

PERISKOP

CODE OF CONDUCT

A Company's Code of Conduct* is a behavioural guideline that defines ethical principles, corporate values and rules for respectful and compliant cooperation.



2025

*Please note that the English version serves solely as a translation. In case of doubt, the German version is to be treated as the original and the source of truth.

AGENDA

01 OUR VALUES & BASIC PRINCIPLES

- 1.1 Compliance - goal & importance
- 1.2 Group-wide implementation of the compliance guidelines

02 LEGAL & ETHICAL PRINCIPLES

- 2.1 Ethical behaviour in investments
- 2.2 Fair labour
- 2.3 Travel expenses & procurement policy

03 BUSINESS RELATIONSHIPS & RESPONSIBILITIES

- 3.1 Dealing with business partners
- 3.2 Avoiding conflicts of interest
- 3.3 Company & business secrets, assets

04 INFORMATION SECURITY & DATA PROTECTION

- 4.1 IT security & governance
- 4.2 IT policy for employees
- 4.3 Policy on the use of mobile devices
- 4.4 Data protection

05 REPORTING & CONTROL

- 5.1 Indications of violations & weaknesses in the Compliance Management System (CMS)
- 5.2 Contact persons & monitoring

FOREWORD

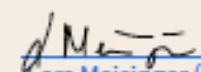


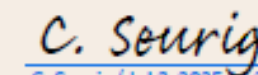
Periskop Partners has set itself the goal of positioning itself as a leading investment strategy consultant and asset management service provider in all areas of the property value chain. Our principle is to always achieve these goals in line with our responsible behaviour and positive impact on society and the environment, and in compliance with applicable laws, guidelines and industry-specific standards.

Periskop's reputation and the trust of our business partners, employees and the public are largely dependent on the specific behaviour of each individual. Everyone at Periskop should help to ensure that the positive expectations associated with Periskop are fulfilled. This Code of Conduct therefore represents a binding guideline that is intended to provide a reliable framework for daily professional behaviour and contains legal and ethical requirements for all Periskop employees.

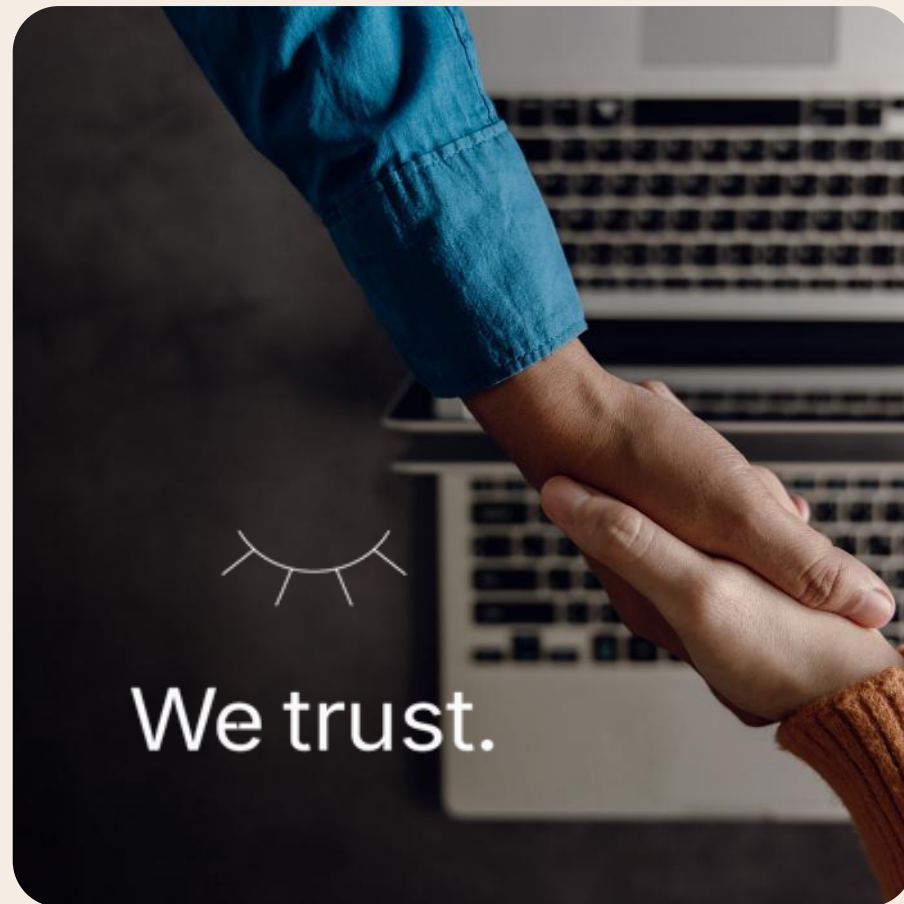
Anyone who violates the Code of Conduct and internal guidelines damages Periskop's reputation and can cause serious economic damage. Violations will not be tolerated by Periskop and, regardless of the legal consequences, such violations may result in disciplinary action.

