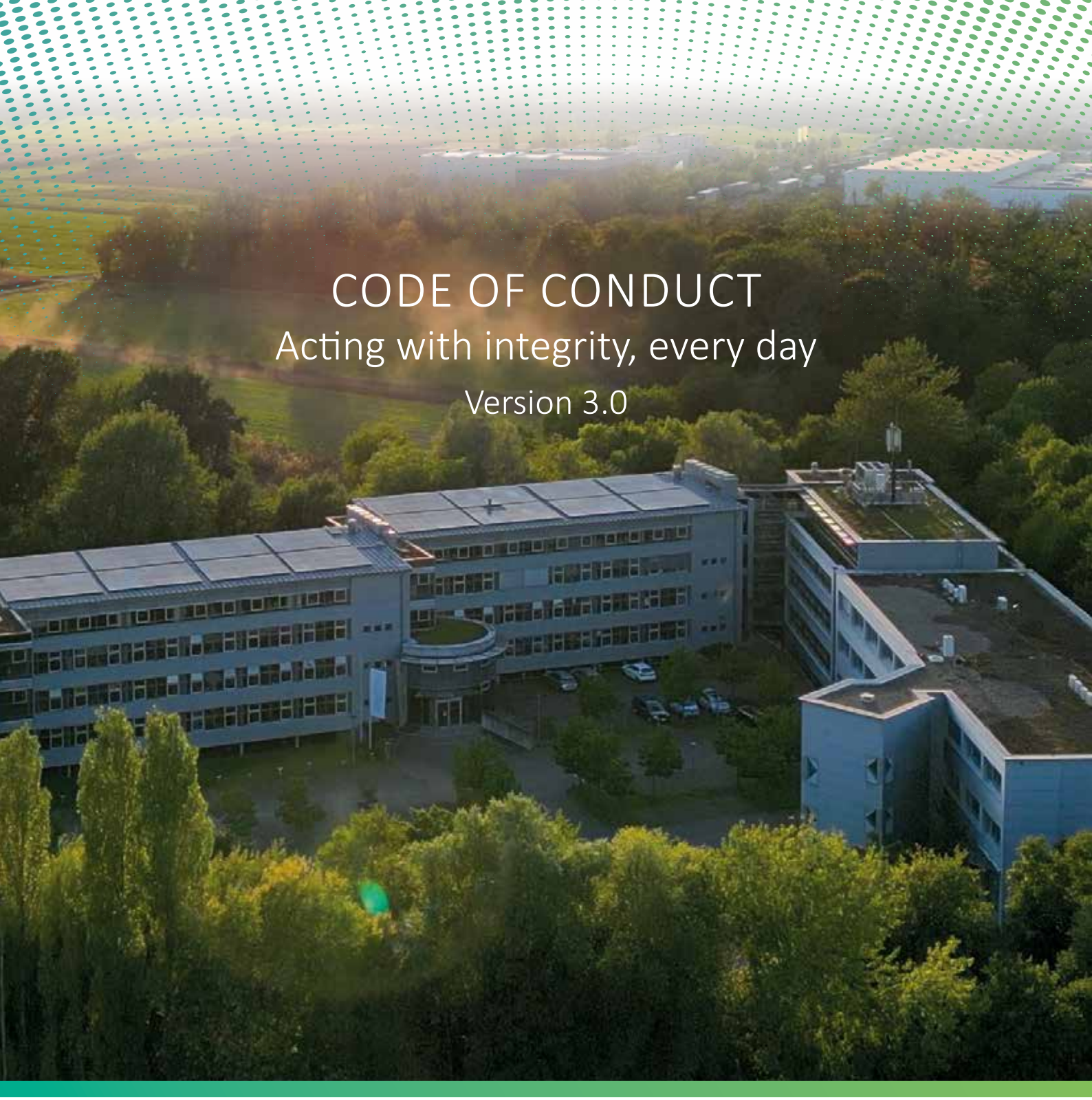


CODE OF CONDUCT

Acting with integrity, every day

Version 3.0

VIVAVIS

IT MEETS ENERGY

CONTENT

Foreword by the Executive

Luis Goncalves, CEO

Dr. Karl Ludwig Kley, CFO

Dear Colleagues,

VIVAVIS stands for trust, team spirit, added value, competence and foresight. These values shape the way we work together and our commitment to acting with integrity. Our success is built on trust. We earn it through reliability, respectful cooperation and followable conduct, every day and in every role.

This Code of Conduct provides guidance. It describes what we expect from ourselves at VIVAVIS. It helps us assess situations correctly and take responsibility. Integrity is not negotiable. It applies at all times, even when it is inconvenient. We expect our managers to lead by example, and all employees to comply with this Code.

Precisely because we develop and operate digital solutions, we bear a special responsibility for data protection, information security and the responsible use of new technologies, including artificial intelligence, cybersecurity and product security.

