



The Whistleblower Friend and Enemy of the CEO

This document addresses the point intersection between the new Trade Secrets Act (GeschGehG) and the new EU guideline for the better protection of whistleblowers! In terms of content it, serves the C-Level of German-mid-sized companies!

The paper realizes the scene of a sudden and rapidly increasing number of whistleblower reports as well as the resulting additional burden on the C-Level management. As a consulting and service provider in the protection of trade secrets, it is our task to protect organizations against an only alleged dispositional ethics and to

examine the substance of whistleblower reports quickly and cost-effectively. In this context, we use our technology to investigate whether the whistleblower meets the requirements for legal protection. Results obtained are included in recommendations for action to our customers and, if necessary, substantiated by court-proof evidence.

Introduction

On April 16th, 2019, the European Parliament voted for a better protection of whistleblowers and adopted another EU-wide directive. This directive must be implemented into national law within a period of two years in each of the member states. In Article 2 (2), the European legislator refers to the possibility of adopting whistleblowing rules for the national legislature in other areas of law as well. Whether and to what adjustments it will come in Germany, is remains to be seen. But it is very likely that Berlin will prevent a patchwork. It will avoid the possibility of unequal treatment of breaches of national law and of EU law.

Summary of the Whistleblower Policy

In its final version, the Directive now obliges small businesses (with 50 or more employees) to set up several whistleblower channels. A distinction is made between internal, governmental and notifications to the public or the media. Each channel must allow a written, electronic, telephone or personal message type. There is a strict obligation for the company to respond to reported misbehavior within a period of 3 months! Enterprises are required to ensure effective protection and mechanisms to prevent retaliation (such as workplace harassment, discrimination, disadvantage or dismissal) through access to free advice and appropriate remedial action. A statement on the side. It is logical to assume that the internal relationship in these 90 days will be very difficult! The productivity of the affected companies will definitely suffer. Therefore, from a legal and economic point of view, it can only be of great interest to the company to ensure a swift clarification of facts!



The expected increase in reports

Honest whistleblowers are worthy of protection and this law should also play positively in the hands of management. However, realistically, many executives fear that the lower instincts of the human species tempt them to alienate a well-intentioned law from its natural purpose. The obligation to respond on any kind of whistleblower reports will demand much more attention from the CEO, than he can afford! The number of reports and liability to investigate them will definitely explode because of widespread dogmatism. A large number of reporting channels as well as the fact that many faultfinder (often in a poor condition on particular days) are among the whistleblowers. threatens with bad consequences for both sides. Publicized reports will not bring any apparent infringement to the company except reputational damage. In this context, it should be mentioned that a certain criminal risk for any type of notification will accompany the whistleblower. Imagine the defense of false accused colleagues or superiors. For the company, this EU directive means with high guarantee a massive amount of time and special budgets for implementation, treatment of hints and long-term system maintenance. According to the common lexicon of the C-Suite, it is a very expensive management point!

The point of intersection between the new Trade Secrets Act and the Whistleblower Directive

The new Trade Secrets Act (GeschGehG) has not become a good law for companies. On the contrary, it presents new and difficult challenges. In addition, its entry into force has left defenseless all companies overnight. Already in its implementation as an EU-wide guideline, dealing with the whistleblower, especially in connection with trade secrets, has caused a delay of almost one year. The EU Directive 2016/943, therefore, came into force as its own Trade Secrets Act (GeschGehG) on April 26th, 2019. At the last moment, a marginal addition was made regarding a potential trade secret conflict of interest.

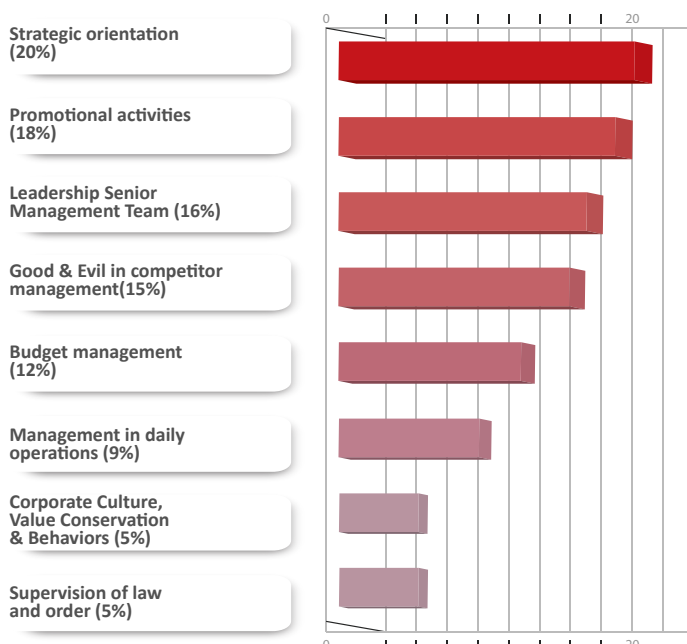


It is about the possibility of legitimizing the disclosure of trade secrets, provided that there is a reasonable suspicion of a breach of national and Union law. Secretly hides behind the hope of authorities and journalists that evidence of unlawful behavior in the company will leave the company by whistleblowers. The role that the whistleblower plays in this violation is, in the first place, unimportant to the information hungry sites. With the enlightenment, the companies will be on their own. Especially when it comes to proving that it is just an only alleged dispositional ethics!