We would like to thank everyone for their support in implementing our principles by complying with the Code of Conduct. This is an essential contribution to the successful realisation of our goals.


Lars Meisinger (Jul 3, 2025 14:05 GMT+1)


C. Seurig (Jul 3, 2025 14:26 GMT+2)

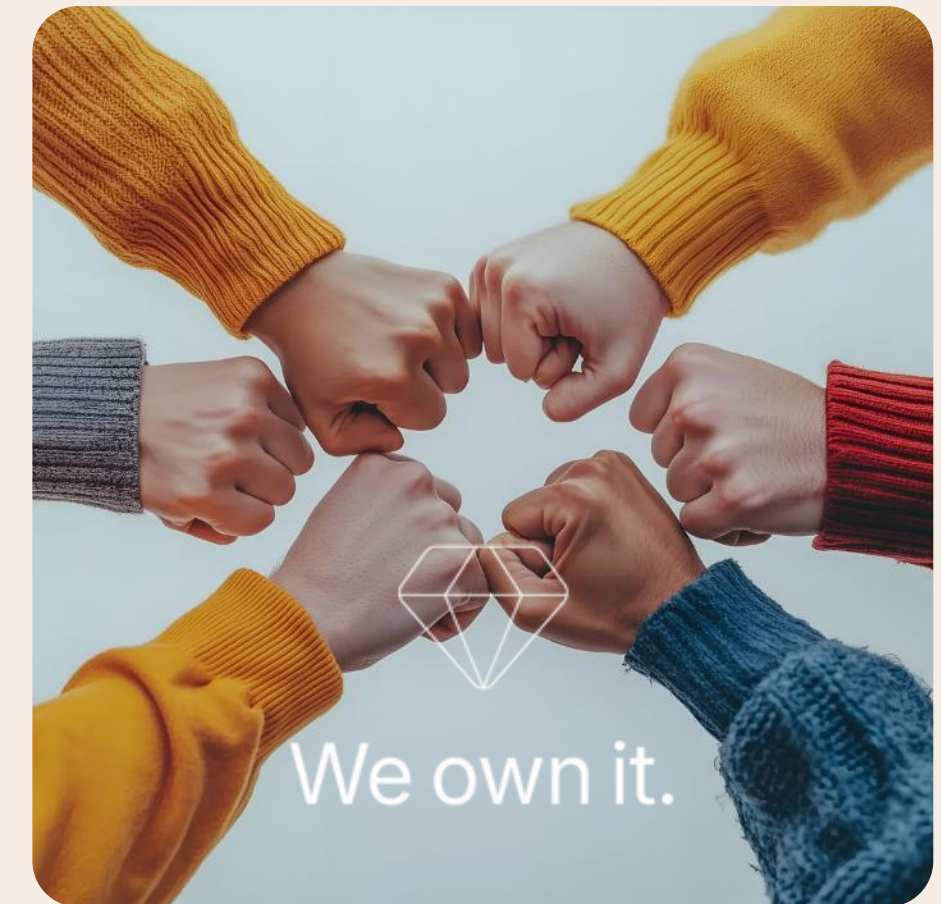
1 OUR VALUES & BASIC PRINCIPLES



Trust and **transparency** form the basis of our collaboration. We rely on **open communication** to work hand in hand as a team and pave the way for long-term growth.