Please raise questions and concerns at an early stage. Anyone who reports concerns in good faith will be protected. We want to foster a culture in which we communicate openly, take responsibility and learn from mistakes.

Thank you for putting this Code into practice in your daily work.

The Executive Board of VIVAVIS AG

Luis Goncalves

Dr. Karl Ludwig Kley

About VIVAVIS

Purpose of this Code of Conduct and How We Use It

This Code of Conduct describes what we expect from ourselves at VIVAVIS. It helps us make sound decisions in our daily work and provides guidance in difficult situations.

However, the Code cannot address every possible situation in detail. If you are uncertain, seek advice. Use the designated contacts within the respective departments or our reporting channels. Questions are expressly encouraged.

Anyone who reports concerns in good faith will be protected. We seek to foster a culture in which issues are addressed openly and responsibility is actively assumed.

Who We Are and What We Stand For

VIVAVIS develops and operates software, systems and services that support digital processes in networks, facilities and organizations. Our solutions help connect, control and operate processes reliably. Our activities include development, project implementation, integration, operation and support services.

We work for customers in the energy and water sectors as well as for other public and private clients. Depending on the respective company and business area, our activities range from software and system solutions to data and AI services, as well as installation, project and operational services. Together, we pursue one common goal: creating robust and future-proof solutions that make our customers' daily operations simpler, more transparent and more reliable.

Our conduct is based on integrity, responsibility and respect for people, the environment and society. We handle information with care, protect confidential data and safeguard the security of our systems and products. In doing so, we strengthen trust among our customers, partners and within VIVAVIS itself.

Our Framework and Our Responsibility

Scope and Binding Nature

This Code of Conduct applies throughout VIVAVIS. Within this Code, "VIVAVIS" refers to VIVAVIS AG, its foreign subsidiaries and all other subsidiaries[1] of the Group. The Code applies to all employees, managers and corporate bodies. It also applies to individuals acting on behalf of VIVAVIS where contractually or organizationally required. We expect third parties acting on our behalf to comply with equivalent standards.

The Code is reviewed regularly and updated where necessary. It does not replace the applicable law. Where conflicts arise with local laws, the legal requirements take precedence. Where a more in-detail regulation is required, this Code refers to additional policies and processes.

We act in accordance with applicable legal requirements as well as our internal policies and management systems. These include, in particular, the General Data Protection Regulation (GDPR), the EU Artificial Intelligence Act, the NIS 2 Directive and the Cyber Resilience Act, where applicable to VIVAVIS.

Our Guiding Principles

Our understanding of responsible business conduct is aligned with internationally recognized frameworks, particularly the OECD Guidelines for Responsible Business Conduct and the Ten Principles of the United Nations Global Compact relating to human rights, labour, the environment and anti-corruption. These principles complement legal and internal requirements and help us make decisions in a consistent and transparent manner.

Leadership and Responsibility

Managers bear a special responsibility. They lead by example, act transparently and support employees in addressing questions and making decisions. They create an environment that encourages open communication and ensure that concerns are taken seriously. Protection against discrimination, disadvantaging and retaliation is mandatory.

All employees are expected to be familiar with this Code, comply with its requirements and seek advice when in doubt. Policies, procedures and designated contacts serve as resources whenever further clarification is required.

[1] AMW Anlagen-Montagen Werder GmbH, Berg GmbH, CAIGOS GmbH, eoda GmbH and VIVASECUR GmbH.

Our Values as a Guide

Our corporate mission statement, "Acting with Integrity", defines the values of trust, value creation, foresight, competence and team spirit as the foundation of our daily conduct. Our leadership principles further describe how leadership and collaboration should be practiced, including responsibility, communication, innovation and strategic thinking. These principles complement the Code of Conduct. They demonstrate what we stand for as a company. This Code of Conduct explains how we put these values into practice as binding standards in our everyday work.

Questions and Concerns, Protection Against Retaliation

Questions and concerns help us improve. We encourage all employees to seek guidance at an early stage and to raise inconsistencies, risks or potential violations. In many cases, this may begin with a discussion with their manager or another appropriate point of contact. Reports and concerns are handled confidentially and assessed fairly. Protection against discrimination and retaliation is a fundamental principle of VIVAVIS.

If a matter cannot be resolved directly, or if confidential reporting is appropriate, employees may use the channels described in the section "Whistleblower Protection and Reporting Channels."

Implementation, Training and Updates

Executive management is committed to this Code. Compliance coordinates its implementation. The responsible specialist functions support employees and provide guidance where required, including Information Security, Data Protection, Human Resources, Legal, Occupational Health and Safety, and Sustainability. Employees receive regular training. In the event of significant revisions, VIVAVIS may require employees to acknowledge the Code, for example through a brief electronic confirmation or participation in training.

