Insights into the perspectives of customers and end-users are gathered through surveys, customer contributions, and direct contact via the brands' service hotlines. The Nemetschek Group is not currently aware of any customers or end-users who are particularly vulnerable to the impacts of the Group's business activities or who could be directly marginalized by them. All customers and end-users can address their perspectives equally to the brands or the Group via the existing communication channels. Customer and end-user engagement is primarily managed at the brand level, allowing each brand to tailor its approach to its specific market and target audience. To enhance interaction and collaboration with larger, multinational, and multidisciplinary customers and end-users, the Nemetschek Group implemented a global KAM system in the past fiscal year. The global KAM aims to provide even more tailored support to customer groups, particularly large international customer, based on their individual needs.

Through the customer service of each brand, the Nemetschek Group offers its customers and end-users the opportunity to directly address their concerns, needs, or requests to the respective brand. The customer service function is internally organized within each brand and does not rely on external partners. Customers and end-users can contact Nemetschek Group brands directly via various channels, such as the website, social media platforms, email, and telephone hotline. Since the end of the 2024 fiscal year, the Nemetschek Group's processes, including customer service and support processes, have been ISO-certified across the entire Group (ISO/IEC 27001), with the exception of the GoCanvas brand (and SiteDocs, part of GoCanvas), which was acquired in July of the reporting year. Certification for GoCanvas is planned for the fiscal year 2025. For grievances, customers and end-users of the Nemetschek Group also have access to the global whistleblowing system at the Group level. This whistleblowing system allows customers and end-users to submit complaints to the Nemetschek Group, anonymously if desired. It includes structures and procedures to protect identities and safeguard individuals involved from retaliation.

2.4 Governance Information

Business Conduct

The Nemetschek Group reports relevant disclosures on material sustainability aspects in the area of governance in its sustainability statement, including material information on corruption and bribery as well as the Group's payment practices. For the company-specific topic of Cyber and Information Security, additional material information and relevant metrics are disclosed to assess performance and effectiveness in relation to information security.

Management of Impacts, Risks and Opportunities – Business Conduct

Good corporate governance and taking responsibility for employees, society, and the environment are of great importance to the Nemetschek Group. The Nemetschek Group aims to be a trustworthy, reliable, and honest partner for its customers, business partners, employees, and the general public. Every employee and management shares responsibility for ensuring that the Nemetschek Group fulfills its legal and social responsibilities worldwide. The Code of Conduct, approved by the Executive Board of Nemetschek SE and communicated internally, defines Group-wide behavioral principles in a format that is easily understandable for all employees. It serves as a values-based guideline within the Group. The responsibility to identify, investigate, and prevent unethical, inappropriate, or unlawful behavior is firmly embedded in the corporate culture of the Nemetschek Group.

The three most important topics promoted and communicated as part of the corporate culture are:

Establishing and Evaluating Corporate Culture

- Regular feedback sessions: To measure employee satisfaction and engagement, regular feedback sessions between employees and managers are to be held. Employee surveys are already an integral part of the corporate culture in some brands. The Nemetschek Group is conducting a global employee survey in the first quarter of 2025.
- Professional development: Professional training and career development opportunities strengthen employees' commitment to the Nemetschek Group.
- Recognition of achievements: Individualized recognition of successes aims to motivate employees across the Nemetschek Group.

Development of Corporate Culture

- Management culture: Management acts as positive role model for employees.
- Speak-up culture: Employees have the opportunity to confidentially report concerns via the whistleblower tool or raise questions during hybrid town halls.

A Board Letter to all Nemetschek Group employees is used to communicate key behavioral principles across the Group. Further communication takes place between management and employees in collaboration with HR.

Corporate Legal & Compliance and the risk management function regularly conduct risk analyses. The corporate risk analysis, managed by the risk management function, covers corporate and business risks, among others. The compliance and human rights risk assessments, conducted by Corporate Legal & Compliance, focus on identifying, assessing, and managing specific risk areas within the compliance area, for instance, with money laundering- or antitrust risks; or within the human rights area, for instance, with forced or child labor, anti-corruption or human rights. These analyses also serve to identify grievances and shortage in the respective areas and are further complemented by audits conducted by the Internal Audit function at the Group level.

