Code of Conduct
of cyan Security Group GmbH (“cyan”)

Version: 2.0
Effective Date: 1 January 2026
Owner: Legal & Compliance Department
Review Cycle: Annual

1. INTRODUCTION AND SCOPE

This Code of Conduct, which is binding for all employees of cyan, describes the ethical and legal framework that guides our daily actions. It is based on our corporate culture, which is found on trust, reliability, transparency and fairness.
The aim of this Code of Conduct is not to regulate every conceivable situation conclusively, but rather to provide all employees, managers, and executive bodies with guidelines that they can use as a basis for their own decisions and actions in their daily work.
We pay particular attention to competition law requirements, as they affect many aspects of our daily business, for example, in relation to contracts with our partners, tenders, the handling of gifts and invitations, and the protection of confidential information, trade secrets and (sensitive) data.
For us at cyan, it is not only what we achieve that matters, but also how we achieve it.
Managers have a special responsibility: they serve as role models and actively support the communication and implementation of the principles set out in this Code of Conduct.
At the same time, this Code of Conduct serves to further promote and secure the positive working atmosphere that already exists at cyan.
By signing the declaration of commitment attached at the end of this document, all persons working for the company acknowledge the principles of this Code of Conduct and undertake to comply with them in their daily work.

This Code of Conduct forms part of cyan’s overall compliance and sustainability framework and is complemented by additional internal policies, in particular:

- Environmental Policy
- Human Rights / Social Policy
- Supplier Code of Conduct
- Data Protection and Information Security Policies

These documents further specify and support the principles set out in this Code of Conduct and must be applied together.

2. COMPLIANCE PRINCIPLES

For cyan, "compliance" means that we act responsibly and in accordance with the rules, in compliance with applicable laws, internal company guidelines, recognized safety standards, and our ethical values.

This includes, among other things:

- Compliance with the GDPR and the Data Protection Act
- Criminal law, in particular with regard to corruption offenses
- competition and antitrust law
- Compliance with ISO standards and internal information security guidelines (ISO/IEC 27001)
- the application of and compliance with our internal policies, and

cyan Security Group GmbH
ICON Tower 24
Wiedner Gürtel 13, AT-1100 Vienna
T +43 (0) 1 33 66 911-0
office@cyansecurity.com
www.cyansecurity.com
FN 416622f Handelsgericht Wien, UID ATU68749722
Raiffeisenbank Attersee-Süd
IBAN AT05 3436 3000 0005 9279, BIC RZOOAT2L363

- our corporate values:

  Growth: We place the highest value on continuous growth—both personal and organizational. This development is firmly anchored in our culture and is actively promoted.

  Collaboration: Collaboration is at the heart of everything we do. We live an open, respectful, and team-oriented culture that transcends departmental boundaries and is integrated into all processes.

  Ownership: Everyone takes responsibility for their own actions and the collective results. We promote a culture of initiative, in which responsibility is not only assumed but actively shaped with full commitment.

The term "**compliance**" comes from the English phrase "to comply with" and refers to all measures that ensure everyone associated with cyan acts in accordance with the law and our values.

Compliance-related provisions are not only found in the Criminal Code, but also in numerous other legal regulations, such as the Data Protection Act, employee protection, the Employee Act, or even in our internal guidelines.

Violations of these provisions can not only have legal consequences, but also damage trust in our company and our brand, e.g. through negative public reporting. That is why we focus on prevention, transparency, and a culture of compliance throughout the entire company.

cyan applies a risk-based approach to compliance management. Potential legal and ethical risks are regularly identified, assessed, and mitigated through appropriate measures.

3. CORRUPTION, GIFTS AND INVITATIONS

cyan pursues a zero-tolerance policy toward corruption and unethical behavior.

Prohibited:

- Accepting or offering monetary gifts or monetary benefits to influence business decisions
- Offering, promising, or granting benefits to initiate business dealings

Permitted:

- Promotional gifts or invitations of low value, provided no conflict of interest arises and transparency is ensured.

If employees receive an unusually valuable gift from an external or business partner, they are obliged to report this immediately to their manager or the compliance department and may not accept it without prior review and approval.

All employees are required to participate in regular training on data protection, information security, and compliance – at least once per year. Participation is documented and serves to ensure continuous awareness and a consistent understanding of applicable legal and internal requirements.

4. COMPETITION LAW AND FAIR BUSINESS PRACTICES

cyan promotes an open and transparent corporate culture in which employees are encouraged to raise concerns and report potential misconduct without fear of retaliation. Respectful and responsible handling of reports is a fundamental principle at cyan.

cyan is firmly committed to fair competition and strongly rejects any form of anti-competitive behavior. Business decisions at cyan are made independently and autonomously, without any collusion with competitors, bidders, or contractors.

We select our contractors and business partners exclusively on the basis of transparent, objective, and fair performance assessments in accordance with legal requirements and our internal procurement guidelines.

