applied®

Code of ethics

6. IT and Cyber security

6.1 IT SECURITY PRINCIPLES
6.2 REGULATORY COMPLIANCE (GDPR, NIS2 AND OTHERS)
6.3 INCIDENT RESPONSE
6.4 CLOUD DATA PROTECTION
6.5 CYBER RESILIENCE
6.6 EMPLOYEES' SECURITY RESPONSIBILITY
6.7 ONGOING TRAINING

7. Innovation, professionalism and sustainability

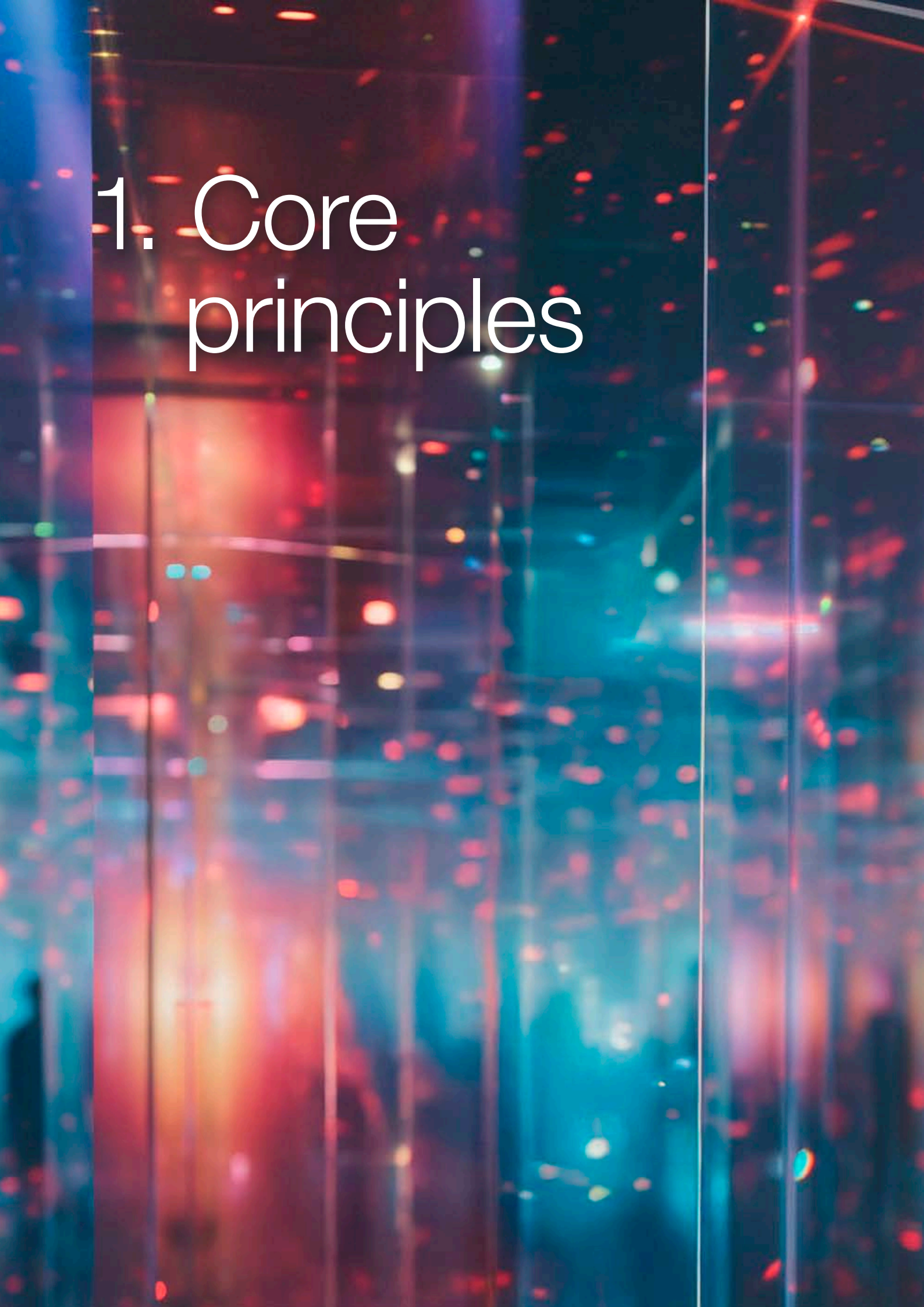
7.1 PROFESSIONAL COMMITMENT
7.2 TECHNOLOGICAL INNOVATION
7.3 ENVIRONMENTAL AND CORPORATE SOCIAL RESPONSIBILITY