This Code is reviewed regularly and updated where necessary. Amendments will be communicated accordingly. Questions and comments may be addressed to Compliance or submitted through the designated reporting channels.

Addressing Reports of Misconduct Fairly and Taking Action

Reports of misconduct and identified irregularities are reviewed fairly, confidentially and without undue delay. All parties involved are treated with respect. Relevant information is gathered and documented in a transparent and traceable manner. Cooperation with investigations is part of our responsibilities.

Where violations are confirmed, appropriate action will be taken. Such measures may include coaching, training, process improvements or employment-related actions up to and including termination of employment. With regard to business partners, contractual measures may be taken, including termination of the business relationship. Where legally required or otherwise appropriate, the relevant authorities will be involved.

Retaliation against anyone who raises concerns in good faith or assists in an investigation is prohibited.

Integrity in Our Business Activities

Integrity and Conflicts of Interest

Conflicts of interest may arise from time to time. What matters is that they are identified early and disclosed transparently. What we avoid situations in which personal interests could influence business decisions or create the appearance of improper influence. Existing or potential conflicts of interest must be raised promptly with a manager or Compliance and resolved in accordance with internal requirements. Examples include secondary employment, financial investments, personal relationships with customers, suppliers or applicants, as well as the acceptance of benefits or advantages.

What we do

- We disclose a personal relationship with a person involved in a tender, procurement or recruitment process, document our involvement and withdraw from the decision-making process
- We notify the company of planned outside employment in an industry-related business and commence such activity only after approval has been granted
- We disclose financial interests in suppliers or sales partners and refrain from participating in related decisions

What we avoid

- Participating in selection or procurement decisions involving close relatives or personal partners
- Privately engaging a service provider that we manage within the same area of responsibility
- Using internal information or contacts to obtain private benefits, including discounts, preferential terms or preferential treatment

Anti-Corruption and gratuities

We protect ourselves and our business partners through ethical conduct. Corruption, bribery and unfair business practices have no place at VIVAVIS. This applies equally in our dealings with customers, business partners, intermediaries, public authorities and public-sector clients. We actively oppose corruption in all its forms and align our conduct, among other things, with Principle 10 of the UN Global Compact.

Gifts, invitations and hospitality may form part of normal business relationships. However, they are only permissible within reasonable and local customary limits and must never create any expectations of preferential treatment, or even the appearance thereof. We neither offer nor accept hidden payments or improper benefits. This includes so-called “facilitation payments”, meaning small payments or advantages intended to accelerate processes or influence decisions, regardless of amount, location or assumed local practice. Gratuities provided to public officials (for example employees of ministries, local authorities or state-owned enterprises) are subject to particularly strict standards. Donations and sponsorships must be transparent, purpose-specific and approved through documented procedures. Political contributions and political sponsorships may only be made through the designated approval process and must be fully documented. Benefits in connection with procurement procedures or governmental decisions are strictly prohibited. Whenever doubt exists, Compliance must be consulted. Further details and approval requirements are defined in the Anti-Corruption Policy.

What we do

- We review invitations to professional events that include social programmes, document the business purpose and appropriateness, obtain the necessary approval and participate only where no decision-making conflict exists
- We may accept a small and customary gift from a customer at the conclusion of a project, provided it has been reported, its value documented and accepted, and it is given without any expectation of reciprocity
- We request donations and sponsorships transparently, disclose purpose and intended reward, and process payments only after documented approval through approved channels

What we avoid

- Cash gifts, cash-equivalent vouchers and hidden gratuities
- Gratuities provided shortly before or during procurement procedures, evaluations or governmental decisions, particularly where public officials are involved
- Facilitation payments or the use of non-transparent intermediaries to circumvent rules and controls

Political Advocacy and Interaction with Public Officials

We represent the legitimate interests of VIVAVIS in a transparent, objective and compliant manner. Contacts with public officials, authorities and public-sector customers are conducted through approved channels, are appropriately documented and comply with applicable laws as well as internal requirements. Improper advantages are strictly prohibited. Political contributions and sponsorships in a political context may only be made following documented approval and for clearly defined purposes.

We participate constructively in industry associations, expert bodies and standardization committees. We maintain a strict distinction between company positions and personal opinions and always adhere to the principles of fair competition.

What we do

- We openly disclose our role, coordinate public statements in advance and use approved communication channels
- We document significant contacts in the prescribed form
- Within associations and industry bodies, we share only information that is objectively necessary and not competitively sensitive

What we avoid

- Providing gratuities or advantages to public officials or creating the impression of improper influence
- Informal agreements regarding procurement procedures, as well as exchanges of prices, margins, bidding plans or customer allocations
- Using external intermediaries to circumvent transparency or conduct requirements

Third Parties

Our business partners shape how we are perceived externally. For this reason, we engage suppliers, intermediaries, consultants and other business partners carefully and on the basis of clear and transparent criteria. Procurement decisions are made objectively, transparently and in a properly documented manner. Prior to engagement, and at appropriate intervals thereafter, we conduct risk-based due diligence on third parties in accordance with internal requirements. This includes consideration of human rights and social risks within the supply chain, including modern slavery and conflict minerals. We expect our business partners to acknowledge and comply with our Supplier Code of Conduct and, depending on risk exposure, to provide reliable commitments and supporting evidence.

