

Einblicke in die Perspektiven von Kunden und Endnutzern werden über Umfragen, Kundenbeiträge oder auch den Kontakt über die Service-Hotlines der Marken gewonnen. Der Nemetschek Group sind derzeit keine Kunden und Endnutzer bekannt, die besonders anfällig für Auswirkungen und/oder durch die Geschäftstätigkeit des Konzerns direkt marginalisiert sein könnten. Alle Kunden und Endnutzer können ihre Sichtweisen gleichermaßen über die bestehenden Kommunikationskanäle an die Marken beziehungsweise den Konzern adressieren. Die Einbindung der Kunden und Endnutzer wird primär auf Markenebene gesteuert, sodass jede Marke ihren Ansatz auf ihren spezifischen Markt und ihre Zielgruppe abstimmen kann. Um den Austausch und die Zusammenarbeit mit größeren, multinationalen und multidisziplinären Kunden und Endnutzern zu intensivieren, wurde im vergangenen Geschäftsjahr ein globales KAM für die Nemetschek Group implementiert. Das globale KAM zielt drauf ab, die Kundengruppen, insbesondere die großen, international tätigen Kunden, der Nemetschek Group zukünftig noch stärker basierend auf individuellen Kundenbedürfnissen zu betreuen.

Durch den Kundenservice in jeder Marke bietet die Nemetschek Group ihren Kunden und Endnutzern die Möglichkeit, ihre Anliegen, Bedürfnisse oder Anforderungen direkt an die Marke zu richten. Der Kundendienst ist in jeder Marke intern organisiert und nicht auf externe Partner angewiesen. Die Kunden und Endnutzer können über individuelle Kanäle direkten Kontakt zu den Marken der Nemetschek Group aufnehmen, beispielsweise über die Website, Social-Media-Kanäle, E-Mail und Telefon-Hotline. Die Prozesse der Nemetschek Group, darunter auch der Kundenservice-/Supportprozess, sind seit Ende des Geschäftsjahres 2024 über den gesamten Konzern hinweg ISO-zertifiziert (ISO/IEC 27001), mit Ausnahme der Marke GoCanvas (und SiteDocs, Teil von GoCanvas), die im Juli des Berichtsjahres akquiriert wurde. Die Zertifizierung für GoCanvas ist für das Geschäftsjahr 2025 geplant. Für Beschwerden steht den Kunden und Endnutzern der Nemetschek Group auf Konzernebene zusätzlich das globale Hinweisgebersystem zur Verfügung. Dieses Hinweisgebersystem, über das Kunden und Endnutzer Beschwerden, auf Wunsch auch anonym, an die Nemetschek Group adressieren können, verfügt über Strukturen und Verfahren zum Schutz der Identität sowie vor Vergeltungsmaßnahmen an beteiligten Personen.

## 2.4 Governance-Informationen

### Unternehmenspolitik

Die Nemetschek Group berichtet in ihrer Nachhaltigkeitsklärung relevante Angaben für wesentliche Nachhaltigkeitsaspekte im Bereich Governance, darunter wesentliche Informationen zu Korruption und Bestechung sowie zu Zahlungspraktiken im Konzern. Für das unternehmensspezifische Thema Cyber- und Informationssicherheit werden zusätzliche wesentliche Informationen und relevante Kennzahlen berichtet, die der Bewertung der Leistung und Wirksamkeit in Bezug auf Informationssicherheit dienen.

### Management der Auswirkungen, Risiken und Chancen – Unternehmenspolitik

Eine gute Unternehmensführung und die Übernahme von Verantwortung für die eigenen Mitarbeiter, die Gesellschaft und die Umwelt sind für die Nemetschek Group von großer Bedeutung. Die Nemetschek Group zielt darauf ab, ein vertrauenswürdiger, zuverlässiger und ehrlicher Partner für ihre Kunden, Geschäftspartner, Mitarbeiter und die breite Öffentlichkeit zu sein. Jeder Mitarbeiter und jede Führungskraft ist mitverantwortlich dafür, dass die Nemetschek Group ihrer rechtlichen und gesellschaftlichen Verantwortung weltweit gerecht wird. Der Verhaltenskodex, der vom Vorstand der Nemetschek SE freigegeben und intern kommuniziert wurde, definiert konzernweite Verhaltensgrundsätze in einer für alle Mitarbeiter verständlichen Form und dient als Wertekompass innerhalb des Konzerns. Die Verantwortung, unethisches, unangemessenes oder illegales Verhalten aufzudecken, zu untersuchen und zu beenden, ist fest in der Unternehmenskultur der Nemetschek Group verankert.