We create stable values together through **empathy, respect** and **diversity**. We inspire each other and strengthen our collaboration - **together we achieve more!**



We **take responsibility, act with agility** and **make well-founded decisions**. We see mistakes as a valuable learning opportunity and use them to **continuously develop** ourselves **further**. Each of us actively contributes to the success of the Company!

1.1 COMPLIANCE - OBJECTIVE & SIGNIFICANCE

What does "compliance" mean for Periskop?

We understand the term "compliance" in a sense that all employees, managers and board members of Periskop ("**employees**") adhere to the applicable laws and internal regulations in all business activities in order to prevent economic damage and damage to Periskop's reputation. Such legally compliant behaviour at all times and in all places also protects against personal liability. This requires each of us to pay constant attention to the issues contained in this Code of Conduct, which may entail significant risks in our day-to-day work.



PERISKOP



Who is responsible for compliance at Periskop?

Compliance affects **all of us**. All employees and managers, including the management, are responsible for this in their daily work. Only if we know, understand and comply with the rules and regulations that are relevant to us can we achieve Periskop's goals in the long term.

Who does the Code of Conduct apply to?

The Code of Conduct applies to **all** Periskop **employees and managers**. Our managers are responsible for ensuring that all employees are aware of their responsibilities and understand this Code of Conduct. Managers are supported in this task by the Compliance Officer.

To ensure that all employees understand the rules of conduct set out in the Code of Conduct and are able to apply them in their day-to-day work, mandatory interactive training courses are held regularly in the form of e-learning sessions in accordance with the annual training plan.

To what extent does the Code of Conduct apply in the legal environment?

This Code of Conduct forms the **minimum standard** for the activities of all Periskop employees. If additional or deviating regulations apply in special constellations abroad, these naturally take precedence.

If you discover or suspect any discrepancies between a compliance guideline and the law applicable in your jurisdiction, please inform Periskop's Compliance Officer immediately.



1.2 GROUP-WIDE IMPLEMENTATION OF THE COMPLIANCE GUIDELINES

PERISKOP PARTNERS

As the **parent Company of the Group**, **Periskop Partners** defines the **compliance guidelines** for all **Periskop Group companies** in Germany and abroad. This means that for the Periskop Group companies, including Periskop Partners ("Periskop Group" or "Periskop"), the compliance guidelines issued by Periskop Partners take precedence over any compliance guidelines issued within a Group Company. Anything else shall only apply if Periskop Partners has authorised this accordingly vis-à-vis the respective Group Company.

What does the Code of Conduct contain?

In addition to **general standards of conduct** and **ethical principles**, **compliance with** which is **a top priority** for Periskop, this Code of Conduct contains **an overview** of the **group-wide behavioural guidelines**, rules and regulations for which Periskop has issued individual and more detailed compliance guidelines (the "Compliance Guidelines", see the overview at the beginning of this Code of Conduct). Where Periskop Partners has issued such Compliance Guidelines, you will find a corresponding reference in the relevant section of this Code of Conduct. Where reference is made to "this Code of Conduct", this always refers to this document together with all Compliance Guidelines, which form an integral part of this Code of Conduct, unless reference is made to another circumstance. The definitions in this Code of Conduct also apply to all compliance guidelines.



2 LEGAL & ETHICAL PRINCIPLES

2.1 ETHICAL BEHAVIOUR IN INVESTMENTS

- (1)** At Periskop, we **compete aggressively** for our business success. However, we must not violate laws or make statements that could damage our reputation for integrity and fair business practices. We are all committed to conducting ourselves and our business in a **fair, ethical and legal manner**.
- (2)** We must ensure that the **information about our solutions and services** that we pass on to existing and potential investors and business partners is **fair, factual and complete**. We must not make deceptive or misleading statements in order to induce decisions or remain in business. We **provide objective and unbiased advice** in the best interests of our clients.
- (3)** In the course of our business, we must not induce anyone to make investment decisions or certain recommendations for investment decisions in order to gain a direct or indirect personal advantage. In particular, the investment guidelines of funds must always be observed in our activities.
- (4)** The internal guidelines must always be adhered to. They serve the purpose of **quality assurance** and must be strictly observed when selecting potential investments as well as during due diligence reviews and when making recommendations. Our activities must also always be aligned with this Code of Conduct when preparing and making decisions for internal and external investment committees and legal requirements must be observed and implemented.
- (5)** We **do not make false, misleading or disparaging statements** about the services of our **competitors** and win contracts thanks to our integrity and expertise, not by disparaging our competitors.

