowing is drawing more and more attention. The media regularly reports on whistleblowers who have reported legal violations in politics and business. The topic has now moved onto the legislator's agenda in several countries. The different national regulations range from whistleblower protection regulations to requirements for reporting channels. In October 2019, the European Union adopted a new directive to protect people reporting on breaches of EU law. The aim of the directive is to set minimum standards for whistleblowing protection in Europe.

The subject is also gaining in importance for non-EU Member States: The International Standard Organization ("ISO") is planning to issue Standard 37002 at the end of 2021, which will establish guidelines for whistleblowing management systems.

With the arrival of the EU directive and the ISO standard, companies face within two uncertainty with regard to the requirements for internal reporting channels. Who is obliged to implement a reporting channel and how must such a channel be designed?

Dr. Gabriele Haas and Partner Carolina Muñoz give an overview of the expected changes from the EU Directive and the ISO standard respectively. Based on their years of experience with whistleblower systems, Partners Diego Pol and Dr. Rainer Markfort offer insights into common problems in implementing internal reporting channels. In this context, Dr. Jan Scharfenberg and Sebastian von Haldenwang discuss the data protection requirements when implementing such a channel. Partner Judith Aron presents what has to be taken into account in an internal investigation following a whistleblower report. The second part of our guide looks at different national approaches to whistleblowing. For more detail on individual countries please consult our comparative database **here**.

The new European Directive for the protection of whistleblowers

In many societies whistleblowers are regarded as traitors – sometimes for historical reasons, sometimes because the motives of whistleblowers are not always purely altruistic. Irrespective of the individual motives and to the extent that no criminal defamations happen, the protection of whistleblowers is necessary. Without safeguards against retaliation and protection of their identity, whistleblowers would be afraid to step forward and, as a result, serious compliance breaches would likely remain undetected.

In October 2019 the European Parliament adopted the Directive on the protection of persons reporting on breaches of EU law ("Whistleblowing Directive"). EU member states must implement the Whistleblowing Directive into national law by 17th Dec 2021. Only after being implemented into national law will its content be binding. At the time of the Whistleblowing Directive's publication, 10 out of 28 member states already had explicit national provisions for the protection of whistleblowers, namely France, Hungary, Ireland, Italy, Lithuania, Malta, Netherlands, Slovakia, Sweden, and the United Kingdom. For more detail on the directive click here.

The Whistleblowing Directive covers actual or potential violations of EU Laws in areas such as public procurement, prevention of money laundering and terrorist financing, product safety, protection of the environment, public health, protection of privacy and personal data and security of network and information systems, competition and state aid, and tax avoidance. However, when implementing their national regime, member states are encouraged

to protect whistleblowers in a comprehensive way, not only for violations of EU Law, but for all relevant compliance incidents, including fraud and corruption.

The law protects persons with a direct work-related link: this includes present and former employees, new hires, members of the administrative, management or supervisory board, personnel of contractors, subcontractors and suppliers, and legal entities that the reporting person owns, works for or is otherwise connected with in a work-related context. It also applies to third parties related to the reporting person. These persons enjoy immunity from liability for reporting information or submitting documents that they lawfully acquired or obtained access to.

After intense discussions during the legislative process, whistleblowers were given the right to publicly disclose information on breaches if the internal reporting or external reporting to the competent authority does not lead to appropriate action, or if they have reasonable grounds to believe that the external reporting is not appropriate. This might occur in cases where there is a low prospect of the breach being effectively addressed or in cases of an emergency situation or a risk of irreversible danger.

Member states are free to decide whether they implement an obligation to process anonymous reports. Regardless of their decision, anonymous whistleblowers shall always be protected to the same extent as non-anonymous whistleblowers. Recognizing the danger of direct and indirect retaliation, the EU stipulates that the whistleblower's identity cannot be disclosed beyond authorized and dedicated staff members without the explicit consent of the whistleblower or if required by law. In any case, the whistleblower, generally, should be informed about the disclosure of his/her identity. The Whistleblowing Directive foresees that organizations will keep records of each report received but only for as long as necessary and proportionate. However, all personal data collected that is not relevant for the handling of a specific case must be deleted without undue delay.