Any unlawful coordination or anti-competitive arrangements with competitors are strictly prohibited.

We treat confidential information from our suppliers, customers, business partners, and employees with the utmost care and do not pass it on.

cyan Security Group GmbH
ICON Tower 24, 15th Floor
Wiedner Gürtel 13, AT-1100 Vienna
T +43 (0) 1 33 66 911-0
office@cyansecurity.com
www.cyansecurity.com
FN 416622f Handelsgericht Wien, UID ATU68749722
Raiffeisenbank Attersee-Süd
IBAN AT05 3436 3000 0005 9279, BIC RZOOAT2L363

This applies in particular to:

- Company data, strategic information, and trade and business secrets
- Personal data processed within the scope of our business relationship

Personal data is processed and transferred only in compliance with applicable data protection laws:

Personal data will only be transferred if it is required by law, based on the express consent of the person concerned, or on a contractual basis that is necessary for the performance of our services. Any data transfer will be carried out in accordance with the applicable data protection regulations and only to the extent necessary.

Our employees are not permitted to use such information for personal gain or for the benefit of third parties.

cyan clearly distances itself from any form of:

- price fixing
- insider trading
- unfair influence on tendering or award procedures

Our Employees are obliged to maintain the trade and business secrets of our partners in accordance with their employment contract obligations, in particular the confidentiality agreement signed upon commencement of employment. In the case of particularly sensitive projects, project-related non-disclosure agreements (NDAs) are also concluded to ensure the protection of confidential information.

Example: A manager offers a supplier preferential treatment in return for the delivery of private IT hardware.

This constitutes an improper acceptance of benefits and a possible case of bribery.

5. FRAUD AND MONEY LAUNDERING

cyan does not tolerate any form of fraud or money laundering.
All employees are obligated to critically assess suspicious business transactions and, if necessary, report them to the appropriate authorities—particularly their supervisor and/or the compliance team. Unusual payment flows, opaque customer structures, or missing beneficial owners are potential warning signs.

6. SECONDARY EMPLOYMENT AND CONFLICTS OF INTEREST

Employees are expected to perform their duties diligently and avoid activities that may conflict with the legitimate interests of cyan. During the term of employment, no self-employed or employed secondary activity or any other gainful occupation may be carried out without prior approval from the employer.

Secondary employment includes all income-generating activities outside of the employment with cyan, regardless of whether they are carried out regularly or occasionally. This also includes the **unpaid assumption of official roles** (e.g., managing director, association leadership, board positions), which must be **reported in writing in advance** to the management.

At cyan, business and private matters must be clearly separated. While we do not dictate how employees spend their free time, **no conflicts of interest may arise** in connection with activities at cyan.

7. CONFIDENTIALITY, DATA PROTECTION AND INFORMATION SECURITY

Personal data, trade secrets, and security-related information may only be processed for specific purposes, securely, and in accordance with applicable data protection regulations.

Our comprehensive IT security policy contains important information and binding instructions on safe and data protection-compliant behavior in the workplace, including end-user guidelines such as the clear desk and screen policy, the installation of software, the secure storage of information, the handling of visitors, the use of Internet tools, and behavior in the event of data loss.

To ensure the protection of sensitive data, all employees are required to complete the annual training courses on data protection and information security offered by the company and to apply the knowledge they have learned in their daily work.

cyan Security Group GmbH
ICON Tower 24, 15th Floor
Wiedner Gürtel 13, AT-1100 Vienna
T +43 (0) 1 33 66 911-0
office@cyansecurity.com
www.cyansecurity.com
FN 416622f Handelsgericht Wien, UID ATU68749722
Raiffeisenbank Attersee-Süd
IBAN AT05 3436 3000 0005 9279, BIC RZOOAT2L363

We have implemented internal IT security policies and guidelines, including an End-User Guideline.

8. USE OF OPEN SOURCE SOFTWARE AND TOOLS

Before purchasing and using external software solutions, cyan must carefully check the license terms, data protection compliance, and relevant security aspects.

9. HANDLING OF CYAN'S MATERIAL RESOURCES

cyan employees are obliged to handle the work equipment provided, such as company cell phones, laptops, or other technical equipment, with care and responsibility. These devices must be protected against unauthorized use, loss, theft, or damage.

If an incident does occur, it must be reported immediately to management, the legal department, and the IT administrator.

Intellectual property such as copyrights, trademark rights, and patents also represent a significant value for the company and must be protected accordingly against unauthorized use or disclosure. This applies equally to our own developments and to the rights of third parties with whom cyan cooperates.

10. INTERNAL AND EXTERNAL COMMUNICATION

Requests that are unusual, difficult to define, interview-like, or critical in nature should be handled with friendliness but firm reserve.

In such cases, the following applies:

- The request will first be recorded;
- Feedback will be provided later, after internal consultation with management;
- External communication is carried out exclusively by authorized persons (e.g., marketing/communications, management).
- Internal information must not be passed on via social media or to third parties.