Agreements must clearly define services, reciprocal obligations and duration. Compensation arrangements, payment channels and responsible contacts must be transparent. Third parties must never be used to circumvent rules or exert improper influence on decisions. Any concerns or irregularities are addressed promptly, and relevant activities are suspended until clarification has been obtained. This requirement also applies to lobbyists, public affairs consultants, law firms, associations and their subcontractors.

What we do

- Before engaging a third party, we conduct a risk-based integrity review, clearly define services and compensation, identify responsible contacts and specify the agreed payment method
- We require acceptance of the Supplier Code of Conduct and, where risk levels are elevated, request evidence relating to labour conditions, human rights and conflict minerals
- If irregularities arise, such as changed bank account details, requests for cash payments, unusual advance payments or missing documentation, we halt the process, clarify the commercial rationale and proceed only after documented resolution

What we avoid

- Success-based compensation arrangements without clearly defined and verifiable reciprocal deliverables
- Payments to personal accounts, uninvolved third parties or cash payments without approval, proofs of receipt, supporting evidence or contractual basis
- Backdated quotations, sham offers or service reports devoid of content used as the basis for invoicing

Anti-Money Laundering, Sanctions and Export Controls

Financial integrity is essential for VIVAVIS. We prevent money laundering and comply with applicable sanctions and export control requirements. Business relationships and transactions are conducted transparently and are reviewed on a risk-based approach where appropriate.

This includes payments, deliveries, software, technology and technical support. Any irregularities are raised promptly, and transactions involving unresolved concerns are suspended until clarification has been obtained. Where necessary, the identity of contractual counterparties, beneficial owners and the purpose of a transaction must be established. We do not use third parties to circumvent export control, sanctions or regulatory requirements. Where appropriate, we assess end-use and end-users on a risk-based basis, particularly in connection with software incorporating encryption functions, remote access capabilities, certain cyber-surveillance functions or other applications falling within the scope of the EU Dual-Use Regulation. Questions and uncertainties must be escalated to Compliance.

Specific requirements are determined by applicable law and internal procedures.

What we do

- We identify business partners and beneficial owners, screen applicable sanctions lists and document the results prior to transactions
- For deliveries, software or support involving encryption, remote access or potential dual-use relevance, we review export control requirements and obtain any necessary authorizations
- We accept unusual payment methods, such as third-party accounts, split payments or cash payments, only with a documented business justification and appropriate approval; otherwise, the process is suspended pending clarification

What we avoid

- Transactions involving sanctioned persons, organizations or destination countries
- Circumvention of sanctions through alternative routes, shell companies or chain transactions
- Deliveries, software transfers, remote access or technical support without required export authorizations or without adequate review of the end-user and intended end-use

Account Books, Records and Tax Integrity

Reliable accounts and records are the basis for trust, sound decision-making and legal compliance. Business transactions must be recorded completely, accurately, promptly and in a traceable manner. Supporting documents must be maintained properly and retention periods must be observed. If we receive a legal hold notice or a preservation requirement in connection with legal proceedings, we immediately suspend deletion processes and preserve the affected information without alteration.

Requests from authorities and regulatory audits are coordinated through the responsible functions, and information is provided completely, accurately and on time. Documents must not be altered or destroyed where retention obligations exist. Accounting entries, reports and disclosures must be truthful.

Fraud and misappropriation are not tolerated. This includes fictitious engagements, sham contracts, kickbacks, hidden rebates, manipulated time or performance records and the splitting of orders to circumvent approval requirements.

We address suspected cases, report them through the designated channels, and withhold payments pending clarification.

What we do

- We record transactions completely and promptly, supported by appropriate documentation, performance periods and correct cost allocation
- We report travel expenses, reimbursements and working time accurately, provide original supporting documents and clearly identify private portions
- In the event of a legal hold, we immediately suspend deletion routines, secure affected data and transparently document any changes

What we avoid

- Off-book transactions, shadow accounts and the splitting of contracts or supporting documents to avoid approval requirements
- Backdated documents, fictitious agreements, sham proposals or duplicate reimbursement claims
- Manipulation of time records, service records, cost centre allocations or tax information

Fair Competition

We win fairly. This protects our customer relationships, our reputation and trust in VIVAVIS. We comply with antitrust and competition laws and the rules of fair competition.