Die drei wichtigsten Themen, die im Rahmen der Unternehmenskultur gefördert und kommuniziert werden, sind:

### Aufbau und Bewertung der Unternehmenskultur

- » Regelmäßige Feedback-Runden: Um die Zufriedenheit und das Engagement der Mitarbeiter zu messen, sollen regelmäßige Feedback-Runden zwischen Mitarbeiter und Manager stattfinden. Mitarbeiterbefragungen sind in einigen Marken bereits fester Bestandteil der Unternehmenskultur. Im ersten Quartal 2025 führt die Nemetschek Group eine weltweite Mitarbeiterbefragung durch.
- » Berufliche Weiterbildung: Angebote zur beruflichen Weiterbildung und beruflichen Entwicklung stärken die Bindung an die Nemetschek Group.
- » Anerkennung von Leistungen: Individualisierte Anerkennung von Erfolgen zielt darauf ab, die Mitarbeiter der Nemetschek Group zu motivieren.

### Entwicklung der Unternehmenskultur

- » Führungskultur: Führungskräfte agieren als positive Vorbilder für die Mitarbeiter.

» „Speak-up-Kultur“: Die Mitarbeiter haben die Möglichkeit, vertrauliche Meldungen über das Hinweisgebertool zu erstatten oder sich im Rahmen der hybriden Townhall-Sessions mit Fragen zu Wort zu melden.

Mit dem Board-Letter an alle Mitarbeiter der Nemetschek Group werden zentrale Verhaltensgrundsätze innerhalb des Konzerns kommuniziert. Die weitere Kommunikation erfolgt zwischen Führungskraft und Mitarbeiter in Zusammenarbeit mit HR.

Corporate Legal & Compliance sowie die Risikomanagementfunktion führen regelmäßig Risikoanalysen durch. Die Unternehmensrisikoanalyse, die von der Risikomanagementfunktion verantwortet wird, umfasst unter anderem Unternehmens- beziehungsweise Geschäftsrisiken. Die von Corporate Legal & Compliance durchgeführten Compliance- und Menschenrechts-Risikoanalysen sind auf die Erfassung und Bewertung von sowie den Umgang mit spezifischeren Risikofeldern ausgerichtet; innerhalb des Compliance-Bereichs sind das beispielsweise Geldwäsche- oder Kartellrisiken, innerhalb des Menschenrechtsbereichs beispielsweise Zwangs- oder Kinderarbeit, Korruptionsbekämpfung oder Menschenrechte. Diese Analysen dienen unter anderem dazu, Beschwerden und Mängel in den genannten Bereichen zu ermitteln, und werden zusätzlich durch Prüfungen der Konzernfunktion Internal Audit ergänzt.

Darüber hinaus fordert und fördert die Nemetschek Group eine offene „Speak-up-Kultur“ im gesamten Konzern. Mitarbeiter werden ermutigt, Verhaltensweisen zu melden, die gegen den Verhaltenskodex oder andere interne oder externe Vorschriften verstoßen könnten. Zu diesem Zweck setzt die Nemetschek Group proaktive Kommunikationsmaßnahmen wie regelmäßige E-Mails, Intranetveröffentlichungen und Vorstandspublikationen ein. Über ein modernes Hinweisgebersystem können Beschwerden nicht nur von Mitarbeitern, sondern auch von externen Dritten auf Wunsch auch anonym eingereicht werden. Dieses digitale System fungiert auch als Hinweisgebersystem für alle Marken der Nemetschek Group und legt besonderen Wert auf den Hinweisgeberschutz und damit auf den Schutz der Identität beteiligter Personen und Datensicherheit. Das Hinweisgebersystem ist derzeit in den Sprachen Deutsch, Englisch und Ungarisch verfügbar.