Balancing these conditions is already challenging enough when a clear breach of law has been reported but even more so in cases where it is not immediately clear if the law has been broken.

The Whistleblowing Directive asks member states to take measures to protect whistleblowers who have reasonable grounds to believe that the information they are reporting is true at the time of reporting. Whistleblowers shall not incur any liability in respect to the acquisition of or access to the relevant information, as long they obtained that information legally. It will be interesting to see how this fits together with the national provision on the protection of business secrets.

To protect whistleblowers the Whistleblowing Directive also implements the principle of reverse burden of proof in case of disciplinary measures.

While the protection of whistleblowers and their immunity from liability is very important to boost compliance, member states are likewise asked to impose penalties and compensating damages on the whistleblower if it is established that the whistleblower knowingly made false reports. Whether this provision effectively balances the rights of the whistleblowers with those of persons targeted by false accusations remains to be seen. Balancing the rights of whistleblowers and those of employees and others who are target of defamation remains challenging. Internal and external investigations must always be handled with the greatest care and the principle of "innocent until proven guilty".

ISO Standard: Whistleblowing Management System

The new ISO standard 37002 (scheduled for completion by the end of 2021) is expected to provide guidelines for developing and implementing an effective and responsive whistleblowing management system. It may represent a useful tool for organizations of all types and sizes – public or private companies in all industry sectors – seeking not only to improve the overall management of their whistleblowing policies and procedures but also to comply with local or international whistleblower legislation.

This standard will adopt the high-level structure developed by the International Standardization Organization to improve alignment among its international standards for management systems. It is intended to be adaptable and suitable to enhance the whistleblowing-related requirements in other management systems (e.g. ISO 37001 Anti-bribery Management System, ISO 19600 Compliance Management System, soon to be replaced by ISO 37301).

Based on the principles of trust, impartiality and protection, ISO 37002 guides organizations in managing the full whistleblowing cycle, namely:

a. Receiving reports of wrongdoing;

b. Assessing reports of wrongdoing;

c. Addressing reports of wrongdoing; and

d. Concluding whistleblowing cases.

As a highlight, some of the potential benefits for organizations that adopt a robust and effective whistleblowing management system are included in the standard:

I. Promoting ethical and legal practices;

II. Conforming to society, markets, regulators, the organization's owners and other stakeholders, and that the organization has all-encompassing governance practices;

III. Ensuring compliance with the organization's internal control systems; and

IV. Attracting and retaining personnel devoted to the organization's values and culture.

Implementation of whistleblower systems

In principle, a whistleblower system may be based on written reports by letter, fax or e-mail or verbal reports by telephone or in a personal conversation. However, due to data protection regulations, in practice it is advisable to implement an online system whereby the user acknowledges having read the privacy notice before he/she provides any personal data.

If local law allows it, organizations may consider using a third party to manage the whistleblowing system on its behalf. On the other hand, in some jurisdictions applicable law requires the compliance officer or compliance committee to manage the internal reporting channel or at least be somehow involved in the management of the complaints received. This may prove tricky in multinationals that centralize all complaints concerning its subsidiaries, using regional or global whistleblowing channels.

Once implemented, it is paramount that the organization ensures that all personnel are aware of the existence of the whistleblowing system and of their rights and protections under it.

Whistleblowing and data protection issues

Most countries do not have specific whistleblower laws, so general labor law and data protection regulations usually apply. This can pose several challenges for companies.

Many of these challenges stem from information rights. Data protection regulation often requires the persons whose personal data (i.e. data that can lead directly or indirectly to the identification of a natural person) is collected, used, transmitted or otherwise processed to be informed about this. Where a whistleblower's report concerns the behavior of a natural person, information requirements can pose a threat to the ongoing investigation.

Where the applicable data regulation offers no direct solution to this issue it is necessary to issue a general information notice to all employees before implementing a whistleblower system. The wording and implementation of such a notice is a complicated matter, often involving works councils or similar employee representations.

