WOLF THEISS

SECUREVEAL SYSTEM PRIVACY NOTICE - WOLF THEISS

This privacy policy provides an overview on how personal data is processed within the whistleblowing system SecuReveal. The protection and confidentiality of personal data is an integral part of the architecture of SecuReveal, providing protection for all users. This particularly includes avoiding tracing of the whistleblower's identity. All reports and communication are anonymous unless the whistleblower discloses his identity in the report or to the compliance officer.

Personal data is processed in relation to the following data subjects:

- Website visitors
- Reporters (Whistleblowers)
- Suspects, witnesses or other third parties involved in a reported case

1. CONTROLLER AND CONTACT

WOLF THEISS Rechtsanwälte GmbH & Co KG

Schubertring 6, 1010 Vienna, Austria
T. + 43 1 515 10
F. + 43 1 515 10 25
E. wien@wolftheiss.com

2. PERSONAL DATA AND PURPOSES OF DATA PROCESSING

2.1 Website security

We process personal data to offer our goods and services on our website. When accessing our website your browser automatically transmits your IP-Address, as well as other information about your system (e.g. your operating system and browser version). This data is necessary to deliver the contents of our website to your device and to ensure that they are displayed correctly. Our firewall monitors this connection data with automatic protocols (logs) to prevent malicious access or other attacks. These protocols are automatically deleted after three months the latest.

2.2 Whistleblowing platform

SecuReveal and our website are optimized for the maximum level of data protection for our whistleblowers. The system can be used without providing any personal data and therefore protecting your identity. This service uses, among others, Secure Socket Layer (SSL) technology - the industry standard for encryption in the internet - in order to ensure the safety of the data provided by whistleblowers. This internet encryption standard encrypts data during the transfer from the computer of the whistleblower to the server of the service. We do not use any tracking technologies or third-party cookies.

SecuReveal uses unique encryption methods. This encryption ensures that only the whistleblower and the involved compliance officer(s) and competent case handlers can read the report and the associated communication. Neither we nor any of our processors can read reported content.

If you wish to remain anonymous you can use the case code assigned upon finishing the report and your specified password to access the electronical mailbox of this website. You can use this mailbox to communicate anonymously with the compliance officer handling the case. To further increase your privacy please note the following:

- do not disclose personal information (e.g.: your name, relationship to the accused) or any information as such in the message, that could lead to your identification;
- do not use the service from company or authorities-owned networks or other networks that may monitor the internet use.

If you decide not to disclose any contact details and do not use the mailbox of this website our compliance officer might not be able to pursue your case if vital questions remain unanswered. We therefore recommend using our anonymous mailbox to ensure that the issues you address can be handled correctly.

Depending on the data you provide we process the following (personal) data:

- Case code (you may use the case code to login anonymously)
- Password
- Case type (e.g. insider trading, bribery, corruption, market abuse, discrimination, harassment, breach of data protection, fraud, money laundering, misappropriation of trade secrets)
- Report (incl as provided by you: personal data of suspects, witnesses or other third parties involved; incident description; as well as data regarding criminal offences)
- Identity e.g. name and contact details (if disclosed by you)
- Any attachments provided by you (Please note: digital files may contain hidden personal data that could compromise your anonymity (e.g. information on the author in the document properties). We thus recommend to diligently review the content and the settings of your files and to remove any unwanted personal data before any upload.
- Communication regarding your case within our system

We process the personal data based on our legitimate interest to investigate any filed case of misconduct and to provide our whistleblowers a secure communication system with our compliance officers (Art 6 para 1 lit f GDPR).

2.3 Cookies

This website uses cookies. Cookies are small text files which are temporarily stored on your device when you visit our website. Cookies cannot access, read or change other data stored on your device. The following table provides an overview of the cookies used on our website:

Cookie(s)	Provider	Purpose	Storage period
Session	/ (First Party Cookie)	This data is necessary to manage your current connection (Art 6 para 1 lit f GDPR).	For the duration of the visit

Further information about the cookies stored on your device can be found on: http://www.youronlinechoices.com

3. STORAGE PERIOD

We only store personal data within the statutory retention periods or insofar as there are justified interests in further processing (e.g. for the exercise and defense of legal claims). Your report and the corresponding communication data will be processed until not more than two months after investigations on your report are close or enforcement measures are decided on final and binding. For the storage period of cookies please refer to the cookie section of this privacy policy. You may also delete cookies in your browser settings at any time.

4. RECIPIENTS OF DATA

Incoming reports are received only by our respective compliance officer(s) assigned to your region and case type. Our compliance officer(s) evaluate the case and engage in any further investigations required by your case. For this purpose and where necessary, report details may be shared with employees or authorities involved in handling the specific case. Furthermore, your reports may be forwarded to our group companies you select or otherwise include in your report. Our employees are obliged to data secrecy and will handle each case with utmost discretion.

Our service providers may process your personal data on our behalf in order to provide our services (esp. IT service providers and their relevant sub-processors). The encryption methods embedded in SecuReveal ensure that data is not legible for these service providers.

SecuReveal is hosted on high-security servers in Austria and provided by:

RBS Responsible Business Solutions GmbH
Hegelgasse 13, 1010 Vienna, Austria
T: +43 (0) 800 80 20 46
E: office@secureveal.com

5. YOUR RIGHTS

Within the statutory provisions you have the following rights concerning the processing of your personal data:

- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to object to a processing based on legitimate interests
- Right to withdraw a data protection consent at any time
- Right to data portability for data provided by you, as well as
- Right to lodge a complaint with the competent supervisory authority (in Austria: Austrian Data Protection Authority, https://www.data-protection-authority.gv.at/)

Furthermore, you may change the use of cookies in your browser settings or on the following websites: https://www.youronlinechoices.com

We do not process your personal data for the purpose of making decisions that are based solely on automated processing, including profiling, which produce legal effects on you or may similarly significantly affect you (Art 22 GDPR).

For requests and general questions regarding data protection please refer to: data.protection@wolftheiss.com