We do not enter into agreements with competitors concerning prices, bids or offers, margins, markets, customers or other competitively sensitive topics. When participating in associations, working groups, consortia, bidding groups and events, we limit exchanges to what is objectively necessary and share only information that is public or clearly non-sensitive. For consortia and bidding groups, we define scope, roles, permissible information flows and cooperation arrangements in advance, obtain legal review and document decisions and withdrawals.

If discussions become problematic from a competition-law perspective, we terminate the discussion, leave the meeting and seek guidance from Compliance without delay.

What we do

- At meetings with competitors, we restrict discussions to public or clearly non-sensitive information. If pricing, margins or bidding plans are raised, we end the discussion, leave the meeting and document the incident
- We do not use competitor information received unsolicited. We document its receipt, inform the sender and involve Compliance
- Before commencing consortium or bidding-group activities, we define scope, roles and permissible information flows in writing, obtain legal review and document decisions

What we avoid

- Agreements on prices, bids, margins, market allocation or customer allocation
- Informal discussions concerning ongoing or planned offers, including conversations outside formal meetings
- Exchanging sensitive competitive information, including pricing calculations, quantities or strategic plans

Customer Interests and Honest Communication

Customers rely on accurate and reliable information. Statements concerning our products and services, including sustainability-related claims, must be clear, specific and substantiated. Sustainability or environmental claims may only be made where supported by a sound basis. General or vague statements lacking verifiable evidence must be avoided. Information concerning performance, security and intended use must be honest and understandable. This includes assumptions, limitations, data sources, relevant standards and service levels where these are relevant to customer decisions.

Statements made on behalf of VIVAVIS are issued only through approved contacts and communication channels. This also applies to participation in consultations and legislative processes.

Non-public information relating to customers, business partners or VIVAVIS must never be used for securities trading or for providing investment tips to others. If in doubt, guidance should be sought.

What we do

- We make efficiency or CO_2 reduction claims only where supported by reliable data, specifying the relevant period, baseline and methodology and making evidence available upon request
- In proposals and presentations, we disclose conditions of use, dependencies and limitations, such as required interfaces, minimum software versions or methods used to measure service levels in service level agreements
- We formulate forward-looking statements realistically, describe interim steps and timelines and clearly identify them as plans rather than guarantees

What we avoid

- General sustainability claims that lack a verifiable basis or imagery suggesting benefits that cannot be substantiated
- Omitting material exceptions relating to availability, security, as well as giving performance figures that apply only under ideal conditions
- Using non-public information about customers, partners or VIVAVIS for securities transactions or for providing investment tips to third parties

RESPECT FOR PEOPLE, HEALTH AND THE ENVIRONMENT

Respect, Diversity and Fair Treatment

We work together with respect and create an environment in which everyone can contribute their strengths. Diversity and equal opportunity shape our collaboration within teams, with managers and with our business partners. Respect is reflected in our language, our decisions and our daily interactions, whether in the office, working remotely, at customer sites or on construction sites. Harassment, discrimination and bullying are inconsistent with our values. Managers have a particular responsibility to act as role models. They foster an open culture of dialogue, address inappropriate behaviour and support affected individuals.

In our daily work, we communicate respectfully, provide constructive feedback and take differing needs into account, for example regarding working hours, accessibility or religious observance where operationally feasible. We address concerns at an early stage and seek support whenever needed. Reports are handled confidentially. Individuals who raise concerns in good faith are protected.

What we do

- We communicate respectfully in emails, chats and meetings, stop inappropriate comments and redirect discussions back to professional matters
- We provide feedback objectively, preferably in private, listen actively and work together to find solutions
- We accommodate legitimate needs, such as accessibility requirements, working-time arrangements or religious considerations, and comply with customer and site-specific rules

What we avoid

- Offensive, Degrading, suggestive or exclusionary remarks
- Public humiliation, ridicule or ignoring inappropriate conduct
- Retaliation against individuals who raise concerns in good faith or seek assistance

Human Rights and Working Conditions

We recognize our responsibility to respect human rights. This commitment is reflected in our voluntary Human Rights Policy Statement. Our due diligence processes are aligned with the UN Guiding Principles on Business and Human Rights and the OECD Guidelines for Responsible Business Conduct. Our principles concerning labour and social standards reflect Principles 1 through 6 of the UN Global Compact.

Although VIVAVIS does not currently fall directly within the scope of the German Supply Chain Due Diligence Act (LkSG), we align our human-rights due diligence processes with its core elements. These include risk analysis, preventive measures, remediation, accessible grievance mechanisms and appropriate documentation. For practical implementation, we rely on the guidance issued by the German Federal Office for Economic Affairs and Export Control (BAFA) concerning risk analysis and complaint procedures.

We support decent work, reject child labour and forced labour, and respect freedom of association. We implement internationally recognized labour and social standards.