Neben dem digitalen Hinweisgebersystem können sich Mitarbeiter auch direkt an ihre Vorgesetzten, den zuständigen Personalleiter oder die (lokale oder unternehmensweite) Legal & Compliance Funktion wenden. Alle eingehenden Meldungen werden zunächst unter Wahrung höchster Vertraulichkeit auf Plausibilität geprüft. Gegebenenfalls werden weitere Untersuchungsmaßnahmen und Schritte eingeleitet. Falls im Einzelfall erforderlich, werden andere Niederlassungen/Funktionen des Unternehmens oder externe Berater hinzugezogen. Die Konzernfunktion Legal & Compliance fungiert als unabhängige, interne Meldestelle, überprüft regelmäßig die Wirksamkeit des Whistleblowing-Prozesses und passt diesen bei Bedarf an. Die Aufdeckung, Untersuchung und Beendigung von unethischem, unangemessenem und illegalem Ver-

halten ist einer der wichtigsten Leitsätze der Nemetschek Group und daher fest in der Unternehmenskultur verankert. Dieser findet sich sowohl in extern zugänglichen als auch in intern verfügbaren Dokumenten und Richtlinien und wird vom Unternehmen regelmäßig kommuniziert (zum Beispiel in E-Mails und Intranetpublikationen).

Alle Informationen, die über einen der vorab beschriebenen Whistleblowing-Kanäle der Nemetschek Group übermittelt werden (zum Beispiel Hinweise über mutmaßliche Korruptions- oder Bestechungssachverhalte), werden über einen standardisierten Prozess verarbeitet, der sich an den gesetzlichen Anforderungen gemäß der Richtlinie (EU) 2019/1937 und den national anwendbaren Gesetzen zur Umsetzung der Richtlinie orientiert und damit unter anderem die gesetzlichen Fristen einhält. Dieser standardisierte Prozess umfasst nicht nur das Hinweismanagement und die Kommunikation im Anschluss an Whistleblowing-Meldungen, sondern beschreibt auch die Untersuchungs- und Abhilfemaßnahmen, die nach Erhalt einer Whistleblowing-Meldung zu ergreifen sind. Die Konzernfunktion Legal & Compliance der Nemetschek Group bearbeitet und evaluiert Whistleblowing-Meldungen weisungsunabhängig und objektiv nach einem standardisierten Verfahren, um die Rechte aller Beteiligten zu schützen – insbesondere die der hinweisgebenden Person.

Die Nemetschek Group stellt die Einhaltung vorstehender Regelungen durch ein verpflichtendes gruppenweites Compliance-Training sicher, in dem Wissen zu den Themen Antikorruption und Bestechungsbekämpfung vermittelt wird. Das Training ist zu Beginn des Arbeitsverhältnisses abzuschließen und je nach Tochtergesellschaft regelmäßig, überwiegend mindestens zweijährlich zu wiederholen.

Korruption und Bestechung stellen nicht nur eine erhebliche Gefahr für das Vermögen und den wirtschaftlichen Erfolg der Nemetschek Group dar, sondern auch für ihre Existenz. Die Nemetschek Group verpflichtet sich daher, die eingeführten Maßnahmen gegen Korruption und Bestechung auf alle Mitarbeiter gleichermaßen verpflichtend anzuwenden, um ein möglichst umfassendes Bewusstsein für diese Risiken zu schaffen. Dabei ist sich die Nemetschek Group bewusst, dass insbesondere Funktionen mit Schnittstellen zu externen Geschäftspartnern, wie Einkaufs- und Vertriebsabteilungen sowie der Vorstand, vermehrt Risikoszenarien durch Korruption und Bestechung ausgesetzt sind.

Die Nemetschek SE und ihre in der EU ansässigen Tochtergesellschaften unterliegen der Richtlinie (EU) 2019/1937 und den nationalen Gesetzen zur Umsetzung der Richtlinie. Die Nemetschek Group fordert und fördert eine offene, gruppenweite „Speak-up-Kultur“. Um sicherzustellen, dass sich Whistleblower sicher fühlen, wenn sie Hinweise abgeben, hat die Nemetschek Group eine Reihe von Schutzmaßnahmen ergriffen. Dazu gehören Erklärungen, zum Beispiel im Verhaltenskodex, in denen es heißt, dass „kein Mitarbeiter aufgrund einer Meldung Nachteile erleiden wird“. Diese Botschaft wird auch durch weitere Kommunikations-

maßnahmen wie Flyer und Richtlinien verbreitet, die allen Mitarbeitern im Intranet zur Verfügung stehen. Hinweisgeber, die keine Mitarbeiter sind, finden die erforderlichen Informationen auf der Website der Nemetschek Group, einschließlich einer FAQ-Seite, auf der noch einmal betont wird, dass selbst sich als falsch erweisende Meldungen, sofern sie nicht vorsätzlich erfolgen, keine negativen Folgen für die meldende Person haben.