2.2 FAIR LABOUR

(1) Equal opportunities & Prohibition of discrimination

Periskop stands for **multicultural, supportive co-operation and equal opportunities**. Discrimination or disadvantage on the basis of e.g. ethnic origin, gender, religion, ideology, disability, age, sexual identity or other personal characteristics is prohibited.

(2) Occupational safety & health protection

Our **employees** are our **most valuable asset**. That is why their safety is of particular concern to us. We include occupational safety in all our business considerations. All our employees are encouraged to make suggestions for improvement to their line managers.

(3) Diversity and inclusion

Diversity and inclusion play an important role at Periskop. Our workforce must **reflect** our **diverse investor base** in order to better understand and fulfil their needs.

(4) Alcohol and drug abuse

Our Company also stands for a **safe, productive and drug-free working environment**. No one may be under the influence of illegal drugs, alcohol or other illegal substances at work.

(5) Fair working conditions

We at Periskop ensure that **fair working conditions** exist both in our Company and with our business partners.



2.3 TRAVEL EXPENSES & PROCUREMENT POLICY



TRAVEL EXPENSES POLICY

At Periskop, we understand the term "travel expenses policy" to mean compliance with the principles for **planning, authorising, booking** and **invoicing business trips**. All employees, managers and members of the Executive Board are obliged to comply with this policy and applicable law when travelling on business. The aim is to use the available **resources responsibly**, ensure **economic efficiency** and guarantee the **traceability** of all business-related expenses.

The guideline creates a clear framework to enable the transparent and orderly processing of travel expenses. Among other things, it regulates **the travel booking process**, the **authorisation requirements** and the **requirements for the documentation** and **settlement of expenses**. A **central booking system** is available to support this process, which must be used to plan and book trips efficiently.

Behaviour that complies with the rules when preparing and carrying out business trips not only **protects against economic risks** and **liability**, but also makes an important contribution to the **integrity** and **professionalism** of our Company. It is therefore in the interests of all of us to consistently observe the guidelines.

PROCUREMENT GUIDELINE

The procurement guideline sets out binding rules for **fair**, **legally compliant** and **transparent purchasing processes**. All employees are responsible for complying with them.

Procurement takes place under competitive conditions and is based on **objective, documented criteria**. Suppliers are selected on the basis of **quality, performance** and **cost-effectiveness** - conflicts of interest must be disclosed and avoided.

Periskop only works with **trustworthy partners** who pay attention to **data protection, reputation** and **sustainability**. **These criteria** are taken into account when making decisions. Suppliers with negative sustainability or compliance profiles are excluded.

Bribery, political influence, inappropriate donations and a lack of transparency are prohibited. In addition to **quality**, contractors must also demonstrate **reliability**, **innovativeness** and **compliant behaviour**.

The guideline protects against risks and promotes **integrity**, **fairness** and **sustainable success**.



Periskop acts responsibly and refrains from the following activities and projects:



- (1) Business relationships with partners who operate an **illegal business** or are **criminals**, in particular with regard to **arms, drug or human trafficking**, the **financing of terrorist organisations** or the **facilitation of wars or incitement to hatred**. In this context, particular reference is made to the Directive on Combating Money Laundering and Terrorist Financing, which contains further details on this topic.
- (2) Profits from the business areas of **tobacco production, (legal) weapons production** and **gambling**.
- (3) Projects whose realisation would require the **demolition of existing residential buildings**. **Excluded** from this restriction are residential buildings that **are dilapidated or predominantly vacant** or consist of **fewer than 15 residential units**.
- (4) Transactions **for purely speculative reasons** without Periskop's activities adding value.