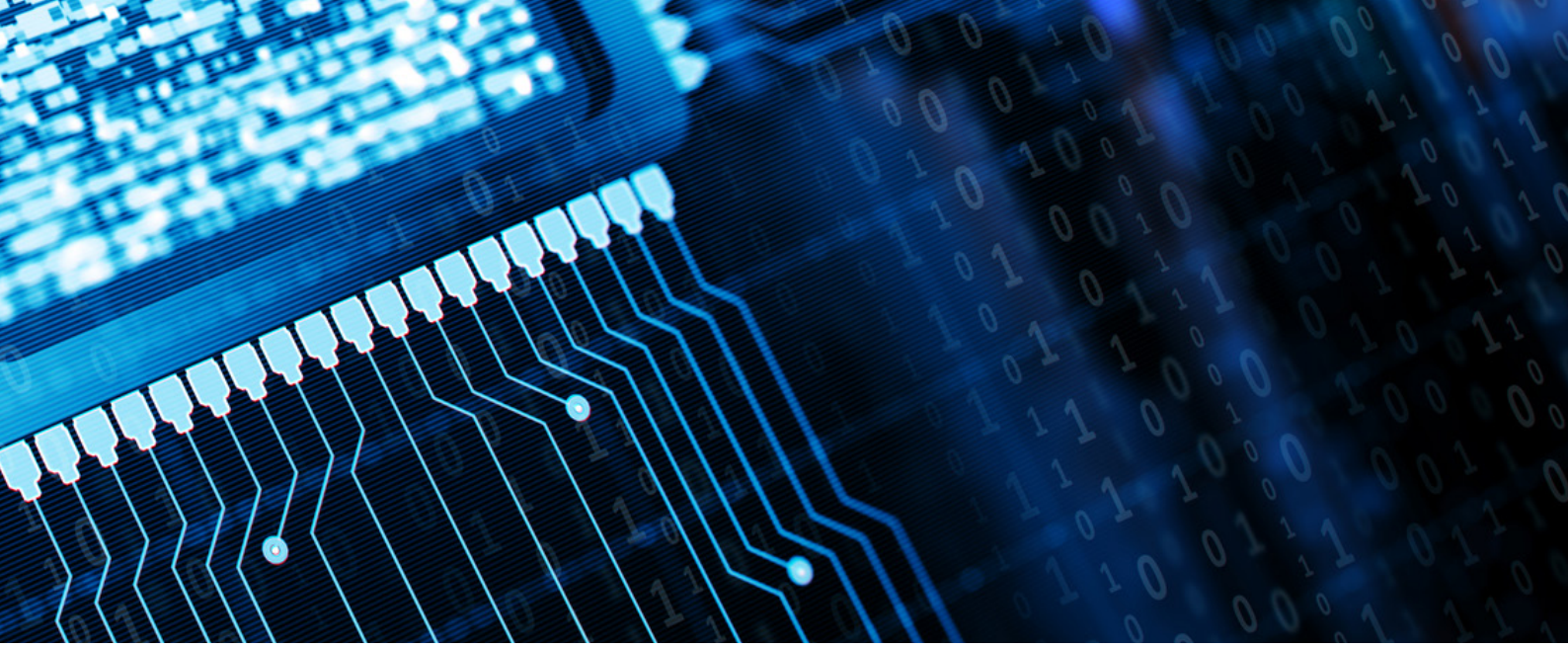
A particularly challenging situation is the implementation of a whistleblower system in globally active companies and groups. In most jurisdictions such companies are required by law to set up a functioning compliance system. They can often only achieve this by establishing a centralized system, meaning that employee data will be transmitted across borders, often between countries with differing levels of data protection. Companies must then comply with the national regulations of several jurisdictions simultaneously, which may present hurdles for a centralized compliance system.

Before introducing a centralized whistleblower system, it is absolutely essential to conduct an in-depth analysis of the labor and data protection laws across all relevant jurisdictions. Failure to do so can result in costly and time-consuming conflicts with employee representatives and/or data protection authorities.

Analysis may reveal that implementing a centralized whistleblower system requires local adaptations, which might include one or more of the following steps:

- Limiting reportable topics or processing reports locally;
- Operating in a local language;
- Implementing local intake-channels and/or investigation units;
- Pre-selecting reports and only escalating certain reports to the centralized group function;
- Only transmitting anonymized data for the purpose of statistical analysis.