Neben den Kommunikationsmaßnahmen hat die Nemetschek Group (technische) Sicherheitsvorkehrungen innerhalb des Whistleblowing-Tools selbst implementiert. Hinweisgeber können Sachverhalte beispielsweise anonym melden. Die Offenlegung der eigenen Identität oder von Informationen, die zu einer Identifizierung des Hinweisgebers führen könnten, sind nicht zwingend erforderlich und weder für den Hinweis selbst noch für die anschließende Kommunikation während der Bearbeitung des Hinweises notwendig. Selbst wenn die Person, die den Hinweis abgibt, sich dafür entscheidet, ihre Identität freiwillig offenzulegen, wird diese Information nur dann preisgegeben, wenn dies tatsächlich notwendig ist (zum Beispiel bei behördlichen oder gerichtlichen Verfahren), oder mit Zustimmung des Hinweisgebers.

Die Konzernfunktion Legal & Compliance der Nemetschek Group bearbeitet und bewertet Whistleblowing-Meldungen unabhängig und objektiv nach einem standardisierten Verfahren, um die Rechte aller Beteiligten – insbesondere der meldenden Person – zu schützen. Dies spiegelt sich auch in einem internen Meldeverfahren an die Aufsichtsorgane wider, das einen ausreichenden Überblick über die Fakten ermöglicht, um als Grundlage für Entscheidungen der Organe herangezogen werden zu können, jedoch gleichzeitig die Persönlichkeits- und Datenschutzrechte der meldenden Person und weiterer Beteiligter bestmöglich wahrt. Die Nemetschek Group hat ein Konzept in Bezug auf die wesentliche positive Auswirkung zur Unternehmenspolitik und zur Förderung der Unternehmenskultur. Bestandteil dieses Konzepts ist der „People Letter of Commitment“, der im Kapitel [2.3 Sozialinformationen](#) beschrieben wird.

Als international tätiger Konzern hat die Nemetschek Group Beziehungen zu vielen Lieferanten und Geschäftspartnern aufgebaut, die den Konzern mit Waren und Dienstleistungen versorgen. Die sorgfältige Auswahl von Lieferanten und Geschäftspartnern ist ein wichtiges Element für das profitable Wachstum und das Ansehen der Nemetschek Group. Regeln und Grundsätze für die Auswahl von Lieferanten und Geschäftspartnern, die Geschäftsabwicklung, die erworbene Leistung und das Risikomanagement dienen dazu, die Verhandlungsposition der Nemetschek Group zu stärken und die finanziellen, ethischen und reputationsbezogenen Risiken zu reduzieren.

Die im Berichtsjahr 2024 eingeführte Konzernbeschaffungsrichtlinie der Nemetschek Group bietet einen Rahmen für die Durchführung von Beschaffungsmaßnahmen sowie zur Förderung bewährter, harmonisierter Praktiken im Beschaffungswesen, darunter Einkaufs- und Zahlungspraktiken. Die Konzernbeschaf-

fungsrichtlinie gilt für alle Mitarbeiter der Nemetschek Group weltweit, die für jegliche Art von Beschaffung verantwortlich sind oder in irgendeiner Weise in Beschaffungs- und Einkaufsprozesse involviert sind. Die Konzernbeschaffungsrichtlinie wurde vom Head of Global Procurement verabschiedet und vom Vorstand der Nemetschek SE geprüft und genehmigt. Die Konzernbeschaffungsrichtlinie erlaubt eine Zahlungsfrist von 30 Tagen und beugt damit verspäteten Zahlungen an Lieferanten und Geschäftspartnern vor.