Our expectations of business partners are further specified in our Supplier Code of Conduct. We expect compliance with internationally recognized human rights and safe and fair working conditions. Where risks arise, we implement preventive and remedial measures and make use of grievance mechanisms. We seek transparency throughout our supply chains and work with our partners to improve conditions wherever risks are identified. Particular attention is given to risks relating to modern slavery, child labour and conflict minerals, which we assess and address on a risk-based basis.

Where indications of risks or potential violations arise, we address them promptly and use the designated reporting channels where appropriate.

What we do

- Before starting a project or selecting a supplier, we assess and document human-rights risks and agree on concrete preventive measures where elevated risks exist
- We immediately investigate indications of child labour or forced labour, suspend orders where necessary, implement corrective measures and monitor progress
- We respect employee rights, including freedom of association and access to grievance mechanisms, and ensure that working hours, rest periods and travel requirements are planned in compliance with applicable laws

What we avoid

- Awarding business to partners that clearly fail to meet minimum standards regarding occupational safety, wages or working hours
- Ignoring warning signs identified through audits, site visits or reports within the supply chain
- Contractual provisions that restrict legitimate grievance mechanisms or disadvantage individuals for raising concerns

Occupational Health and Safety

Health and safety in the workplace are non-negotiable. We share responsibility for maintaining a safe and healthy working environment. We act proactively, report hazards and near misses at an early stage and stop work whenever an immediate danger exists. Prevention is supported through clear procedures, training and appropriate conduct in daily operations. These principles also apply when working at customer sites, on construction sites and in cooperation with subcontractors and partner companies. Mental and social aspects of workplace safety are equally important.

Working under the influence of alcohol, illegal drugs or improperly used medication is prohibited. Where signs of impairment are observed, we address the situation, refrain from commencing safety-critical activities or stop such activities immediately and seek support. Preventive and assistance programmes are available on a confidential basis.

At our locations, we maintain occupational health and safety management systems and implement appropriate measures to prevent accidents and work-related illnesses. Specific requirements are determined by applicable law and internal policies.

What we do

- We report hazards and near misses immediately, stop work in cases of immediate danger and secure the affected area
- We use personal protective equipment and follow work instructions, while also observing customer-specific safety requirements at external sites
- Where signs of excessive workload or impairment exist, we redistribute tasks, schedule breaks and request appropriate support

What we avoid

- Continuing safety-critical work despite a known hazard or missing authorization
- Working under the influence of alcohol, illegal drugs or misused medication
- Ignoring risk assessments, safety instructions or protective measures, whether on construction sites or during off-site assignments

Sustainability and the Environment

Sustainability and environmental responsibility are integral to our corporate responsibilities. We use resources efficiently and work continuously to reduce negative environmental impacts. Environmental considerations and life-cycle thinking are integrated into development, operations and service delivery.

We develop solutions that help our customers improve efficiency and use resources more responsibly. We follow a precautionary and responsible approach and promote environmentally friendly technologies in accordance with Principles 7 through 9 of the UN Global Compact and the expectations set out in the OECD Guidelines.

These commitments apply at our facilities as well as in customer projects and field operations. We act in compliance with applicable environmental laws and our internal policies. Sustainability-related statements are made only where supported by verifiable evidence and in a manner consistent with the OECD Guidelines. At our sites, we operate environmental management systems and implement suitable measures, including efforts to reduce energy consumption, waste generation and emissions.

What we do

- On construction sites, we protect soil, water, air quality and the surrounding environment from noise and pollution. Hazardous substances are stored safely, and spill-containment measures are used where appropriate. Accidents and releases are reported immediately
- In development, operations and service activities, we consider the full life cycle of products and services, including energy-efficient default settings, update strategies and repair-friendly designs
- In our daily activities, we conserve resources by combining travel where possible, replacing travel with remote meetings, separating waste correctly and ensuring proper return and reuse of project-related packaging materials

What we avoid

- Unnecessary idling of vehicles or generators on construction sites and customer premises, as well as heating or cooling unoccupied rooms
- Disposal without proper waste separation or improper handling of hazardous substances on project sites or customer premises
- Failure to comply with local environmental requirements, including operating hours, noise restrictions and emission limits

Protection of Information, Technology and Products

Data Protection and Information Security

The protection of data and information is a fundamental basis for trust. We safeguard personal data and confidential information. Personal data is processed lawfully, for specified purposes only, and only to the extent necessary in accordance with the General Data Protection Regulation (GDPR).

With respect to information security, we follow a risk-based approach. We protect information through appropriate organizational and technical measures and ensure confidentiality, integrity and availability. Information is accessed strictly on a need-to-know basis, and we comply with internal requirements regarding information classification and handling.

At our locations, we maintain information security management systems aligned with recognized standards, in particular ISO 27001.

We use only approved tools and systems for business purposes. Information security incidents and data protection incidents are addressed promptly and reported through the designated channels.

Further details are set out in the Data Protection Policy and in the policies and procedures of our Information Security Management System (ISMS).