Furthermore, the Nemetschek Group actively promotes and encourages an open speak-up culture across the entire organization. Employees are encouraged to report any behaviors that may violate the Code of Conduct or other internal or external regulations. To support this, the Nemetschek Group implements proactive communication actions, including regular emails, intranet publications, and executive board communications. A modern whistleblowing system allows grievances to be reported not only by employees but also by external third parties, with the option to submit reports anonymously if desired. This digital platform serves as the whistleblowing system for all brands of the Nemetschek Group, placing special emphasis on whistleblower protection, ensuring confidentiality of involved parties, and maintaining information security. The whistleblowing system is currently available in German, English, and Hungarian.

In addition to the digital whistleblowing system, employees can also directly contact their managers, the responsible HR representative, or the (local or company-wide) Legal & Compliance department. All incoming reports are first reviewed for plausibility with the highest level of confidentiality. If necessary, further investigative actions and steps are initiated. In individual cases, other company branches/functions, as well as external advisors, may be involved. The Corporate Legal & Compliance function serves as an independent internal reporting body, regularly reviews the effectiveness of the whistleblowing process, and adjusts it as needed. The identification, investigation, and remediation of unethical, inappropriate, or unlawful behavior is one of the core principles of the Nemetschek Group and is therefore firmly embedded in the corporate culture. This principle is reflected in both publicly accessible and internally available documents and policies and is regularly communicated by the company (e.g., through email and intranet publications).

All information submitted through one of the Nemetschek Group's whistleblowing channels (e.g., a tip-off to suspected cases of corruption or bribery) is processed via a standardized process that is based on the legal requirements in accordance with Directive (EU) 2019/1937 and the nationally applicable laws for the implementation of the Directive, and thus complies with, among other things, the legal deadlines. This standardized process not only covers tip management and communication following a whistleblowing report but also defines the investigation and remediation actions to be taken after receiving a report. The Corporate Legal & Compliance function of the Nemetschek Group handles and evaluates whistleblowing reports independently and objectively, following a standardized process to safeguard the rights of all parties involved – particularly those of the reporting person.

The Nemetschek Group ensures compliance with these regulations through a mandatory, Group-wide compliance training that covers knowledge on anti-corruption and bribery prevention. The training must be completed at the beginning of employment and must be repeated regularly, in most cases at least every two years, depending on the subsidiary.

Corruption and bribery pose a significant risk not only to the assets and economic success of the Nemetschek Group but also to its very existence. The Nemetschek Group is therefore committed to ensuring that the implemented anti-corruption and anti-bribery actions are mandatory for all employees, fostering a comprehensive awareness of these risks. The Nemetschek Group recognizes that certain functions, particularly those with direct interfaces to external business partners, such as procurement, sales departments, and the Executive Board, are more frequently exposed to corruption and bribery risks.

Nemetschek SE and its subsidiaries based in the EU are subject to Directive (EU) 2019/1937 and the respective national laws implementing this directive. The Nemetschek Group actively promotes an open, Group-wide speak-up culture. To ensure that whistleblowers feel safe when submitting reports, the Nemetschek Group has implemented a range of protective actions. These include clear statements in the Code of Conduct, which explicitly affirm that "no employee will suffer any disadvantage as a result of making a report". This message is further reinforced through additional communication actions, such as flyers and policies available to all employees via the intranet. For whistleblowers who are not employees, the Nemetschek Group provides the necessary information on its corporate website, including an FAQ page, which explicitly states that even if a report later turns out to be unfounded, the reporting person will not face any negative consequences – provided the report was not made with malicious intent.

In addition to communication actions, the Nemetschek Group has implemented (technical) safety precautions within its whistleblowing system. Whistleblowers have the option to submit reports anonymously. Disclosing one's identity or providing infor-

mation that could lead to identification is not required and is not necessary for submitting a report or for subsequent communication during the review process. Even if a whistleblower voluntarily chooses to disclose their identity, this information is only shared when it is absolutely necessary (e.g., in official or legal proceedings) or with the explicit consent of the whistleblower.