3 BUSINESS RELATIONSHIPS & RESPONSIBILITIES



3.1 DEALING WITH BUSINESS PARTNERS

(1) Prohibition of bribery and corruptibility

Periskop **does not** tolerate **any unethical business behaviour** such as **corruption, bribery** and **dishonest gain**. Therefore, Periskop refrains from improperly influencing business decisions by giving or accepting improper benefits of any kind.

Periskop has issued an **anti-corruption guideline** that regulates further details.

(2) Gifts and invitations/ Sensitive treatment of public officials

Periskop has set out the principles regarding the acceptance, offering, promising and granting of gifts or invitations in the policy for gifts and invitations based on the general standards. Any **improper influence on public officials** is **strictly prohibited** not only for employees, but also for anyone who works for Periskop in any form. When obtaining official authorisations, for example, any appearance of an attempt at bribery must be avoided. Details can be found in Periskop's policy on gifts and invitations, which must be observed at all times.

(3) Prevention of money laundering

Periskop fulfils its obligations to **prevent money laundering** in every respect. The property sector is a segment of the economy that is particularly susceptible to this risk. **All employees** are called upon to **recognise and report unusual financial transactions**. This applies in particular to transactions using cash or via third parties that could give rise to suspicions of money laundering. Any suspected cases must be brought to the attention of the line manager and/or management. Money laundering often occurs as a complex structured transaction and is sometimes difficult to recognise. Our **guideline for the prevention of money laundering and terrorist financing** helps you to better recognise these risks. Further assistance is available from the Compliance Officer.

3.2 AVOIDANCE OF CONFLICTS OF INTEREST

Periskop respects the privacy of its employees and managers and is not interested in personal matters outside the workplace. On the other hand, it is important for all employees and managers to ensure that **professional and private interests are clearly separated. Conflicts of interest can cast doubt on Periskop's integrity and professionalism.** They must therefore be recognised and avoided at an early stage.

Personal relationships with a business partner, e.g. with family members, must **not lead to preferential treatment** of the business partner and our professional position must not be used for personal purposes.

We report possible conflict situations or cases of doubt and resolve them together with our superiors or the management. In this way, we ensure that **business decisions** are made **neutrally** and **in the interests of Periskop.**

Details can be found in the policy on the avoidance of conflicts of interest, which must be observed at all times. Periskop has also issued a policy on employee transactions and the prevention of insider trading, which also contains more detailed provisions.



3.3 TRADE AND BUSINESS SECRETS, ASSETS

(2) Protection of Company assets

Each of us is responsible for the **protection** and **appropriate** and **resource-conserving use of Company assets**. Assets may not be removed from the Company.

Everyone at Periskop is obliged to use Periskop's assets for legitimate business purposes and to protect them from loss or unauthorised use.

(1) Protection of confidential Company information

Trade and business secrets and confidential information are **important assets of Periskop**. All employees are obliged to **treat** information about Periskop or business partners that is not publicly known as **strictly confidential** and to protect it against unintentional disclosure; this also applies to facts that are expressly marked as confidential or whose need for confidentiality is recognisable. This applies in particular to important **intellectual assets** such as **patents, trade and business secrets, trademarks** and **copyrights**, but also to **funding conditions**. The duty of confidentiality continues to apply even after employees have left the Company.

Periskop has issued an organisational guideline on the protection of confidentiality, which contains more detailed provisions.



4 INFORMATION SECURITY & DATA PROTECTION

4.1 IT SECURITY & GOVERNANCE

By IT security & governance, we mean the **responsible and compliant handling** of digital systems, data and information. All Periskop employees are obliged to comply with technical and organisational measures to protect our IT infrastructure - from **secure passwords** to the **prudent handling of sensitive information**. Only by working together can we prevent cyberattacks, data loss and system failures. IT governance also ensures that our IT processes are transparent, controlled and in line with legal requirements. In this way, we not only protect our business foundation, but also the trust of our customers and partners.

4.2 IT GUIDELINES FOR EMPLOYEES

(1) IT basics

All employees are provided with **Company IT equipment** that is to be used **exclusively for work purposes**. The installation of private software and the independent modification of system configurations are prohibited. Updates are carried out centrally by the IT department to ensure a uniform security standard.