Die Grundsätze der Zusammenarbeit mit Lieferanten und Geschäftspartnern sind zudem im Verhaltenskodex für Lieferanten der Nemetschek Group festgehalten. Die Nemetschek Group erwartet, dass ihre Lieferanten und Geschäftspartner sowie deren Mitarbeiter stets verantwortungsvoll handeln und bei all ihren Aktivitäten die Gesetze, Regeln und Vorschriften der Länder, in denen sie Geschäftstätigkeiten ausüben, in vollem Umfang einhalten. Darüber hinaus werden die Einhaltung der Grundprinzipien des Verhaltenskodex sowie die Einhaltung der Prinzipien des UN Global Compact (UNGC) und der Grundprinzipien der ILO erwartet. Im Verhaltenskodex für Lieferanten ist festgehalten, dass die Nemetschek Group ein fairer und verantwortungsvoller Marktteilnehmer ist, der sich an vertragliche Verpflichtungen gegenüber seinen Lieferanten und Geschäftspartnern hält.

Als internationales Softwareunternehmen legt die Nemetschek Group großen Wert auf nachhaltige und verantwortungsvolle Beziehungen zu ihren Lieferanten. Der Konzernansatz berücksichtigt sowohl die Risiken in der Lieferkette als auch die Auswirkungen auf Nachhaltigkeitsaspekte. Im Rahmen der Business-Partner-Due-Diligence achtet die Nemetschek Group unter korruptionsrechtlichen Aspekten auf eine sorgfältige Auswahl der Geschäftspartner. Im strategischen Beschaffungsprozess werden bei der Auswahl von Geschäftspartnern je nach Waren und Dienstleistungen ökologische Kriterien integriert, wie die Art der Verpackung, der Energieverbrauch sowie Recyclingmöglichkeiten. Diese tragen aktiv zur Reduzierung der indirekten Umweltauswirkungen bei.

Um die Transparenz und Effizienz in der Lieferkette zu erhöhen, plant die Nemetschek Group die Einführung einer cloudbasierten Einkaufsplattform. Diese innovative Lösung soll es ermöglichen, Risiken in der Lieferkette frühzeitig zu identifizieren und zu adressieren sowie die Zusammenarbeit mit strategisch wichtigen Lieferanten weiter zu intensivieren. Die damit verbundene erhöhte Datenverfügbarkeit und Datenqualität soll dazu beitragen, fundiertere Einkaufsentscheidungen zu treffen.

Die Integration ökologischer Kriterien spielt bei der Auswahl der Lieferanten und Vertragspartner eine zentrale Rolle. Der moderne Beschaffungsansatz berücksichtigt diese Aspekte systematisch und zielt darauf ab, eine nachhaltige und verantwortungsvolle Lieferkette zu gewährleisten. Die Nemetschek Group bewertet potenzielle Partner unter anderem anhand von Nachhaltigkeitsfaktoren wie beispielsweise Energieeffizienz und Nutzung erneuerbarer

Energien, Abfallmanagement und Kreislaufwirtschaftsansätze. Soziale Kriterien, die über die Einhaltung der Grundprinzipien des Verhaltenskodex für Lieferanten, die Prinzipien des UNGC beziehungsweise der ILO hinausgehen, werden bei der Auswahl der Lieferanten derzeit noch nicht berücksichtigt. Diese Kriterien, neben Faktoren wie Qualität, Innovationskraft und Preis, fließen unterschiedlich stark in die Lieferanten-Gesamtbewertung ein.

### **Vorfälle in Bezug auf Korruption oder Bestechung**

Die Nemetschek Group bekennt sich uneingeschränkt zum fairen Wettbewerb und lehnt insbesondere Korruption und Bestechung strikt ab. Dahinter steht die Überzeugung, dass nur durch gesetzeskonformes und verantwortungsbewusstes Handeln langfristiger Geschäftserfolg erzielt werden kann und sich diese Anstrengungen ebenso positiv auf die Zufriedenheit der Stakeholder auswirken. Eine offene Unternehmenskultur und ein etabliertes Compliance-Management-System (CMS) sind wichtige Maßnahmen im Kampf gegen Korruption und Bestechung. Diese Botschaft wird den Mitarbeitern der Nemetschek Group weltweit durch „Tone from the Top“-Maßnahmen wie den regelmäßigen Board-Letter vermittelt, der ebenso wie der konzernweite Verhaltenskodex in deutscher und englischer Sprache veröffentlicht wurde und im Intranet sowie auf der Website der Nemetschek Group zu finden ist. Der Verhaltenskodex wurde konzernweit bekannt gemacht und ist für alle Mitarbeiter – ungeachtet ihrer Position im Unternehmen – bindend.