The Corporate Legal & Compliance function of the Nemetschek Group processes and evaluates whistleblowing reports independently and objectively in accordance with a standardized procedure to protect the rights of all parties involved – particularly those of the reporting person. This is also reflected in an internal reporting process to the supervisory bodies, which ensures a sufficient overview of the facts to serve as a basis for decision-making. At the same time, it strictly safeguards the privacy and data protection rights of the reporting person and other involved parties. The Nemetschek Group has established a policy regarding its material positive impact, corporate policies, and the promotion of corporate culture. A component of this policy is the "People Letter of Commitment", which is described in *<< 2.3 Social Information >>*.

As a globally operating company, the Nemetschek Group has established relationships with numerous suppliers and business partners that provide the Group with goods and services. The careful selection of suppliers and business partners is a key factor in the profitable growth and reputation of the Nemetschek Group. Rules and principles governing supplier and business partner selection, business transactions, service quality, and risk management serve to strengthen the Group's negotiating position and reduce financial, ethical, and reputational risks.

The Nemetschek Group's Group Procurement Policy, introduced in the 2024 reporting year, provides a framework for procurement activities and promotes good, harmonized practices in procurement, including purchasing and payment practices. The Group Procurement Policy applies to all employees worldwide who are responsible for procurement or are involved in any way in purchasing and procurement processes. The Group Procurement Policy was approved by the Head of Global Procurement and reviewed and endorsed by the Executive Board of Nemetschek SE. The policy stipulates a 30-day payment term, ensuring timely payments to suppliers and business partners.

The principles governing collaboration with suppliers and business partners are also outlined in the Supplier Code of Conduct of the Nemetschek Group. The Nemetschek Group expects its suppliers and business partners, as well as their employees, to act responsibly at all times and to fully comply with the laws, regulations, and policies of the countries in which they operate. Furthermore, compliance with the core principles of the Supplier Code of Conduct, the UN Global Compact (UNGC), and the fundamental principles of the ILO is required. The Supplier Code of Conduct also affirms that the Nemetschek Group is a fair and responsible market participant that adheres to its contractual obligations toward suppliers and business partners.

As an international software company, the Nemetschek Group places great importance on sustainable and responsible supplier relationships. The Group approach considers both supply chain risks and their impact on sustainability aspects. As part of Business Partner Due Diligence, the Nemetschek Group ensures a careful selection of business partners with regard to anti-corruption compliance. In the strategic procurement process, environmental criteria, such as packaging materials, energy consumption, and recycling opportunities, are incorporated into supplier selection, depending on the type of goods and services. These actions actively contribute to reducing indirect environmental impacts.

To further enhance transparency and efficiency in the supply chain, the Nemetschek Group plans to introduce a cloud-based procurement platform. This innovative solution will enable the early identification and mitigation of supply chain risks while strengthening collaboration with strategically important suppliers. The improved availability and quality of data will support more informed procurement decisions.

The integration of environmental criteria plays a key role in the selection of suppliers and contract partners. The modern procurement approach systematically incorporates these aspects and aims to ensure a sustainable and responsible supply chain. Potential partners are evaluated based on sustainability factors, such as energy efficiency and the use of renewable energy sources, waste management, and circular economy approaches. Social criteria that go beyond compliance with the core principles of the Supplier Code of Conduct, the principles of the UNGC, and the ILO are not yet considered in supplier selection. These criteria, alongside factors such as quality, innovation capacity, and pricing, are weighted differently in the overall supplier evaluation.

Incidents of Corruption or Bribery

The Nemetschek Group is fully committed to fair competition and explicitly rejects corruption and bribery. This commitment is based on the firm belief that long-term business success can only be achieved through lawful and responsible conduct, which also has a positive impact on stakeholder satisfaction. An open corporate culture and a well-established Compliance Management System (CMS) are key actions in combating against corruption and bribery. This message is consistently communicated to employees worldwide through "Tone from the-Top" actions, such as the regular Board Letter, which, like the Group-wide Code of Conduct, is published in both German and English and made available on the Nemetschek Group intranet and website. The Code of Conduct has been communicated across the entire Group and is binding for all employees, regardless of their position within the company.

Actual or suspected violations of applicable laws – including anti-corruption and anti-bribery laws – internal standards, or other regulations, are regularly reviewed, identified, and assessed through various risk analyses and audits conducted by Corporate Legal & Compliance, the risk management function, and Internal Audit. The assessment is conducted based on (industry)-standard parameters, including likelihood of occurrence and potential amount of loss. These audits and analyses are further supplemented by the Group-wide whistleblowing system, which serves as an additional mechanism for detecting bribery and corruption risks.