8. Legal compliance and reporting

8.1 LEGAL OBSERVANCE
8.2 REPORTING CHANNELS

9. Code of Ethics in artificial intelligence and the use of algorithms

9.1 PRINCIPLES OF ETHICAL USE OF AI
9.2 ETHICAL DATA MANAGEMENT AND AI TRAINING
9.3 CORPORATE SOCIAL IMPACT AND FUNDAMENTAL RIGHTS



1. Core principles

1.1 MISSION AND VISION

Applied was founded with the commitment to provide innovative, secure and customised digital solutions capable of supporting clients' growth and generating value for the entire community.

Our vision is to build a reliable technological ecosystem in which data security, respect for people and sustainability are the fundamental principles that guide every decision, action and business strategy.

This Code of Ethics translates these values into concrete rules of conduct that guide our daily operations and strengthen the trust we wish to establish with our clients, employees, partners and communities. It is an essential reference for ensuring integrity, accountability and transparency in all Applied's activities.

1.2 GUIDING PRINCIPLES

We base our identity of the following principles:

- **Integrity**: always acting with honesty, transparency and consistency, knowing that every choice reflects who we are, with the desire to build a relationship of trust with those who entrust us with their projects.
- **Responsibility**: operating with seriousness, rigour and awareness, contributing to the well-being of the company and the community.
- **Respect**: valuing each person for their uniqueness, promoting an open, inclusive and collaborative working environment. Respect guides us in creating relationships based on listening, empathy and mutual dignity.
- **Security**: carefully protecting the information, data and IT systems entrusted to us. Security is an act of protection towards clients, collaborators and partners, and is an integral part of our commitment to a reliable digital environment.
- **Innovation**: investing in growth and experimenting with new technological solutions with the aim of continuous improvement, putting skills and creativity at the service of people and their goals.
- **Sustainability**: working responsibly towards the environment and society, reducing impacts and supporting a sustainable future, in which progress coexists with respect for resources and communities.

1.3 WHY HAVING A CODE OF ETHICS

At Applied, we believe that ethics is not just a set of rules, but the foundation on which we base all our decisions. The Code of Ethics was created as a practical guide to steer the behaviour of everyone who is part of our organisation or who, in various capacities, collaborates with it.

Through the Code of Ethics, Applied expresses its identity and commitment to promoting a culture based on integrity, transparency and responsibility, in full compliance with national and international laws and best practices.

The Code represents a pact of consistency and credibility: respecting it means protecting not only the organisation, but also the people who make it up and the reputation we build together.

Being part of Applied means sharing the belief that no economic goal, personal advantage or immediate interest can ever justify behaviour that goes against the principles of fairness and responsibility that define how we operate.

2. Code implementation

2.1 DISCLOSURE AND APPLICATION

This Code of Ethics is binding for all employees, collaborators, partners and suppliers who have dealings with the company. The document is made publicly available on Applied's corporate website and on the company's intranet, so that anyone can consult its contents and understand its principles. Every person who works in relation to the company is required to comply with and apply the provisions of the Code, integrating them into their daily professional conduct.

2.2 UPDATES

The Code of Ethics is subject to periodic reviews to ensure its continued consistency with regulatory and technological developments and with the requirements of the company.

Any changes or additions are approved by management and published on the corporate website to ensure full transparency and maximum accessibility for all stakeholders.

3. The value of people

3.1
DISCRIMINATION

Applied promotes a work environment based on respect, fairness and inclusion, and is committed to preventing any form of discrimination or behaviour that undermines personal dignity. The company prohibits any form of unequal treatment based on age, gender, sexual identity or orientation, ethnic origin, nationality, religion, political opinions, disability, health status or trade union membership, guaranteeing equal opportunities for access, growth and professional development at all stages of the employment relationship.

Applied is also committed to maintaining a professional environment free from harassment, abuse and offensive behaviour of any kind. Every position of responsibility must be exercised with impartiality, respect and ethical awareness, avoiding favouritism or unjustified treatment. This is accompanied by the adoption of transparent selection and recruitment procedures based exclusively on skills, merit and consistency with company values.

