WOLF THEISS

An external electronic whistleblowing system has significant advantages over the alternatives

Whistleblowing is all about protecting the whistleblower. But shouldn't the company affected also be protected against a possible leak? What are the options for protection?

The EU Whistleblowing Directive provides for a secure reporting channel that must be made available by the company and all others, including external parties. This can be implemented in person, in writing, or electronically. *Upon closer examination of the word "secure," the scope for implementation quickly becomes very small.*

If a company decides to use a hotline, a mailbox, or an e-mail system, it must not forget the documentation obligation required by the Directive. This means that sensitive data will remain within the company and will probably be digitally processed in the company's own network.

Once stored in the company network, it can happen very quickly through one's own convenience, but also simply through carelessness, that unauthorised employees gain access to this sensitive data – rumours can arise, and so on. The avenues for access through internal IT should also not be ignored in these considerations. It may well happen that external help is required due to a tip containing potentially delicate information.

At this point, at the latest, an external data leak may occur, since data must be transferred from the internal company network to a lawyer, for example. This is usually accompanied by lively written communication, usually by email.

In order to significantly reduce the risk of these unwanted events from occurring, an external electronic whistleblowing system is the best solution.

With a good solution, all data, from the initial contact to

Roland Marko

Partner, Wolf Theiss
Senior Legal Consultant, Responsible Business Solutions
roland.marko@wolftheiss.com
+43 1 51510 5880

Gernot Rauter

CFO, Wolf Theiss
Management, Responsible Business Solutions
gernot.rauter@wolftheiss.com
+43 1 51510 3200

Helmut Waitzer

CIO, Wolf Theiss
Management, Responsible Business Solutions
helmut.waitzer@wolftheiss.com
+43 1 51510 3300

the conclusion of the case, remain in a closed system, whereby a possible leak within the company network **can be virtually ruled out**.

However, this is offset by the fact that the system is freely accessible on the internet for all potential whistleblowers and could therefore provide an interesting target for cybercriminals. The fact that credible systems comply with the current state of data encryption does not need to be mentioned here - *what is much more important is the system architecture on which it is based*.

No data processing system is 100% secure: it is and will forever be a cat-and-mouse game between system providers and cybercriminals. In the worst-case scenario, if there is a successful attack, it may not immediately affect all of the provider's other customers. There may be a trace of it, but the actual degree of risk to the business often only emerges on the basis of the documents that may be attached. Even if, from an architectural point of view, the possibility of other customers being affected can be virtually ruled out, it must still be ensured that none of these documents are removed and thus fall into the wrong hands.

In addition, there must be a way to make the report from the whistleblower, including the documents and correspondence, available to other authorised persons (including external ones, e.g., a lawyer) within the closed system in order to avoid the risk of an external data leak.

Data security is also very much related to trust of the solution provider - who is the provider, who operates the solution and also from a GDPR perspective, where does the data reside?

If a company relies on a professional external solution, **this is the best way to protect not only the whistleblower, but also their own company** - a good solution costs a fraction of any blackmail attempt or loss of reputation.

Comparison of whistleblowing systems

WOLF THEISS

Reporting channels and specific requirements	Email	Ombudsman (person in the middle)	WB Hotline (off-site ombudsman, compliance officer)	Electronic System
Can be used by employees	Yes	Yes	Yes	Yes
Can be used by third parties	Yes	Yes	Yes	Yes
Availability	365 days, around the clock	By arrangement	according to agreement	365 days, around the clock
Internal impartial person accepts	Can be designed with a person nominated for this purpose	Ombudsman needs one or more nominees	Hotline needs one or more nominated persons	Can be designed securely in system
External impartial person accepts	Can be designed with a person nominated for this purpose	Yes = Ombudsman	Hotline needs one or more nominated persons	System can also be operated by external person
Acknowledgement of receipt of report (7 days) and feed-back on action taken (90 days)	Must be designed to Exchange Server level if this is to be done automatically	Must be guaranteed organisa-tionally > Feedback is not (easily) possible with anonymous reporters	Must be guaranteed organisationally > Feedback is not (easily) possible with anonymous reporters	First response is made automatically after receipt of the message, record keeping of the message in the WB system
Communication channel (bi-directional)	Yes, but unless end-to-end encryp-tion is active, this could be seen by internal IT or mail system operators	Yes, but must first be determined individually with WB	Must be set up organisationally parallel to the hotline	Secured (return channel) exchange of information between compliance and the notifier possible
Exchange additional files	Possible in the context of attachments	Yes, but depends on the communication channel individually defined with WB	Difficult --> where to send the files; logistics	Notifier can submit any kind of files (photos, PDFs, etc.)
Completeness of the message	Email is a free text - it is up to the notifier to report correctly	Yes, but logging is the sole responsibility of the ombudsman	Telephone logs/recordings must be transmitted	Organisationally, the notifier is helped to enter everything necessary in the notification form
Integrity of the message	Cannot be verified	Cannot be verified	Cannot be verified	The information and data are transmitted to compliance in full
Confidentiality of the message	Unless end-to-end encryption is active, this is not guaranteed.	Difficult - > as soon as correspondence, files...follow; access by company IT possible	Difficult --> as soon as correspondence, files…follow; access by company IT possible	No filing of e-mails, files...outside the WB system
Access by unauthorised persons	If no end-to-end encryption is active, this is not guaranteed.	Many interfaces - cannot be excluded	Many interfaces - cannot be excluded	Only the compliance officer or persons authorised by the compliance officer are informed about the report.