To prevent bribery and corruption, the Nemetschek Group has implemented a range of processes to raise and strengthen awareness of bribery and corruption risks across the organization. As a general principle, employees receive guidelines, instructions, and support materials to help them manage corruption and bribery risks in their daily work. Corporate Legal & Compliance uses various communication channels, including intranet publications, emails, and mandatory e-learning, which incorporates practical scenarios to help employees act in compliance when faced with corruption or bribery risks. Employees also have access to the Group-wide anti-corruption policy, which provides detailed requirements and specifications, refining the principles outlined in the Code of Conduct. This policy is supplemented by additional documents for specific processes and situations, such as guidelines on gifts, hospitality, and corporate event planning. The policy has been globally communicated and implemented across all business units of the Nemetschek Group.

As a global software provider, the Nemetschek Group naturally interacts with a wide range of business partners across its upstream and downstream value chain. To minimize the resulting legal, financial, and reputational risks, such as those arising from allegations of corruption and bribery, the Nemetschek Group has developed a risk-based approach to ensuring compliant and diligent business partner management. This approach includes a selection of risk mitigation actions that employees can choose from depending on the level of risk exposure. This includes the Supplier Code of Conduct, which defines the Nemetschek Group's expectations towards third parties, as well as guidance for employees on how to assess and evaluate potential risks through a due diligence process. Depending on the business partner's risk exposure, the due diligence process may be conducted with varying levels of detail. The guidance provides employees with different courses of action to address these risks.

Finally, the Nemetschek Group has also established a standardized internal investigations process covering all types of compliance violations, including actual or suspected cases of corruption and bribery. This process includes the investigation and management of compliance violations, as well as the development and implementation of remediation actions. The process consistently follows the four-eyes principle and ensures confidentiality.

To fulfill its corporate governance responsibilities, Corporate Legal & Compliance serves as an independent reporting body for evaluating and investigating reported concerns. Specific procedures have been established to prevent conflicts of interest in cases where Executive Board members or Corporate Legal & Compliance itself are subject to reports. In such cases, alternative responsibilities and reporting structures have been defined and documented within the process description. The results of internal investigations are presented to the Executive Board and Supervisory Board in a summarized and abstract format as part of quarterly reporting. This includes, among other things, the appropriate consideration of legal requirements regarding the confidentiality of whistleblowers' identities and data protection regulations. In addition to periodic reporting, ad hoc reporting is conducted if necessary.

Group policies, including the anti-corruption policies, are of particular importance in the context of prevention. They contribute to ensuring employee compliance in key areas, such as the prevention and detection of corruption and bribery. These policies protect both employees and the company, thereby contributing to sustainable development. Therefore, the communication and implementation of group policies at the Nemetschek Group follow a standardized process to ensure that all relevant stakeholders across all local entities receive the policies and are adequately informed about their content.

The Corporate Legal & Compliance function ensures that each compliance policy is endorsed at the global executive board level ("Tone from the Top") and that a formally documented resolution by the board is obtained. Corporate Legal & Compliance then communicates policies, such as the Group-wide anti-corruption policy, via the intranet and email. To ensure that the policy is communicated and implemented across all relevant local entities, Corporate Legal & Compliance forwards the policies to all brand managing directors and utilizes the globally established compliance network, which consists of designated compliance coordinators responsible for each brand within the Nemetschek Group. The compliance coordinators are responsible for obtaining internal approvals at the brand level and securing the support of local management for the respective policies ("Tone from the Top"). They then communicate the policy content to all employees and provide necessary training sessions

One component of the Nemetschek Group's portfolio of preventive actions to prevent violations of anti-corruption and anti-bribery laws is the mandatory computer-based compliance training, which is offered in various formats. These training sessions aim to promote a corporate culture where all employees are aware of potential compliance risks. The Nemetschek Group utilizes a modern compliance training tool to efficiently and sustainably disseminate knowledge on anti-corruption and bribery prevention across the Group. The e-learning program has been rolled out across all Nemetschek Group subsidiaries and is mandatory for all employees, including management. The training must be completed at the beginning of employment and must be repeated regularly, in most cases at least every two years, depending on the subsidiary. The training includes both theoretical content and practical examples related to anti-corruption and bribery prevention. Additionally, Corporate Legal & Compliance regularly provides further training sessions for compliance coordinators, who act as local multipliers within their respective brands ("Train the Trainer principle").