Compliance with these principles is essential for Applied in order to build an inclusive and sustainable corporate culture that recognises and values diversity as a strategic resource.

3.2
GENDER EQUALITY

Applied recognises gender equality as a fundamental principle of fairness and as a strategic value for the growth of the organisation. The company promotes a working environment in which every person can fully express their skills and aspirations, operating in conditions of equality and mutual respect. To this end, it guarantees equal opportunities in terms of access, career and professional development, regardless of gender, while also ensuring fair remuneration consistent with skills, responsibilities and results achieved.

Applied adopts transparent selection, evaluation and promotion processes based exclusively on merit and competence criteria, and supports work-life balance through inclusive and flexible organisational solutions.

Gender equality is an essential element for Applied in building a corporate culture based on respect, inclusion and the enhancement of people.

3.3
HEALTH AND SAFETY AT WORK

Applied considers the health and safety of people to be a top priority and an essential value for the sustainability of its activities. The company is committed to ensuring a safe, healthy and respectful working environment, ensuring full compliance with current health and safety regulations in all contexts.

Applied promotes a culture of prevention, focused on risk awareness and responsible behaviour by employees and collaborators.

Every worker is required to strictly observe company rules and all safety measures, actively contributing to the creation of a safe working environment. Applied considers safety to be a shared responsibility, requiring the joint commitment of the organisation and the people who work there to ensure safe and sustainable working conditions.

3.4
RIGHT TO ORGANISE

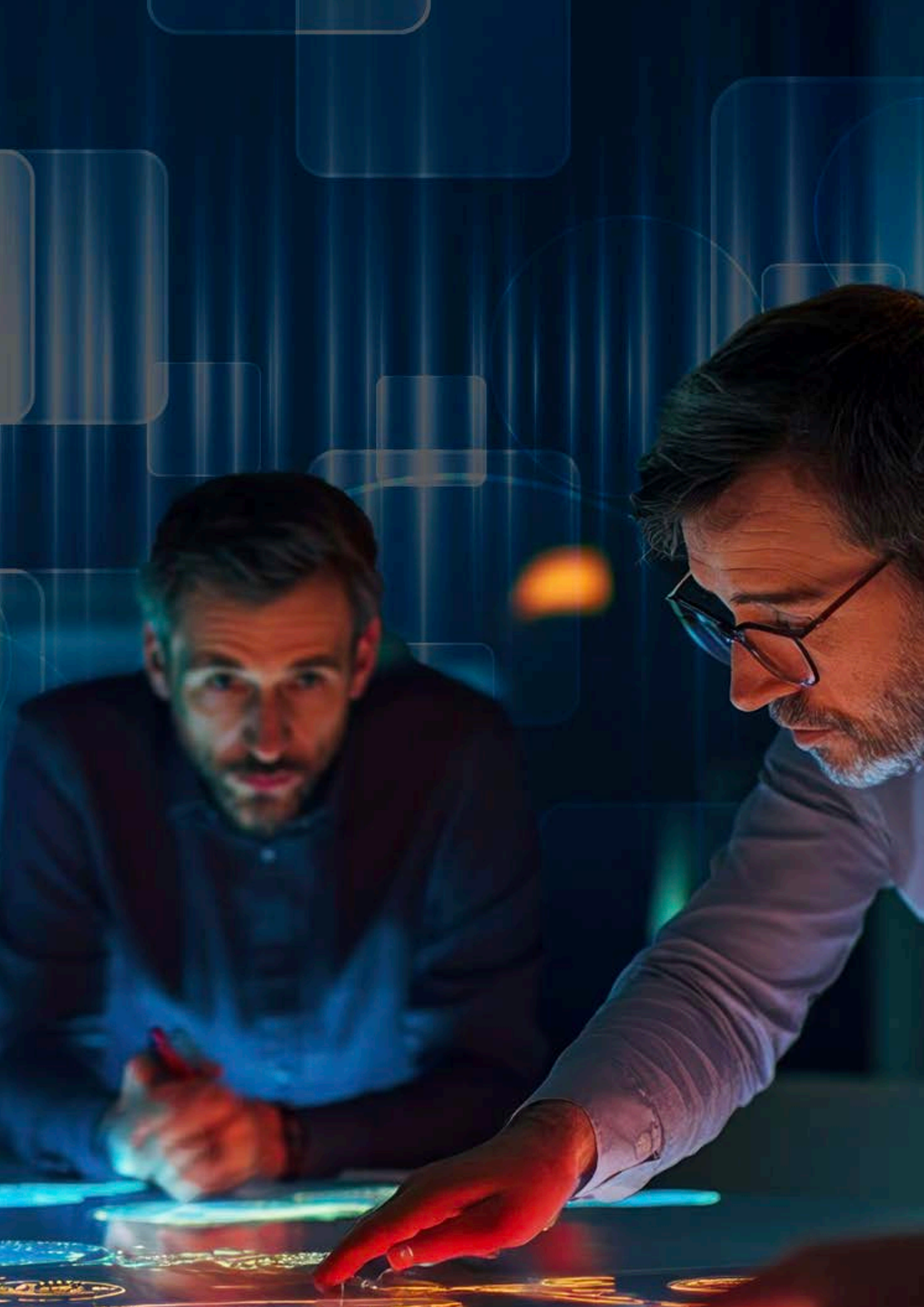
Applied recognises and protects the right of workers to freedom of association, in full compliance with international conventions and applicable national laws. The company guarantees every person the opportunity to join, or not to join, trade unions of their choice, without any form of discrimination.