However, as long as companies can prove to the competent authorities that national regulations stand in the way of a completely centralized whistleblower system, the authorities' assessment of the functionality of the system should not be negatively influenced.



Internal investigations after a whistleblower report

"Where there's smoke, there's fire" or so the saying goes. Internal investigations are often triggered by an allegation or a single piece of evidence but rarely do you have the whole story. That takes time, effort and an open mind. Many business organizations have implemented a whistleblowing system but fewer are clear on what to do when they receive a report of wrongdoing. Here we will provide some guidance on how to evaluate a whistleblower's veracity and effectively respond to the complaint.

Many things can motivate a whistleblower: sometimes they seek to redress a wrong, settle scores with a nemesis or simply report an event of concern. Separating the wheat from the chaff will be the first task of the investigator. In many cases, a prompt review of the alleged misconduct by an experienced investigator can quickly establish whether the allegation is internally consistent and involves personnel actually employed by the relevant entity.

Once the allegation is determined to be credible, the investigator should move on to evaluate the evidence, through document review and interviews. The goal, of course, is to determine if the allegations can be substantiated or disproved. But often there is not conclusive evidence. Either way, it is critical for investigators to keep an open mind, not jump to conclusions based on the nature of the allegations or personalities involved, and to always be willing to re-evaluate their conclusions. Often the full picture does not come into view until all of the pieces of the puzzle are in place.

To ensure the integrity of all investigations and to encourage reporting the investigator should always focus on protecting the whistleblower to the maximum extent possible. If possible, the whistleblower's identity should remain anonymous or his or her identity should remain confidential. In all cases, even where the allegations cannot be substantiated, the whistleblower should be entirely immune from retaliation.

Retaliation or perceived retaliation against a whistleblower raises cultural and legal risks and undermines the effectiveness of a whistleblowing program. If a company is serious in its efforts to foster a corporate culture where employees, suppliers and contractors have the confidence to raise concerns internally, it must take substantial steps to allay the natural fear of retaliation. In the worst-case scenario, a whistleblower may take action against the company for reparation or may bypass the internal reporting channels and directly report to regulators if there is a lack of trust in the internal system.

Companies are under a heightened duty to protect the identity of the whistleblower since the enactment of the GDPR. Indeed, under these regulations they need to give careful consideration to the collection and recording of personal data. It is important to seek legal advice on data protection obligations as early on as possible.

Corporations should be careful during the initial review of a whistleblower allegation and take legal advice at an early stage. Assessment of the legal risks by an external lawyer may prevent problems arising later if the investigation uncovers serious wrongdoing by the company's employees or executives.

Part 2
Internal whistleblowing around the world

This part looks at different national approaches to whistleblowing. First, Aurélien Chardeau and Cynthia Jackson discuss how French and US law handle anonymous whistleblower complaints. Then Daren Allen and Fred Reinke examine another thorny issue, whether whistleblowers should be incentivized with payments, with reference to US and UK legislation. Finally Ladislav Smejkal, Igor Svitlyk, Marcin Swiderski and Vladislav Arkhipov explain the cultural obstacles to encouraging a whistleblower culture inside companies in the former Eastern bloc. For more detail about individual countries please consult our comparative database **here**.

Confidentiality vs. anonymity in France

The two notions of confidentiality and anonymity are sometimes confused by laymen but must be clearly distinguished.

Confidentiality refers to the obligation that exists in most jurisdictions to protect the identity of the whistleblower. This obligation often entails involving as few as possible personnel in the processing of alerts made by whistleblowers and ensuring that people who have knowledge of the identity of the whistleblower keep this information confidential. In practice, confidentiality means that the recipient of the alert (e.g. the corporation's ombudsperson or an external whistleblower system operator), who is aware of the whistleblower's identity, is not permitted to disclose it to the corporation without the whistleblower's consent.

Anonymity refers to the ability of the whistleblower not to provide his identity when making an alert. The approach regarding anonymity varies significantly from one country to another: some make it mandatory or optional to give this ability to whistleblowers while others prohibit it altogether.