Corruption and bribery represent a general risk to the Nemetschek Group. Therefore, the Nemetschek Group applies its established anti-corruption and anti-bribery actions equally to all employees to raise broad awareness of these risks. The Nemetschek Group recognizes that functions with direct interfaces to external business partners, such as procurement and sales departments as well as the Executive Board, are particularly exposed to corruption and bribery risk scenarios. The Executive Board maintains regular dialogue with Corporate Legal & Compliance to ensure that the Nemetschek Group's compliance management system continues to meet evolving internal and external regulatory requirements. To maintain this standard, the Executive Board supports the establishment, maintenance, and enhancement of new and existing compliance actions. This includes reinforcing a consistent "Tone from the Top" culture and leading by example in fulfilling compliance obligations and training requirements ("Walk the Talk"). Executive Board members therefore participate in the same anti-corruption training as regular employees. Considering their particularly high-risk exposure to corruption and bribery scenarios, Executive Board and Supervisory Board members have been provided with additional training materials by Corporate Legal & Compliance, outlining bribery and anti-corruption risks, solutions, and appropriate conduct in critical situations.

During the reporting period, no reports or grievances regarding violations of anti-corruption or anti-bribery laws were received through the Nemetschek Group's established reporting channels. Furthermore, the Nemetschek Group is not aware of any ongoing proceedings, resulting convictions, or fines related to violations of anti-corruption or anti-bribery laws in connection with its subsidiaries during the reporting period.

In the 2024 reporting year, a total of 3,846 employees across the Group were recorded as having completed compliance training, representing 86.2%. The metrics also include trained employees who have left the Nemetschek Group within the brand-specific training cycle.

Payment Practices

As a global software company, the Nemetschek Group is committed to ensuring fair payment terms for all suppliers. A 30-day payment term from the invoice date is granted to all suppliers. Longer payment terms, for instance, with larger companies, may be individually negotiated as long as they do not result in unfair disadvantage. During the reporting period, the Nemetschek Group was not aware of any outstanding legal proceedings related to unfulfilled payments by any of its subsidiaries.

Cyber and Information Security Actions

For the company-specific topic of Cyber and Information Security, the Nemetschek Group reports additional material information and relevant metrics in its sustainability statement to assess performance and effectiveness in relation to information security. Since the fiscal year 2024, the Risk Committee of the Nemetschek Group has been discussing not only risks and opportunities but also information security impacts on a quarterly basis with the executive board. These discussions are documented in a quarterly report for the supervisory board.

The Nemetschek Group's security strategy is based on a three-layer security model. This model consists of a "Brand Layer", which focuses on local implementation and security management at the brand level, a "Group Layer", which is mandatory for all brands and ensures fundamental security standards, and a "Flexible Layer" which includes optional services available to brands upon request. The "Group Layer", which is managed by the group-wide and centrally controlled Information Security function and includes shared services operated by the Security Operations Center (SOC), comprises several mandatory services. These cover the implementation of standard technology, asset management, vulnerability management, threat alerts, 24/7 security monitoring, and 24/7 incident response. Web application security is intended to be ensured through the use of web application scanners and other security auditing tools. Employee security awareness is reinforced through phishing campaigns and training sessions. Regular penetration tests are conducted to identify vulnerabilities. The "Group Layer" also includes standardized brand security reports and technical incident response services. The "Flexible Layer", primarily managed by Nemetschek SE, including the SOC, offers advanced services. These include an Managed Detection and Response (MDR) service, which enhances monitoring capabilities, asset-based and brand-specific solutions with result analysis, as well as administrative support services for the entire Group. The brands remain responsible for contract management and the implementation of Group-wide security actions at the local level. The strategy also includes the provision of hardening guidelines and comprehensive training sessions to support these efforts. This multi-layered approach aims to create an appropriate, scalable, and flexible security system that can be tailored to the specific needs of individual brands while ensuring a solid security foundation for the entire Group.