What we do

- We process personal data only to the extent required and, where elevated risks exist, conduct a Data Protection Impact Assessment (DPIA) at an early stage. We document the legal basis for processing and define retention and deletion periods
- We classify information according to its sensitivity and apply appropriate safeguards such as encryption during transmission and storage, role-based access controls and logging of security-relevant events
- We enter into written agreements with data processors, assess their technical and organizational measures and ensure appropriate safeguards when transferring data to third countries

What we avoid

- Sharing sensitive information with unauthorized recipients or through unsecured channels, as well as generating large data extracts without a legitimate business need
- Using product-based personal data for testing, demonstrations or training without anonymization or appropriate authorization
- Processing personal data for new purposes without a legal basis or retaining personal data beyond defined retention periods

Use of Company Resources and IT

We handle VIVAVIS equipment, software, licences and other resources responsibly and with care. For business purposes, we use only approved tools and systems. Software installations as well as the use of cloud services and AI applications are permitted only in accordance with internal requirements. External access to the corporate network is allowed exclusively through approved and technically secure channels as specified by our internal IT.

Credentials must be treated confidentially and must never be shared. Data may be stored and shared only through approved channels and in accordance with its classification and protection requirements. Security controls must not be bypassed. Business information must be stored centrally in authorized repositories. Personal files may not be stored on company systems. Personal devices may not be connected to the corporate network, nor may company systems be used for private purposes. Loss of assets or suspected misuse must be reported immediately.

What we do

- We secure and regularly update company devices, lock workstations when unattended and immediately report loss or theft
- We use only approved software and services and obtain installations through established procedures
- We store business information in designated corporate repositories and manage versions centrally

What we avoid

- Using personal devices within the corporate network or for business access
- Changing security or system settings in ways that weaken security controls
- Using company resources for personal purposes, such as large-scale private printing, personal backups or maintaining personal data collections on corporate systems

Cybersecurity and Product Security

Cybersecurity and product security are fundamental to trust. We protect our systems, data and products against attacks and disruptions and take a risk-based approach. Our security measures are embedded in our Information Security Management System. Security incidents and vulnerabilities must be reported promptly through designated channels, and advice should be sought whenever uncertainty exists. Where products lack conformity with requirements or show security deficiencies, we initiate the required corrective actions and support the notification of affected customers to the extent necessary.

Where applicable, we fulfil our obligations under the NIS2 Directive and cooperate with affected customers in support of their security and reporting processes. For products containing digital elements, we comply with the applicable obligations of the Cyber Resilience Act. This includes ensuring security throughout the product lifecycle, maintaining appropriate technical documentation and managing vulnerabilities appropriately. We also comply with the requirements of ISO/IEC 27001 and all other applicable IT security requirements.

To ensure supply-chain and component transparency, we use internal processes aligned with recognized standards and guidance. Additional details are defined in product, development and information-security policies.

What we do

- We apply security updates for products and operated systems promptly and document all changes in a traceable manner
- We report vulnerabilities through the designated process, assess them appropriately and coordinate remediation measures, including customer notification where required
- In development and operations, we use only approved components, libraries and configurations and document security-relevant decisions transparently

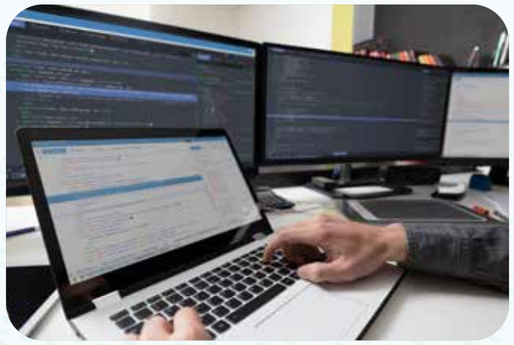
What we avoid

- Releasing or deploying products with known critical vulnerabilities without a documented risk assessment and agreed mitigation measures
- Implementing uncoordinated hotfixes or configuration changes that bypass security standards
- Concealing security limitations or a lack of conformity with requirements from customers or during internal acceptance procedures

Open Source Software and Intellectual Property

We use open source software responsibly. Compliance with licensing and security requirements is essential. We do not incorporate code or components into our work without appropriate review and follow internal requirements regarding selection, assessment and documentation.

We protect both our own intellectual property and that of others. We respect the rights of customers, partners and third parties and use content, software and data only within permitted boundaries. Contributions to open source projects require prior internal approval.