This is to protect sensitive content and maintain cyan's professional image.

Example: *An employee receives a request from journalists about a security incident and begins to provide details.* → Not permitted, such requests must be forwarded to the relevant communications departments.

Example: *An employee posts on LinkedIn about a security feature that has not yet been released.*→ Breach of confidentiality and potential security risk.

11. REPORTING MISCONDUCT (WHISTLEBLOWING)

When employees observe illegal or unethical practices in their work area or environment and report them to a responsible authority, this is referred to as whistleblowing.

At cyan, we see information provided by employees as a valuable opportunity to identify risks at an early stage, clarify misconduct, and avert potential damage to the company.

We value and protect whistleblowers who provide information to the best of their knowledge, regardless of whether it is reported internally or externally.

12. RESPONSIBILITIES & OBLIGATIONS:

- Reporting misconduct is not only an expression of moral courage, but also falls under the duty of loyalty to the employer under labor law.

cyan Security Group GmbH
ICON Tower 24, 15th Floor
Wiedner Gürtel 13, AT-1100 Vienna
T +43 (0) 1 33 66 911-0
office@cyansecurity.com
www.cyansecurity.com
FN 416622f Handelsgericht Wien, UID ATU68749722
Raiffeisenbank Attersee-Süd
IBAN AT05 3436 3000 0005 9279, BIC RZOOAT2L363

- Employees who discover misconduct or are involved in it themselves should address this openly and contact their line managers.
- Managers who receive a whistleblower report are obliged to inform the compliance team or the legal department.
- Discrimination or sanctions against persons who report corrupt behavior or refuse to participate in it are not permitted at cyan.

12.1. Reporting channels at cyan:

cyan provides a confidential and anonymous whistleblower system. Reports can be submitted via the following channels:

By email to: privacy@cyansecurity.com**.** This address is publicly available on the company website and can therefore also be used by external whistleblowers.

Online whistleblower platform: **Link to anonymous reporting**. Reports are completely anonymous and will not result in any legal consequences.

13. CONSEQUENCES OF VIOLATIONS

Corruption has serious consequences for companies and individuals – not only morally, but also legally.

In addition to criminal penalties such as fines or imprisonment, violations can also result in consequences under labor law, civil law, and disciplinary measures.

A violation of this Code of Conduct and applicable anti-corruption provisions is considered a breach of employment obligations, which, depending on its severity, may result in a warning, dismissal, or removal from office.

In addition, civil claims for damages and repayment or return of benefits received may arise.

Our expectation: All employees should demonstrate through their behavior that corruption will not be tolerated or ignored. Each and every individual contributes to securing and strengthening trust in cyan by acting with integrity.

Example: *Use of company resources for private purposes: An employee uses the company laptop for a side project with a private client.* → Violation of the Code of Conduct→ Warning up to and including dismissal

Example: *An employee submits incorrect travel expenses or working hours in BMD in order to gain a personal advantage***.**→ **Compliance violation and potential grounds for dismissal.**

14. GOVERNANCE AND RESPONSIBILITIES

Overall responsibility for the implementation and enforcement of this Code of Conduct lies with the management.

The Legal and Compliance Department is responsible for the operational implementation, ongoing development, and monitoring of the compliance management system. Managers are expected to act as role models, actively promote the principles of this Code of Conduct, and ensure compliance within their area of responsibility. All employees are responsible for complying with the principles set out in this Code of Conduct.

This Code of Conduct is binding. Changes will be published on the intranet. Compliance is mandatory.

15. APPLICATION TO BUSINESS PARTNERS

cyan also expects its business partners, suppliers, and service providers to adhere to comparable ethical and legal standards.

These expectations are defined in particular through contractual agreements and the Supplier Code of Conduct.

16. MONITORING AND CONTROL

Compliance with this Code of Conduct is regularly reviewed through appropriate measures.

- These include in particular:
- internal controls and audits,
- review of compliance-related processes,
- evaluation of reports received through the whistleblowing system.

The results of these reviews are reported to management and contribute to the continuous improvement of the compliance management system.

17. CONTINUOUS IMPROVEMENT

cyan is committed to the continuous development and improvement of its compliance and sustainability practices.

New legal requirements, regulatory developments, and internal findings are regularly reviewed and incorporated into the further development of the system.

Vienna, January 1, 2026

Markus Cserna

CEO

Cyan Security Group GmbH

cyan Security Group GmbH
ICON Tower 24, 15th Floor
Wiedner Gürtel 13, AT-1100 Vienna

T +43 (0) 1 33 66 911-0
office@cyansecurity.com
www.cyansecurity.com

FN 416622f Handelsgericht Wien, UID ATU68749722
Raiffeisenbank Attersee-Süd
IBAN AT05 3436 3000 0005 9279, BIC RZOOAT2L363