Of course, the next EU directive on the protection of whistleblowers creates the appalling notion that the legislator wants a company registered whistleblower entered as a "liaison officer" between companies and public authorities, whose funding and comprehensive dismissal protection should, of course, by the companies themselves. We, therefore, find that both laws are not de facto in favor of companies! Why do both laws appear so well timed? The answer is the experience of recent years. Legislators are well aware that non-compliance with applicable national and Union law is closely related to trade secrets. Via whistleblowers, such cases became headlines in the economic sections of the media. Setting up the two laws together acts as a forced marriage for the sole purpose of creating an interface between business, government and the media. This point of contact should be used by the authorities to make companies more transparent. Ignore the obviously warm words for the protection of the whistleblower! This is also on thin ice, as far as companies proceed more skillfully.

Does it hit the CEO personally?

The leader of a business has a fundamental problem! He has limited time! With an average of 60 hours a week his performance limit has been reached. All 6 to 8 hours, this function displays on the weekend of his free time on! Under the high pressure, not to fail, executives set clear priorities.



The combination of the two laws will mess up the work of a CEO! He will probably devote more internal than external activities in the future. He will also be left alone in the final decision and forced to work with external consultants. It is expected that his direct subordinates will be affected by reports. Successful business leaders know that such company management, in the long run, can not work. The shift in their time spent towards corporate culture, value preservation & behaviors and the oversight of law and order detract from the truly strategic governance tasks. But the tactical work decides on the success and failure of the company! Those knowledgeable in this field know that CEOs with these two laws are not necessarily challenged in their strongest discipline!

The positive aspects of a whistleblower

But enough of the negative words about a whistleblower. The CEO can also expect a lot of positive from whistleblowers. Because of his purely offensive approach, he has very little insight into the daily work of his management team and the workforce in the rest of the organization. In international companies, it is almost impossible to overlook this, let alone to control. For those CEOs in particular, the Whistleblower Directive will provide the opportunity to benefit from reports on the defensive and to readjust corporate guidelines through measures in governance and compliance. Let's ignore malicious or anti-corporate whistleblowers. The majority of employees are honest and dedicated, value their employer and expect the protection they deserve from this new law. If these employees now act as whistleblowers, many of the open questions in companies are resolved. We, therefore, note that among the whistleblowers are also friends of the CEO, who will facilitate his duty of control.



How does the CEO remains in the driving seat?

He cannot ignore neither of the laws! Employees' advocacy organizations will only keep a watchful eye on whistleblower protection law and insist on its swift implementation, while the CEO must act in line with the company's business interest when it relies on the new protection of trade secrets (keyword: liability issue)! But what exactly should the CEO do to benefit from whistleblower reports and at the same time prevent them from being subjected to an only alleged dispositional ethics? The solution can only work in times of digitalization with the help of technology! In doing so, he can follow the legislative timetable and apply the same logic so as not to miss legal deadlines.

The implementation of the Trade Secrets Act is all crucial

In the first step, the legislator demands the implementation of the Trade Secrets Act. Already here, the CEO can turn the tide in favor of the company and look forward to the later threatening reporting rage of his whistleblowers. As mentioned at the beginning, the implementation of the Trade Secrets Act places very high demands on a company. If a company wants to survive the loss of trade secrets without damage, it must fully implement the legal requirements.



It is not necessary here to address all the requirements of the law in order to understand how the company protects its trade secrets and checks the accuracy of the notifications in order to bring out the background and interplay of all factors. It is important for us as a service provider to note that we consider ourselves responsible for complying with the Labor law and the GDPR while strictly adhering to the requirements of the Trade Secrets Act with our services. Essentially in the Trade Secrets Act is the definition of business-specific trade secrets. Thus, information must be categorized as data in three to four levels of confidentiality. During this activity, we naturally focus on the core of our customers' success.

With the synergy of our consulting with our technology, after creating an overall inventory, we succeed in recognizing and classifying trade secrets, regardless of company types and sizes, on a timely basis. Then we follow another requirement of the law, namely, the creation of a knowledge inventory. We look at a holistic overview of the insider knowledge of all types of trade secret holders. In addition, we recognize who has access to the classified trade secrets and when, where and with which access it has taken place.

In the implementation of the Trade Secrets Act, the results will be used later to formulate action catalogs for the creation of a protection concept. For the clarification of whistleblower reports, it is sufficient to update this forensic data source regularly. Each whistleblower triggers an internal investigation of the incident. In this case, an algorithm is used, which provides rapid clarification.

So it determines whether a particular person or a whole group of people has steadily gathered more information or an ever deeper knowledge of one or more trade secrets. This interest can also be presented in a time frame. If the sequence of the skimming off of this information is represented in the time representation and compared with the event time of a whistleblowing report that has taken place, an anonymous or even corrupt whistleblower can be unmasked by using an exclusion method. Conversely, with our service, the claim of a whistleblower can be confirmed!

Our recommendation for action to the CEO

Convert the lawsuit and create a data pool of forensic evidence. This data pool will serve you in the future as a kind of "Source of Truth". Thus, the massive increase to clarify pending whistleblower reports can be handled cost-effectively and promptly. The necessary interface knowledge of business, legal and technological aspects is the guarantor of success of the INTELLIGENCE LOSS PREVENTION AUDIT [ILPA]. Find out more about our service and technology on our website

www.GeschGehG.eu

For more information and consultations please contact us by e-mail on

Zoran.Jovanovic@GeschGehG.eu



If you want to end the vulnerable state of your company, please contact us!
The content was written by Zoran Jovanovic – CEO of Prosper Intelligence Solutions GmbH
Breitenfurterstrasse 378/1/1 in AT-1230 Vienna, Austria. - zoran.jovanovic@GeschGehG.eu
www.GeschGehG.eu