When local law provides for optional anonymity, a corporation's decision in this regard is delicate. On the one hand, anonymity may encourage malicious alerts and may impede any resulting internal investigation, as it is often impossible to request further information from the whistleblower. This concern is heightened when the whistleblower system is open to external parties. On the other hand, anonymity can foster the denunciation of corporate wrongdoing because the whistleblower knows that no one will be able to trace the alert back to him/her, thus rendering retaliation impossible.

In France, anonymous alerts must be treated with the outmost care. According to the latest guidelines on whistleblower systems published by the French personal data agency (CNIL), corporations should not encourage anonymous alerts. Anonymous alerts should only be processed and investigated if (i) the alleged facts are sufficiently serious and detailed; and (ii) the processing of the alert is subject to precautionary measures.

Anonymity requirements and technical implementation in the US

Some of the most prominent US whistleblower statutes Sarbanes-Oxley and Dodd-Frank require an anonymous hotline but it does not mean the same as it does in Europe. It permits persons to report without identifying themselves but does not guarantee to the whistleblower that their identity can never be known. During the course of an investigation, the identity may become known and if known, it could be discoverable in US litigation. That is why there frequently is much softer anonymity language in US whistleblower policies: you may report anonymously but the report will then be handled confidentially to the extent permitted under the law.

Whistleblowing payments in the US and UK

US

This is a brief overview of the current US enforcement environment as it relates to the use of whistleblower incentives by the SEC to support and assist uncovering and prosecuting major corporate financial fraud against investors. The SEC whistleblower program began to operate in 2011 under the authority provided by the Dodd-Frank Act. Other prominent whistleblower programs exist within the Internal Revenue Service and the Commodity Futures Trading Commission, as well as under the False Claims Act. Under the SEC's whistleblower program, individuals can report or tip off enforcement agencies about potentially fraudulent financial activities. If this information results in the payment of fines for provable wrongdoing, individuals in many cases are eligible for financial rewards, including in some cases many millions of dollars.

In 2013, over 3,000 whistleblower tips were provided to the SEC, and in 2018 the number of tips received by the SEC reached 5,200. Also, 2018 was a record year for the SEC in paying whistleblowers, with total payments in the amount of US$168 million, including a US$50 million payment to an individual in March 2018 and US$39 million to an individual in September 2018. Most recently, in March 2019, US$37 million was paid to a whistleblower.

Since the SEC whistleblower program began in 2011, the SEC has awarded US$384 million to 64 individuals, and over 28,000 tips have been received by the SEC. Tips have been received from every state plus 72 foreign countries. Given the enormous potential recovery, we can expect the number of whistleblower complaints to remain high each year. Another reason the SEC will continue to receive significant numbers of tips is that the SEC is required to protect the identity of whistleblowers, so a whistleblower can be confident that his or her name will not be disclosed publicly. Also, targeted companies are specifically prohibited by the Dodd Frank Act from taking any retaliatory actions against a whistleblower.

These payments by the SEC to whistleblowers are financed entirely by recoveries of monetary sanctions paid to the SEC by companies who have been found to have violated US securities laws. These payments are not taken from any separate amounts paid by companies in settling enforcement actions that are used to compensate victims of corporate fraud. To be eligible for an award, a whistleblower must provide "original, timely and credible information" that leads to a successful enforcement action, and the minimum recovery must be US$1 million. Whistleblower awards typically range between 10% and 30% of the monetary sanctions paid by violating companies. As a result of the SEC's whistleblower program, over US$2 billion has been returned to harmed investors.

UK

In the UK, the Public Interest Disclosure Act 1998, which came into force on 2 July, 1999, provides protection for whistleblowers who make a qualifying disclosure in relation to their employer or third parties. Essentially whistleblowers are protected against victimization or dismissal as a result of making a disclosure about a firm or individual. The notion of incentivizing whistleblowing has, however, been consistently rejected on the basis that it is inconsistent with the prevailing culture in the UK.

In recent years there has been an increased focus on whistleblowing in the UK. Following the financial crisis, for example, there was a significant focus in the financial services sector on encouraging and supporting whistleblowers. In this regard, the Financial Conduct Authority ('FCA') has a dedicated whistleblowing unit which has seen the number of reports significantly increase. For the year ended 31 March, 2019, the FCA received 1,119 whistleblower reports, consisting of 1,755 separate allegations.