3.5
TRAINING AND SKILLS DEVELOPMENT

Applied considers continuous training and skills development to be strategic elements for the professional growth of individuals and the sustainable success of the organisation. To this end, it promotes training courses designed to develop each individual and expand both technical and soft skills. Applied invests in professional development and refresher programmes in line with the evolution of technologies, markets and business processes, while fostering a culture based on knowledge and collaboration, in which learning is shared and accessible at all levels of the organisation.

The company also encourages individual responsibility for professional growth, supporting self-managed training initiatives and those characterised by innovative approaches. It guarantees equal opportunities for access to training activities, promoting principles of merit, transparency and inclusion. Applied believes that personal development is a key factor in competitiveness and innovation and invests constantly in enhancing human capital as a distinctive resource for the company.

4. Business integrity



4.1
CONFLICT OF INTERESTS

Conflicts of interest arise when an employee's personal interests conflict, or could potentially conflict, with Applied's interests. All decisions, assessments and activities carried out within the company must be guided by objectivity, impartiality and a sense of professional responsibility.

Any situation that could give rise to a conflict of interest must be reported promptly in order to prevent risks and ensure a transparent and reliable working environment. If an employee finds themselves, even potentially, in a situation of conflict with Applied's interests, they are required to immediately inform their line manager, who will assess the impact and determine the appropriate action to be taken.

4.2
FIGHT AGAINST CORRUPTION

Applied condemns all forms of corruption and prohibits any practice that may encourage corrupt acts in professional, commercial or institutional relationships. Anyone working on behalf of the company is prohibited from offering or accepting money, advantages or benefits of any kind to influence decisions, obtain contracts or gain undue competitive advantages.

Only occasional gifts of modest value and consistent with local customs are permitted, provided that they cannot influence, even potentially, the outcome of business relationships or transactions. Any gift that does not meet these requirements must be refused. Finally, it is prohibited to engage, directly or through third parties, in conduct aimed at improperly influencing government institutions or authorities, or at obtaining favourable treatment in the conduct of business activities.

4.3
FAIR COMPETITION

Applied recognises that the principle of free competition is essential for the development of a dynamic economic environment, benefiting not only consumers but also businesses. Innovation must be conducted in full compliance with intellectual property rights protected by applicable laws.

In order to ensure that Applied always operates within the framework of free and fair competition, it is expressly prohibited to engage in exchanges of confidential information, agreements or arrangements that may, even indirectly, alter the proper functioning of the market or compromise competitive equality between economic operators.

4.4
FRAUD AND MONEY LAUNDERING

Applied bases all its activities on principles of honesty, integrity and fairness, firmly opposing any form of illegal or fraudulent behaviour. Any operation, in Italy or abroad, that could expose the company to the risk of receiving stolen goods, money laundering or involvement with criminal organisations is prohibited.