What we do

- We assess open source components for licence compliance and security before use and document applicable disclosure and attribution requirements
- We obtain internal approval before contributing to open source projects and do not disclose confidential information
- We respect the rights of third parties and customers and treat their data, source code and documents with the same care as our own confidential information

What we avoid

- Incorporating code from public repositories or AI-generated output into production solutions without review
- Publishing source code that contains confidential information, keys, credentials or proprietary logic
- Using open source software in violation of licence terms, for example by failing to provide attribution or by ignoring copyleft obligations

Media and Social Media Communication

We communicate clearly, accurately and responsibly. Statements on behalf of VIVAVIS may only be made through approved contacts and communication channels. Official social media accounts are established, designated and managed only by authorized teams. This ensures reliable communication, consistent brand presentation and protection of third-party rights. In social media, we act professionally, review content before publication and correct mistakes transparently. Personal accounts are welcome; however, political opinions must be expressed solely in a personal capacity and not through company channels.

Confidentiality obligations and third-party rights must always be respected. For images, audio and video content, we use only materials for which the necessary rights have been obtained. This also applies to shared content and to content created or modified using artificial intelligence. Media enquiries are referred to the responsible functions, and communications in sensitive situations are coordinated centrally.

What we do

- We make public statements on behalf of VIVAVIS only through authorized spokespersons and approved channels and verify content before publication. Errors are corrected transparently
- We use images, audio and video only where rights have been clarified. For AI-generated content, we ensure appropriate labelling and rights compliance while maintaining a consistent brand presence
- In incidents and sensitive situations, we coordinate communications centrally and forward media enquiries to the responsible function. Personal accounts must clearly indicate that views expressed are personal opinions

What we avoid

- Publishing confidential, customer-related or protected information via social media or public forums
- Operating official accounts without authorization or mixing business content with personal accounts in a way that creates the impression of official corporate communication
- Misleading presentations, including manipulated screenshots, unlabeled AI-generated content, or the use of third-party material without the necessary rights

Digital Technologies and Artificial Intelligence

We use digital technologies responsibly and in a manner that strengthens trust, security and quality. With regard to artificial intelligence, we comply with the applicable requirements of the EU Artificial Intelligence Act. In doing so, we take into account whether we provide AI functionalities ourselves or use AI in our day-to-day business operations and apply a risk-based approach accordingly.

Internal policies and approval requirements apply, these may be supplemented by company-specific provisions within individual group entities. For business purposes, we use only approved AI tools and systems. We ensure that confidential information and data are processed only in accordance with internal requirements. AI-generated outputs are reviewed carefully and are never adopted without verification and double-checking. Whenever uncertainty exists, guidance should be sought at an early stage.

What we do

- Before deploying a new AI functionality, we classify the intended use case, document its purpose, data sources and risks, and obtain the required approval
- We review AI-generated results from a professional and technical perspective and, where elevated risks exist, ensure that a human retains final decision-making authority. We perform testing for accuracy, bias and robustness
- For customer-relevant outcomes, we communicate the use of AI transparently, explain limitations and assumptions, and maintain reproducible evidence supporting the results

What we avoid

- Introducing AI-generated outputs into production environments or deploying them automatically without prior review
- Processing confidential or personal data within unapproved AI services or using training data whose origin has not been clearly established
- Making performance claims regarding algorithms or AI functionalities that have not been tested, documented and demonstrated to be sustainably achievable

Whistleblower Protection and Reporting Channels

In addition to discussions within teams and with managers, VIVAVIS provides confidential reporting channels through which concerns, irregularities and potential violations may be reported. Reports can be submitted in writing, by telephone or, upon request, in person. These channels are open to employees, business partners and external stakeholders throughout our supply chain. Confidentiality is assured, and protection against retaliation is a core principle. Anonymous reporting is also possible.

We acknowledge receipt of a report within seven calendar days of its submission and provide information regarding planned or implemented follow-up measures within three months after acknowledgement of receipt. If, in exceptional circumstances, acknowledgement of receipt is not possible, feedback will be provided no later than three months after expiry of the seven-day acknowledgement period. These timelines ensure transparency and reliability.

At VIVAVIS, we operate a central multilingual reporting portal that assigns reports to the responsible group company. In addition, reports may be submitted through a dedicated reporting-channel email address, through a reporting hotline or through personal meetings by appointment. Current contact details and applicable deadlines are published in the intranet and in the Whistleblowing Policy

We investigate reports fairly, confidentially and without undue delay and document all steps in a transparent and traceable manner. Independent and authorized individuals review the facts and coordinate any necessary measures. If allegations are substantiated, appropriate actions are taken to stop the misconduct, mitigate its consequences and prevent recurrence.

Depending on the country concerned, external reporting channels operated by public authorities may also be available in addition to the internal reporting channels. For Germany, this includes, for example, the Federal Government's external reporting office at the Federal Office of Justice (Bundesamt für Justiz). Country-specific external reporting channels are described in the Whistleblowing Policy.

Notes

VIVAVIS AG
Nobelstraße 18 I 76275 Ettlingen I Germany
T +49 7243 218 0
E info@vivavis.com
www.vivavis.com

(Status: 09.07.2026, Subject to change without notice)