In 2015 the FCA and the Prudential Regulation Authority ('PRA') published policy statements that required regulated firms to implement whistleblowing policies and procedures to (amongst other things) enable staff to more easily blow the whistle and to ensure that nothing within employment contracts deterred staff from whistleblowing. The FCA/PRA package of measures, however, did not include financial incentives for whistleblowers.

There have been various public and regulatory consultations in the UK on whistleblowing in which US style reward programs have been considered. The responses to the consultations, however, have tended to reject the notion of paying incentives to whistleblowers on the basis that it could (amongst other things) lead to false or delayed reporting and that it was not consistent with the approach traditionally taken in the UK.

There is no question that companies in the UK are alive to the need to take whistleblowing seriously. There remains, however, a deep reluctance to move to a US-style approach of incentivizing whistleblowers and we are unlikely to see any significant change in the near future.

Whistleblowing culture in the former Eastern bloc states

Poland

Most of the former Eastern bloc states have a long history of popular resistance against an oppressive state (either a totalitarian regime, tyrannical ruler or an invader).

The experience of 20th century totalitarianisms is still fresh in the minds of people. For decades, communist regimes established in Eastern bloc states used state security agencies to exert maximum control over the population, to identify and eliminate any dissidents brave enough to challenge the state.

This control was imposed by monitoring and spying on the civilian population in a way that had not been seen before. One of the tools most commonly used by the communist regimes was an extensive net of informants. These individuals, some of them terrorized and forced into cooperation by the state security officers, others collaborating willingly in exchange for personal gains, were despised by the general population. Therefore, even the slightest mention of cooperating with communist authorities would result in a person's reputation being destroyed. Even now, many years after the fall of the Berlin Wall, people accused of collaboration with communist state security agencies face public opprobrium, and it can often end political careers.

These experiences still have a great impact in Eastern bloc states. Even when called by the police or court to testify, many people feel uneasy sharing information, especially if it would result in somebody's criminal or administrative liability. Cooperating with authorities is often not perceived as a part of one's civil duty, but as a weakness or something to be ashamed of.

This cultural legacy and negative attitude towards any form of denunciation makes whistleblowing a difficult idea to encourage in Eastern bloc states. For example, in a recent study in Poland, 36% of respondents indicated that the main reason they would refrain from informing their superiors about irregularities is the fear of being considered a "snitch"[1]. Moreover, when asked how colleagues at work would react if a whistleblower informed a supervisor that one of them was taking or giving bribes, 55% of answers indicated that a whistleblower would suffer some sort of negative consequences of his report from the rest of the staff (including hidden aversion, distancing and exclusion from the group or even open criticism)[2].

Similar results appear in terms of employers' reactions to whistleblowers reporting irregularities externally (to the authorities). Some 32% of respondents indicated that as a result the whistleblower would be dismissed. It is somewhat reassuring that in a similar

1 G. Makowski, M. Waszak, *Oppressed, admired and... deserving of protection. Poles on whistleblowers. Public survey report*, Warsaw 2019, page 13 (available in Polish at http://www.sygnalista.pl/wp-content/uploads/2019/06/Internet_Raport_sygnalisci_12-06.pdf).
2 *Ibidem*, page 21.

study conducted in 2012[3], the result was 56%. This might indicate a shift in employers' mentality but the likelihood of their retaliation is surely discouraging potential whistleblowers.

The data strongly implies that Poland needs a new law to formalize whistleblowing, as well as to support and protect those reporting irregularities. That said, due to the cultural background mentioned above, lawmakers are not keen to tackle this issue. In 2017 there was a draft of an act on transparency of public life which included – among many other things – a partial regulation on whistleblowers but it was widely criticized for taking inadequate measures and for several other shortcomings.

From that perspective, we gladly observe the EU efforts to set standards of comprehensive legal protection for whistleblowers. A new directive on protection of whistleblowers adopted by the European Parliament in October this year rekindled the public debate on whistleblowing in Poland and hopefully will result in proper implementation by Polish lawmakers.