When entering into commercial relationships, Applied requires thorough checks on the reputation and reliability of its counterparties in order to prevent any possible violation of national and international anti-money laundering regulations. The administrative, accounting and tax systems must guarantee maximum transparency and reliability: all transactions must be recorded in a complete, accurate and truthful manner, in full compliance with company decision-making and authorisation processes.

5. Confidentiality, GDPR and data protection


applied

5.1
DATA PROTECTION PRINCIPLES (GDPR)

The company guarantees full compliance with Regulation (EU) 2016/679 – GDPR and national regulations on personal data protection, ensuring that all processing is carried out in accordance with the fundamental principles established by law. All data collection and processing activities must be carried out in accordance with the criteria of lawfulness, fairness and transparency, ensuring that data subjects are always adequately informed and that processing is justified by clear legal grounds.

Personal data is processed exclusively for specific, explicit and legitimate purposes, avoiding any use incompatible with the purposes for which it was originally collected. The company applies the principle of minimisation, limiting the collection and storage of information to only that which is strictly necessary and ensuring that such data is always accurate, up to date and correct.

Data retention is limited to the time strictly necessary to achieve the stated purposes, in compliance with regulatory provisions and internal policies. The company also adopts appropriate technical and organisational measures to ensure the integrity and confidentiality of information, protecting it from unauthorised access, accidental loss, improper disclosure or destruction.

5.2
ETHICAL DATA MANAGEMENT

The company undertakes to process data in a responsible and ethical manner, taking into account not only legal obligations but also the social and moral implications of using the information. Any use of data that could lead to exploitation, discrimination or human rights violations is prohibited. In projects involving the use of advanced technologies, such as artificial intelligence, machine learning or big data analysis, the company adopts an approach based on the principles of AI ethics, ensuring that algorithms do not generate bias or discriminatory treatment towards individuals or social groups. Every new technology or initiative based on data analysis is subject to an ethical and legal impact assessment to ensure fair and transparent use in line with company values.

5.3
EMPLOYEES' AND COLLABORATORS' OBLIGATIONS

All employees and collaborators are required to comply with internal policies on data protection and privacy. The disclosure, even if unintentional, of confidential information or personal data relating to clients, partners or colleagues is prohibited. In the event of a data security breach, or suspicion thereof, employees and collaborators are required to promptly inform the relevant company representatives so that the necessary measures can be taken immediately to manage the incident.

5.4
IT SECURITY AND DATA ACCESS

Applied adopts appropriate and proportionate cyber security measures, including encryption systems, multi-factor authentication procedures and access controls based on authorisation profiles. Access to data is restricted to authorised personnel and must always be tracked, in accordance with the principle of least privilege, which limits permissions to the minimum necessary to perform tasks. Company information and clients' data must not be stored on unsecure media or shared without adequate protection measures in order to prevent breaches, leaks or misuse.

5.5
RIGHTS OF DATA SUBJECTS

Every person whose data is processed has the right to access, rectify, erase, restrict, transfer and object to the processing of their data, in accordance with current regulations on personal data protection. The company undertakes to provide timely, transparent and comprehensive responses to all requests submitted by data subjects, ensuring full respect for their rights and responsible management of information.

6. IT and cyber security

6.1
IT SECURITY PRINCIPLES

The company recognises information security as a fundamental pillar of its responsibility towards the people and community with which it operates. Protecting the data of employees, suppliers, clients and all stakeholders is not only a regulatory obligation, but also a profound ethical commitment, reflecting the company's desire to build relationships based on trust, transparency and respect.

Therefore, the company has adopted an Information Security Management System (ISMS) compliant with the international standard ISO/IEC 27001, which ensures a structured, documented and certified approach to the assessment and treatment of IT risks. This system allows the company to proactively protect its information assets and ensure business continuity even in the most critical situations.

The company's actions are based on three guiding principles that represent the very essence of IT security:

- **Confidentiality**, so that access to data is always restricted to authorised personnel only.
- **Integrity**, to ensure that information remains accurate, complete and is not subject to unauthorised changes.
- **Availability**, to ensure that the necessary services and information are available when required, even in the event of unforeseen circumstances or incidents.