The Nemetschek Group acknowledges its responsibility to continuously improve information security, thereby creating added value for internal and external stakeholders, including customers, business partners, and employees. The company considers the needs of various interested parties, both internally and externally, and addresses relevant information security issues within the Group. The interests and perspectives of key stakeholders in the area of information security are as follows:

- Employees (internal): Implementation of ISMS controls to protect the company information, securing the work environment, and enhancing capabilities through training sessions
- Management (internal): Minimizing operational disruptions and security incidents to maintain brand value and reputation while ensuring cost-efficient information security
- Shareholders (external): Preventing loss events through cost-efficient information security and compliance with legal requirements
- Customers (external): Ensuring the protection of customer information and the availability of services while maintaining confidentiality, integrity, and availability
- Suppliers (external): Implementing controls to meet supplier security requirements and ensure secure operations
- Authorities/Auditors (external): Ensuring compliance with legal requirements and providing evidence of a functioning ISMS
- Cyberinsurance providers (external): Preventing damage through strong cyberdefense

For a globally operating company in the AEC/O and media and entertainment industry like the Nemetschek Group, a comprehensive and reliable information security management system is of central importance. To best protect the Group's software solutions, IT systems, and networks against cyberthreats, investments are made in the company's security infrastructure, and various actions are implemented to enhance security levels. As part of the Group-wide Business Enablement Initiative, operational excellence in information security is also to be increased through greater organizational efficiency and effectiveness, as well as harmonized processes. The centrally managed ISMS, which applies to all segments of the Group, its own operations, and the Nemetschek Group's value chain, is intended to strengthen confidence in the Nemetschek Group as a reliable market partner and contribute significantly to the implementation of the Group's growth strategy.

The process for identifying and assessing the material impacts, risks, and opportunities related to information security follows the process of double materiality assessment as well as the management of material impacts, risks, and opportunities within the Group. During the double materiality assessment, the Group Information Security function was closely involved in identifying and assessing sustainability-related impacts, risks, and opportunities

in the area of information security. The management of material impacts, as well as the actions taken and their effectiveness, is the responsibility of the Corporate Information Security Officer (CISO). As part of the double materiality assessment, actual or potential, positive or negative impacts, risks, and opportunities in the area of information security were identified that are directly linked to the Nemetschek Group's business model, strategy, and value chain. The assessment of impacts, risks, and opportunities in information security has determined that the actual positive impacts related to the Nemetschek Group's security infrastructure exceed the defined materiality threshold and are therefore relevant for this report.

The Nemetschek Group fulfills its social responsibility and is committed across the entire Group to the diligent handling of information from employees, customers, and business partners. The Information Security function oversees group-wide information security activities to always ensure appropriate organizational and technical actions – at the Group level, as well as at segment and brand levels. The function is led by the CISO, who reports directly to the CFO and thus to the Executive Board of Nemetschek SE. Information security is organized through a Group-wide ISMS implemented in the respective brands. At the end of the 2024 reporting year, the ISMS of all brands, except GoCanvas (and SiteDocs), was certified according to ISO/IEC 27001. The Nemetschek Group's corporate structure enables centralized control and monitoring at the Group level, while brands retain responsibility for information security.

The Nemetschek Group's approach to managing information security includes detailed regulations and procedures aligned with international standards and regulatory requirements. The Group-wide information security policies, including the "Group Information Security Guideline" and "Group Information Security Policies", aim to protect IT systems and data, as well as the security of products, employees, and office locations throughout the Group. The policies are based on the Group-wide ISMS, which complies with ISO/IEC 27001 standards, and focus on preventing security incidents, their early detection, and ensuring an appropriate response. The policies include technical and organizational actions for implementing and monitoring information security. The effectiveness of the actions is regularly reviewed by independent bodies and internal audits at least annually. The regulations apply to all entities within the Nemetschek Group and cover management processes, core processes, and support processes. The "Group Information Security Guideline" and "Group Information Security Policies" were adopted by the CISO of the Nemetschek Group and approved and released by the Executive Board of the Nemetschek Group. The regulations are updated as needed, generally at least once a year.