Much needs to be done to ensure whistleblowers get the protection they deserve and to erase the negative image that is so common among Polish society. A new law will be a good first step to achieve these goals, but more steps will need to follow.

Czech Republic

The approach of both the public and the legislatures towards whistleblowing is without a doubt negatively influenced by the era of Communist Czechoslovakia. The collaboration of some citizens with the secret police during that era and the generally passive attitude towards public affairs have likely resulted in today's rather negative perception of whistleblowers by the Czech public. The public considers a whistleblower more like an informer, or even as a rat, than a guardian of the law. This can be seen in almost every discussion in the news reporting on whistleblowing in the Czech Republic. Such an attitude taken by the public means there is almost no pressure on the government and the legislatures to adopt whistleblower protection laws.

The absence of these laws together with the negative public perception of whistleblowers have affected the willingness of individuals to report corruption or any other wrongdoing by their employers or co-workers. Potential whistleblowers fear their actions will be turned against them and, as a result, they will face loss of employment and public criticism.

The general legal provisions of Czech criminal law, data protection law and labor law are considered insufficient with regard to the desired standard of whistleblower protection. Therefore, there have not been many cases of whistleblowing here in the Czech Republic so far and the general willingness of the public to blow the whistle remains low, according to surveys. Since the Czech Republic is a member state of the EU, whistleblower protection laws will inevitably be applied as a result of EU law. The change in perception by the Czech public, on the other hand, will probably require more time. Without it, it cannot be expected that the adoption of EU whistleblower protection laws will result in an immediate increase in the number of whistleblowers. The way multinational companies in the Czech Republic operate might be another factor in the process of change since they are setting a high standard in their compliance programs and encouraging employees to report any potential wrongdoing.

Ukraine

In Ukraine the whistleblowing culture is still in its initial stage of development. Before international business set foot in the country there were no established procedures to handle internal reports, except maybe dedicated paper boxes here and there where employees could put their suggestions and complaints.

In Soviet times denunciators were feared and hated, and for many, reporting on your colleague is still regarded as something shameful and unworthy, rather than for a way of eliminating unethical practices and helping the company to perform better in a challenging business environment.

The landscape is changing, though, as the government starts making the first steps to protect whistleblowers. Companies are also starting to recognize the value of whistleblowing, providing modern tools for employees and encouraging them to speak up. The results are not always consistent and there are many irrelevant reports, but once the process and stakeholders mature, the effort will surely be rewarded.

3 Fundacja Centrum Badania Opinii Społecznej, *Heroes or snitches? What do Poles think about whistleblowers?*, Warsaw 2012, page 14 (available in Polish at http://www.sygnalista.pl/wp-content/uploads/2016/10/Raport_Sygnalisci-Bohaterowie-czy-donosiciele.-CBOS.pdf).

Russia

Today there are many international corporations in Russia which have to abide by Western ethical standards and a number of local corporations take such standards as their role model. However, while in the West whistleblowing is an established part of corporate culture and is aimed at preventing corporate crime, it would not be far from the truth to say that whistleblowing in Russia is still considered as something that is contradictory to local culture. This is probably rooted in the traumatic collective memory that can be traced back to Soviet times or even earlier, since various kinds of informing practices were institutionalized even in Tsarist times.

The Russian language has more than a dozen derogatory words for whistleblowing and whistleblowers. This should hardly be a surprise. As Sergei Dovlatov, one of the prominent Russian writers of the 20th century, wrote, *'we endlessly criticize Comrade Stalin, and, of course, for the cause. Still, I want to ask – who has written four million denunciations?"* In the Russian language, the words "whistleblowing" and "denunciation" are almost similar semantically. There is also a proverb *'a loose lip gets the first whip'* («доносчику первый кнут») known from very old times that shows the distinction that ordinary people tend to draw between their community and authoritarian powers in times of order, or organized crime in times of turbulence. Whistleblowing is seen as pointless or used by others to gain some ill-gotten benefit. During Soviet times, and often now, kids are taught that it is bad to snitch. To a certain extent, these cultural archetypes have been reproduced at the level of corporate culture.