(2) Data backup and data protection

Data is backed up automatically **by the system administration**. Local storage on the desktop or mobile devices should be avoided. It is also **prohibited to transfer data unencrypted via external data carriers or cloud services**. If a device is lost or stolen, this must be reported to the IT department immediately.

(3) E-mail and Internet use

The business e-mail account is intended **exclusively for work-related communication**. Spam or phishing emails must be forwarded to the IT department immediately. **The use of the Internet** is permitted within reasonable limits, provided it **does not interfere with the work process**. Visiting security-related websites (e.g. with illegal content) is expressly prohibited.

(4) Handling data and passwords

A central point is the **confidential handling of sensitive data**. The principle of **data minimisation** applies - only relevant and necessary information may be processed. **Passwords must be changed regularly**, must not be passed on and must comply with the Company's internal security requirements (e.g. minimum length, special characters, combination of letters and numbers)

(5) Training and sensitisation

Regular training is offered to strengthen the IT security culture. New employees undergo mandatory familiarisation with the applicable IT guidelines in order to ensure a basic understanding of secure IT use in everyday working life.

4.3 GUIDELINE ON THE USE OF MOBILE DEVICES



The use of mobile devices is subject to clearly defined regulations in order to ensure both data protection and information security within the Company. **The policy on the use of mobile devices** defines how Company-owned and private devices may be used in a professional context.

Employees are obliged to adhere to the guidelines described therein. These include the obligation to **separate work and private use** and the **handling of work-related data on mobile devices**. **Company systems** may only be accessed via **authorised and secure devices**. In the event that a mobile device is lost or stolen, this must be reported immediately to the IT department so that appropriate protective measures can be initiated.

In addition, the **installation of applications** on devices used for business purposes is only **possible to a limited extent** and **requires prior authorisation**. Regular updates and security precautions such as screen locks, encryption and anti-virus programmes are mandatory.

Compliance with this policy is checked regularly. Violations may have consequences under labour law and may lead to restrictions on the use of mobile devices in individual cases.

4.4 DATA PROTECTION

At Periskop, we understand data protection to mean the **responsible and legally compliant handling of personal data** - be it from employees, applicants, customers or business partners. This data is particularly **sensitive and deserves a high level of protection**. All employees are therefore obliged to only collect, store or pass on data if there is a clear purpose and a legal basis for doing so. Both the **General Data Protection Regulation (GDPR)** and internal guidelines apply.

Conscious and careful handling of personal data not only protects the **rights of those affected**, but also the **integrity of and trust in our Company**. Violations of data protection regulations can have significant legal and financial consequences - for Periskop as well as for individuals. It is therefore important to always act prudently when handling data, to seek advice when in doubt and to comply with technical and organisational protective measures. Data protection is not a one-off issue - it is an ongoing part of our day-to-day work.



5 REPORTING & CONTROL

5.1 INFORMATION ON VIOLATIONS & WEAKNESSES IN THE CMS

Our internal guidelines and training courses promote compliant behaviour in everyday working life and provide guidance - but are no substitute for your own judgement. For this reason, anyone who has **questions** or recognises **ambiguities** should contact their **manager**, the **Compliance Officer** or the **management** at any time.

Possible violations or indications of weaknesses in the compliance management system should **be reported early** and **confidentially - in person**, via an **external organisation** or **anonymously** via a protected web portal. Employees who provide information in good faith are protected from any disadvantages - confidentiality is a matter of course.

5.2 CONTACT PERSON & MONITORING



INTERNAL WHISTLEBLOWING LINE:
KRISTINA LOHFINK (COMPLIANCE OFFICER)
PHONE +49 (0) 160 9487 13 48
E-MAIL compliance@periskop.ag

EXTERNAL ANONYMOUS WHISTLEBLOWING HOTLINE:

PHONE +49 800 3800 999 (whistleblowing hotline)
LINK app.legaltegrity.com/report/3cde1f69-f82c-4a55-886a-4a2dd3c952c8