Comparison of whistleblowing systems

Reporting channels and specific requirements	Email	Ombudsman (person in the middle)	WB Hotline (off-site ombudsman, compliance officer)	Electronic System
Data Security	Unless end-to-end encryption is active, this is not guaranteed.	Depends on the chosen service provider	Depends on the selected service provider	Possible 2 separate databases, in a private cloud in the EU ISO-certified data centre
ID only disclosed with explicit consent	Can be agreed with WB	Can be agreed with WB	can be queried	provided in the system
Is the WB sufficiently protected	Anonymity almost impossible from a technical point of view	Depends on ombudsman, the staff and technical infrastructure; identity may be inadvertently disclosed	Hotline staff, communication with the company and the WB, identity may be accidentally disclosed	Complete technical anonymity. No IP address, no data storage. WB has its own password and case number.
Complete documentation of the message	Standard e-mail systems are not audit-proof and therefore complete documentation cannot be guaranteed.	Difficult to record information objectively and completely in the course of the conversation and not to “filter” it.	Difficult to keep files, emails complete in the course of the conversation	System can be audit-proof, deletion without documentation is not possible.
Audit security	Only possible through additional measures	Not provided	Not provided	Tracking of each case in the database
Internal IT	If no end-to-end encryption is active, IT has technical access to the e-mails and thus also to the content.	Theoretically able to access information from the moment the ombudsman is contacted by the company’s compliance department	Theoretically from the contact of t e hotline at compliance in the company able to access information	Cannot access the reporting system
Handling of group structures	Can be designed with different email addresses, but risk of confusion for the potential WB	Indirectly via checklists	Indirectly via checklists	Group printers and authorisations can be easily designed
Language capability	Depends on the recipient	Depends on the ombudsman as to which languages are offered and when	Depends on call agent regarding which languages are offered and when	Web-Front-End; registration in all languages possible
Others	An email is not anonymous per se	Possible mental barrier and challenges to call a third party	Possible mental barrier and challenges to call a third party. How / when will they then hand over WB directly to company or Ombudsman?	
Costs of the reporting channel – one-time	Setting up an email address - EUR 0, - (external costs)	Coordination and definition of the details for recording and passing on information and communication channels: approx. EUR 2,000	Setting up ISDN extensions, basic training in the logic of information transfer, preparation of checklists by the company: EUR 1.500	Setup in data centre, design of company-specific CI/CD and customisations, EUR 1.500
Costs of the reporting channel – ongoing / p.m / p.a.	Only internal costs, if the recipient is an employee of the company (e.g. Compliance Officer)	Basic flat rate: EUR 500 / month or EUR 6.000 / year + Variable per call / communication process: EUR 200 / hr. (during normal business hours / 2 languages)	Basic flat rate: EUR 500 / month or EUR 6.000 / year, variable per call / communication process approx. EUR 2.5	EUR 700 / EUR 8.400

For additional information and to learn more about whistleblowing options for your business, please contact our experts to set up an appointment.

Responsible Business Solutions is a 100% subsidiary of Wolf Theiss.

About WOLF THEISS

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

Wolf Theiss
Schubertring 6
AT – 1010 Vienna
www.wolftheiss.com