6.2 REGULATORY COMPLIANCE (GDPR, NIS2 AND OTHERS)

The company operates in full compliance with the GDPR, national legislation and Directive (EU) 2022/2555 – NIS2, which introduces advanced cybersecurity requirements for essential and digital service providers. In accordance with this Directive, the company has adopted technical and organisational measures proportionate to the risks, including continuous monitoring systems, strong authentication procedures and the use of encryption techniques to protect data and infrastructure. The company has also implemented a structured risk management system aimed at identifying, preventing and mitigating cyber threats, together with security incident reporting procedures that require notification to the competent authorities within the time limits established by law. Particular attention is also paid to supply chain management, through policies that ensure suppliers and partners comply with security standards that are adequate and consistent with those adopted internally.

The company is committed to maintaining constant compliance updates, supported by internal checks and periodic audits, to ensure that security and protection levels remain high and in line with regulatory and technological developments.

6.3 INCIDENT RESPONSE

The company has an Incident Response Plan that clearly defines responsibilities, response times and corrective actions to be taken in the event of a cyber attack or data breach, ensuring timely and effective management of critical events. In addition, the company conducts periodic resilience tests to verify the effectiveness of the defence measures adopted and ensure continuous improvement in its ability to prevent and respond to security incidents.

6.4 CLOUD DATA PROTECTION

All cloud services used by the company are selected based on strict regulatory compliance criteria and the presence of appropriate security certifications, including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 and CSA STAR. Data stored or processed in the cloud environment is protected through end-to-end encryption systems, granular access controls and anomaly monitoring tools to ensure high standards of security and information protection.

6.5 CYBER RESILIENCE

The company promotes cyber resilience as an essential capability for withstanding, absorbing and recovering quickly and effectively from any cyber incidents. To this end, it adopts proactive monitoring systems that enable threats to be detected and mitigated promptly, ensuring continuous and constantly updated protection of digital infrastructures.

Employees participate in ongoing training programmes dedicated to cyber hygiene, phishing prevention and social engineering techniques, so that everyone can contribute consciously to the overall security of the organisation. At the same time, the company maintains a dynamic process for assessing emerging risks — such as advanced ransomware, supply chain attacks and AI-based threats — in order to anticipate critical scenarios and constantly strengthen its defences.

6.6 EMPLOYEES' SECURITY RESPONSIBILITY

The company requires all employees to use only authorised software that complies with internal policies, avoiding the installation of unauthorised or potentially risky programmes. Company tools must be used solely for professional purposes, in compliance with IT security procedures and guidelines. Everyone is required to promptly report any security incidents, phishing attempts or suspicious behaviour, thereby contributing to the prevention of threats and the protection of information assets. Company devices — such as computers, laptops and smartphones — must be adequately protected with strong passwords, encryption systems and all measures necessary to ensure their security.

6.7 ONGOING TRAINING

All employees regularly participate in training courses dedicated to GDPR and Cyber Security, in order to maintain a high level of awareness and keep up to date with current regulations and best practices in data protection. The culture of IT security is considered a fundamental element of the company's identity and translates into responsible and careful behaviour on the part of every individual. To further strengthen this awareness, the company carries out periodic internal phishing simulation campaigns, which are useful for testing and improving the ability to recognise and manage cyber attack attempts. These activities are accompanied by a constant flow of training and information communications via dedicated e-mails, which provide updates, practical advice and operational guidelines for the safe use of digital tools.

7. Innovation, professionalism and sustainability

7.1
PROFESSIONAL COMMITMENT

Every customer service is carried out with the utmost attention to technical precision, safety and reliability, ensuring high quality standards and truly effective solutions. Projects are developed taking into account the specific needs of each customer, through customised interventions aimed at achieving the expected results.

Each employee is directly responsible for the quality of their work and actively contributes to the continuous improvement of internal processes, aware that service excellence stems from daily commitment and the care with which all activities are carried out.

7.2
TECHNOLOGICAL INNOVATION

The company promotes and supports the continuous updating of its employees' skills, encouraging training courses, dedicated workshops and self-training initiatives that foster continuous professional growth. At the same time, it encourages the development and adoption of new technologies, ensuring that every innovation is introduced in accordance with the principles of ethics, safety and sustainability.

For Applied, innovation does not only mean introducing advanced technological tools, but also seeking more efficient, collaborative and people-friendly ways of working. Innovation is therefore conceived as a cultural and organisational process, capable of generating value through continuous improvement and the empowerment of all employees.