Social science research, however, indicates that the attitude to whistleblowing depends on how employees position themselves. If they consider themselves as separate and, to an extent, in opposition to the management and/or shareholders, this cultural archetype of whistleblowing is predominant. However, if the employees consider themselves as an equal part of a healthy corporate culture which they share an obligation to nurture, whistleblowing may be found acceptable, even though many will still be wary of it. Studies also show that Russian employees tend to assess ethical aspects of whistleblowing differently depending on the subject matter. Thus, people tend to agree that whistleblowing is okay when it comes to reporting actions dangerous to health and safety, or actions concerning racial, religious, ethnic or age discrimination, or sexual harassment. However, for instance, reporting financial corporate crimes is not always approved by employees and depends on the circumstances.

From a formal legal perspective, Russian legislation is not much different from many other legal systems and includes employment law and personal data protection regulations based on European models. At the same time, there is no real legal protection for internal whistleblowers at the statutory level, which, together with the aforesaid cultural differences, makes it hard to expect that whistleblowing systems would work with the same efficiency and in the same as in the West. This does not necessarily mean that the culture is not changing and that it is not possible to implement a whistleblowing system more than on paper. Still, the cultural differences may be the source of many challenges in this area.

Key Contacts and Contributors

Diego Pol
Co-head of the Europe Compliance group, Barcelona
D +34 93 44 52 922
M +34 648 870 897
diego.pol@dentons.com

Judith Aron
Co-head of the Europe Compliance group, Berlin
D +49 30 26473 261
M +49 172 3987 999
judith.aron@dentons.com

Dr. Rainer Markfort
Partner, Berlin
D +49 30 26473 340
M +49 172 3601 492
rainer.markfort@dentons.com

Dr. Jan Scharfenberg
Counsel, Berlin
D +49 30 26473 635
M +49 172 3120 791
jan.scharfenberg@dentons.com

Dr Christian Schefold
Partner, Berlin
D+49 30 264 73 246
christian.schefold@dentons.com

Sebastian von Haldenwang
Associate, Berlin
D +49 30 26473 434
M +49 162 2039 628
sebastian.vonhaldenwang@dentons.com

Dr. Gabriele Haas
Counsel, Frankfurt
D +49 69 45 00 12 393
M +49 160 5065 769
gabriele.haas@dentons.com

Igor Svitlyk
Associate, Kyiv
D +380 44 494 47 74
igor.svitlyk@dentons.com

Daren Allen
Partner, London
D +44 20 7246 7651
M +44 7515 919812
daren.allen@dentons.com

Aurélien Chardeau
Partner, Paris
D +33 1 42 68 45 14
M +33 67 359 63 18
aurelien.chardeau@dentons.com

Ladislav Smejkal
Partner, Prague
D +420 236 082 242
M +42 07 752 20 975
ladislav.smejkal@dentons.com

Carolina Muñoz
Partner, San Jose
D +506 2503-9817
T +506 2503-9800
carolina.munoz@dentons.com

Cynthia Jackson
Partner, Silicon Valley
D +1 650 798 0332
cynthia.jackson@dentons.com

Vladislav Arkhipov
Counsel, St. Petersburg
D +7 812 325 84 44
M +79 21 920 40 84
vladislav.arkhipov@dentons.com

Marcin Swiderski
Senior Associate, Warsaw
D +48 22 242 56 82
M +48 69 697 95 77
marcin.swiderski@dentons.com

Maxwell Carr-Howard
Partner, Washington, DC
D +1 202 496 7141
M +1 202 716 9596
maxwell.carr-howard@dentons.com

Fred Reinke
Partner, Washington, DC
D +1 202 496 7160
fred.reinke@dentons.com

Do you want to know more?

For more information, please visit our Whistleblower Systems comparative **tool**

If you would like to subscribe to our global newsletter covering trending topics in compliance, please contact **Kathryn.Kearns@dentons.com**

ABOUT DENTONS

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Enterprise, Dentons' wholly owned subsidiary of innovation, advisory and technology operating units. Dentons' polycentric approach, commitment to inclusion and diversity and world-class talent challenge the status quo to advance client interests in the communities in which we live and work.

dentons.com

CSBrand-21348-Whistleblowing-guide-06 — 11/12/2019