The implementation of information security policies includes several actions that are particularly relevant for the Nemetschek Group, including:

- ISO/IEC 27001 Certification: In fiscal year 2024, all brands, except GoCanvas (and SiteDocs), were successfully certified according to ISO/IEC 27001. The certification is valid until 2027. GoCanvas (and SiteDocs) will be integrated into the Nemetschek ISMS through a scope extension in 2025, as planned.
- SOC: In fiscal year 2023, a Group-wide standardized information security architecture was established and implemented across brands and their IT systems. Centralized monitoring, evaluation, and response to identified security incidents are managed through the newly established SOC. The SOC provides 24/7 threat detection to identify and mitigate security attacks targeting employees or IT systems. The SOC enables real-time detection and rapid response to threats. Relevant security incidents are escalated into a defined security incident process.
- Training and Awareness: Additional priorities in information security include regular training for all employees through web-based training, phishing email simulations, and targeted communication campaigns to enhance employee awareness of information security. The Group-wide mandatory e-learning program on information security is also updated annually. A well-trained workforce enables the Nemetschek Group to detect and mitigate security threats at an early stage. Regular training is a key component of the Group's commitment to information security.
- Cybersecurity Insurance: To further mitigate information security risks, the Nemetschek Group also maintains a Group-wide cybersecurity insurance policy with coverage appropriate to the size of the Group.

Further actions, such as an improved reporting structure, arise from potential new regulatory requirements, such as the Network and Information Security Directive (NIS2). At the same time, the Nemetschek Group is preparing for the European Cyber Resilience Act (CRA), which provides for an expanded vulnerability program for software products. With its actions in the area of information security, the Nemetschek Group aims to ensure the security and resilience of products with digital elements in order to be prepared for future legal obligations.

The Nemetschek Group's internal security control system monitors the effectiveness of concepts and actions with regard to material impacts, risks, and opportunities in the area of information security. The number of security incidents by severity level, Time to Detect (TTD: time required to identify an incident or security threat), and Time to Respond (TTR: time required to contain and resolve an incident or security threat) are subject-specific control variables, which provide insights into the effectiveness of existing policies and actions in information security. Internal and external security audits, as well as penetration tests, provide additional insights into the effectiveness of the ISMS.

Information security metrics are measured through regular data collection on performance, risk indicators, and governance practices. The Group Information Security function periodically evaluates performance against internal targets, analyzes trends, and compares them with data from the technology industry, which is generated by platform providers using anonymized customer data. Based on these assessments, initiatives for the continuous improvement of the ISMS are introduced to enhance Group-wide policies and processes in the short to medium term. The Nemetschek Group discloses its performance in information security through regular oral and written reports to the ELT and external stakeholders (e.g., customer questionnaires on information security or certification audits). The systematic information security approach of the Nemetschek Group supports efforts to protect IT systems, data, products, employees, and office locations in alignment with corporate goals and the expectations of internal and external stakeholders, enabling the effective management of impacts, risks, and opportunities.

To assess information security performance, the Nemetschek Group conducts regular internal and external audits, including supplier audits and penetration tests. Relevant findings are reported regularly to the management of Nemetschek SE or the respective brand. The information security strategy focuses on the continuous improvement of existing processes and includes regular regulation updates as well as internal corrective actions. The Group Information Security function is committed to transparent reporting on the effectiveness of policies and actions for internal and external stakeholders in compliance with ISO/IEC 27001.

The Nemetschek Group aims for zero security incidents. Security incidents are understood as individual or a series of unwanted or unexpected information security events that are highly likely to affect the Group's business operations and endanger information security. The time spans of TTD and TTR in security incidents should be kept as short as possible. In the event of security incidents, these are thoroughly investigated after resolution and appropriate actions are taken to prevent a recurrence of a security incident. The metrics in the area of Cyber and Information Security are reported for the first time in the current reporting year and serve as a base for future reporting periods.

The Nemetschek Group tracks security incidents and the corresponding TTD and TTR for all brands, except Maxon and GoCanvas, via a SaaS-based "Managed Security Service Provider" (MSSP) platform. Metrics for Maxon and GoCanvas are recorded separately. The Corporate Information Security function validates and consolidates security incidents, TTD, and TTR at the Group level. Security incidents at the Nemetschek Group are categorized into three levels ("medium", "high", or "critical"). The classification is based on an assessment of financial and reputational impacts. In the fiscal year 2024, a total of 9 incidents occurred in the "medium" category. There were no incidents in the "high" and "critical" categories. The average TTD is almost real-time, the average TTR is approximately 26 minutes.