7.3
ENVIRONMENTAL AND CORPORATE SOCIAL RESPONSIBILITY

The company is aware that the IT sector also has an impact on the environment and promotes eco-efficient practices aimed at saving energy, reducing waste and ensuring the correct disposal of electronic waste (WEEE). The company adopts and encourages working methods with a lower environmental impact, promoting smart working, remote meetings and optimisation of travel, with the aim of contributing to a more responsible use of resources and the overall sustainability of its activities.

8. Legal compliance and reporting

8.1 LEGAL OBSERVANCE

All company activities must be carried out in full compliance with applicable national, EU and international laws, ensuring that conduct complies with regulations at every stage of business operations. Any action or practice that may be unlawful, improper or contrary to current legislation is strictly prohibited, even when such conduct appears to offer a direct or indirect advantage to the company.

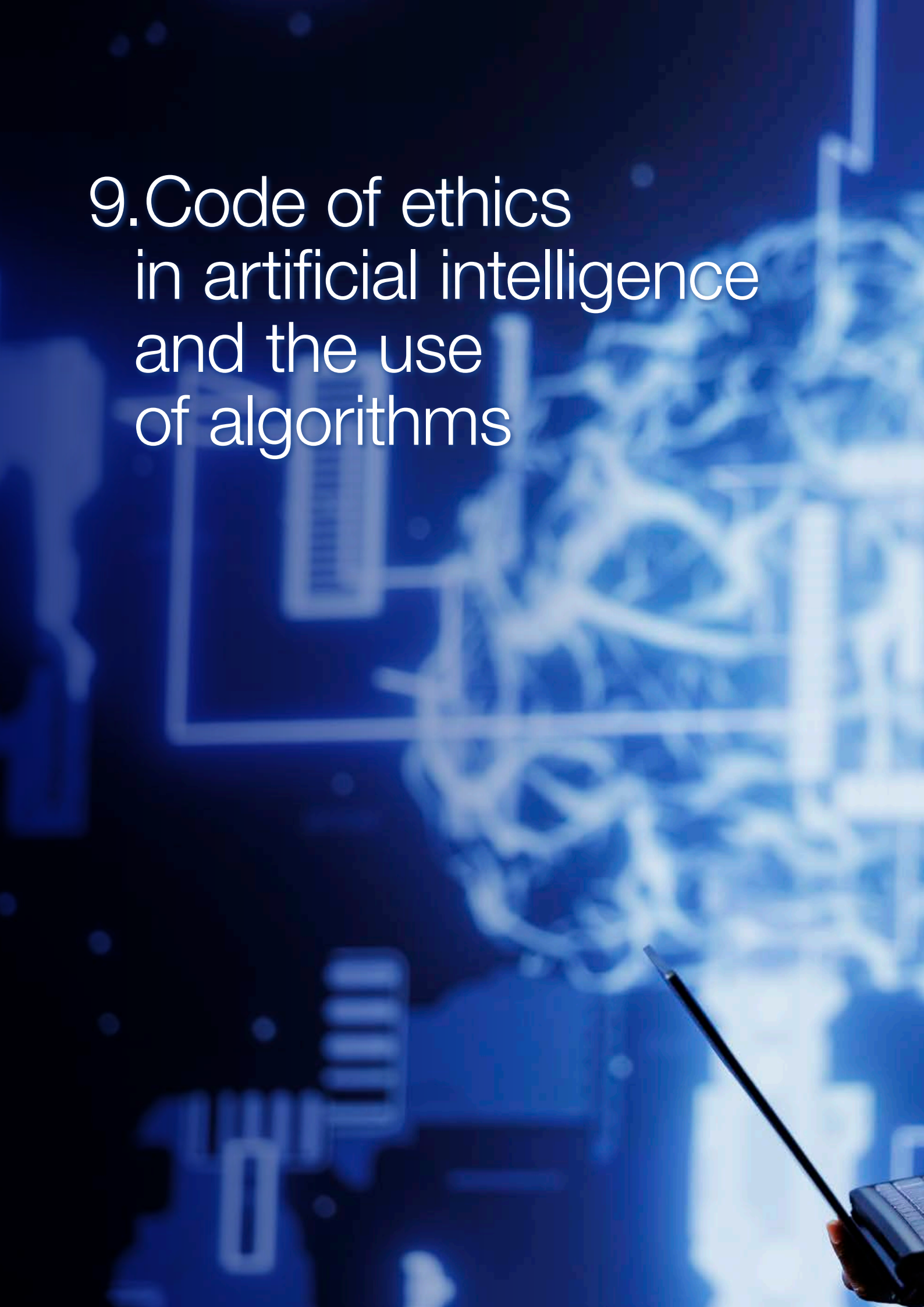
Each employee is responsible for their own actions and is required to behave in accordance with the principles of legality, fairness and transparency, thus contributing to the protection of the organisation's integrity and reputation.

8.2 REPORTING CHANNELS

The company has established a whistleblowing system that allows employees, collaborators, partners and external parties to report any violations of this Code of Ethics, applicable regulations or internal company procedures. Reports may concern illegal or unethical behaviour or behaviour that does not comply with the organisation's rules, and are a fundamental tool for ensuring transparency, legality and integrity in company activities.

All communications received are handled with the utmost confidentiality, protecting the identity of the whistleblower and ensuring that no one suffers retaliation or discriminatory treatment as a result of their report. On Applied's corporate website there is a section dedicated to whistleblowing, which cointains the official channel for submitting reports and the operating procedure to be followed.

Reports are handled according to criteria of impartiality, timeliness and traceability, ensuring accurate analysis of the facts presented and the adoption of any necessary corrective measures.



9. Code of ethics in artificial intelligence and the use of algorithms

9. Code of ethics in artificial intelligence and the use of algorithms

9.1
PRINCIPLES OF ETHICAL USE OF AI

The company recognises that the use of artificial intelligence and data analysis algorithms offers extraordinary opportunities for innovation, but at the same time entails significant ethical and social responsibilities. For this reason, it is committed to ensuring that all AI-based solutions comply with the requirements of the European Regulation on Artificial Intelligence (AI Act), adopting a rigorous, transparent and people-oriented approach.

Every project involving the use of AI systems must be developed in accordance with certain fundamental principles. Transparency is an essential requirement: algorithms must be explainable, adequately documented and understandable to users and stakeholders involved. Equally important is reliability, which is ensured through thorough testing, constant monitoring and maintenance activities aimed at reducing bias, errors and vulnerabilities. The company clearly affirms the principle of human responsibility: every AI application must have an identifiable contact person who guarantees the correct use of the technology and maintains decision-making control ("human in the loop"). Fairness is another key principle, as AI must not generate or amplify discrimination based on gender, ethnicity, religion, sexual orientation, disability or personal characteristics. Finally, security must be guaranteed at every stage of the technology's life cycle, minimising the risks of manipulation, misuse or cyber attacks.

9.2
ETHICAL DATA MANAGEMENT

Ethical data management is a fundamental principle of the company's operations. All data used, whether for training algorithms or for their operation, must be collected and processed in full compliance with the GDPR and current regulations on the protection of personal information. The company applies rigorous procedures for anonymisation, minimisation and security of datasets, ensuring that information is used only when strictly necessary and always under appropriate conditions of protection.

The organisation categorically rejects the use of data from unlawful sources or from processing that may infringe on people's fundamental rights, recognising that the quality, lawfulness and accuracy of data are essential prerequisites for the responsible use of digital technologies. Each dataset undergoes a systematic assessment of quality and ethics, aimed at preventing risks of bias, distortion or discrimination, thus ensuring that the use of data is always consistent with corporate values and respect for human dignity.

9.3
CORPORATE SOCIAL IMPACT AND FUNDAMENTAL RIGHTS

Artificial intelligence applications must be designed and used in full compliance with fundamental human rights, avoiding any use that could be invasive or compromise individual dignity and freedom. The company promotes the use of AI to generate a positive impact on society, contributing to the improvement of processes, increased efficiency and greater accessibility of services, so that technological innovation is always at the service of people and the common good.

Società di riferimento	**APPLIED**
Perimetro di validità	Aziende gruppo Applied
Ambito documento	COMPLIANCE
Codificazione	APPL-COMPL-PL-001
Nome esteso documento	APPL-COMPL-PL-001-Codice Etico-v01
Documento	Codice Etico
Versione	1 del 24/11/2025
Lingua	Inglese
Approvatore	Head of Staff
Autore	Cyber Security & Compliance Manager
Data di approvazione	24/11/2025
Data classification	Pubblico


applied®
innovation makers