Tatsächliche oder vermutete Verstöße gegen geltende Gesetze – einschließlich Antikorruptions- und Antibestechungsgesetze – interne Standards oder weitere Vorschriften werden regelmäßig durch verschiedene Risikoanalysen und Audits überprüft, aufgedeckt und bewertet, die von Corporate Legal & Compliance sowie der Risikomanagementfunktion und Internal Audit durchgeführt werden. Die Bewertung erfolgt dabei gemäß (branchen)üblicher Parameter, unter anderem Eintrittswahrscheinlichkeit und Schadenshöhe. Diese Audits und Analysen werden durch das konzernweite Whistleblowing-System als zusätzliches Verfahren zur Aufdeckung von Bestechungs- und Korruptionsrisiken ergänzt.

Um Bestechung und Korruption von vornherein zu verhindern, hat die Nemetschek Group eine Reihe von Verfahren eingeführt, um das konzernweite Bewusstsein für Bestechungs- und Korruptionsrisiken zu schärfen und zu stärken. Grundsätzlich erhalten die Mitarbeiter regelmäßig Handreichungen, Anleitungen und Hilfestellungen, die ihnen helfen, Korruptions- und Bestechungsrisiken in ihrer täglichen Arbeit zu bewältigen. Zu diesem Zweck nutzt Corporate Legal & Compliance eine Vielzahl von Kommunikationskanälen, wie Intranetpublikationen, E-Mails und ein obligatorisches E-Learning, das praktische Szenarien umfasst, in denen Mitarbeiter lernen, sich bei Korruptions- oder Bestechungsrisiken regelkonform zu verhalten. Des Weiteren können Mitarbeiter auf die konzernweite Antikorruptionsrichtlinie zugreifen, die detaillierte Vorschriften und Vorgaben enthält und damit den gruppenweiten Verhaltenskodex präzisiert. Die Richtlinie wird durch unter-

stützende Dokumente für spezifische Prozesse und Situationen wie Geschenke und Bewirtungsszenarien oder die Planung von Konzernveranstaltungen ergänzt. Die Richtlinie wurde global in alle Geschäftsbereiche der Nemetschek Group kommuniziert und ausgerollt.

Als globaler Softwareanbieter interagiert die Nemetschek Group naturgemäß mit einer Vielzahl von Geschäftspartnern in ihrer vor- und nachgelagerten Wertschöpfungskette. Um die daraus resultierenden rechtlichen, finanziellen und Reputationsrisiken zu minimieren, die beispielsweise aus Korruptions- oder Bestechungsvorfällen resultieren können, hat die Nemetschek Group einen risikobasierten Ansatz für den konformen und sorgfältigen Umgang mit Geschäftspartnern entwickelt, der eine Auswahl an Maßnahmen zur Risikominderung enthält, aus denen die Mitarbeiter je nach Risikoexposition wählen können. Dazu gehört der Verhaltenskodex für Lieferanten, der die Erwartungen der Nemetschek Group gegenüber Dritten definiert, sowie eine Anleitung für Mitarbeiter, wie risikobehaftete Geschäftspartner durch eine Due-Diligence-Prüfung geprüft und bewertet werden können. Die Due-Diligence-Prüfung kann – je nach Risikoexposition des Geschäftspartners – in unterschiedlicher Detailtiefe durchgeführt werden. Hierfür werden den Mitarbeitern in der Anleitung verschiedene Handlungsoptionen an die Hand gegeben.

Schließlich hat die Nemetschek Group einen standardisierten internen Investigationsprozess eingeführt, der alle Arten von Compliance-Verstößen abdeckt, einschließlich tatsächlicher oder mutmaßlicher Fälle von Korruption und Bestechung. Dieser Prozess umfasst die Untersuchung und das Management von Compliance-Verstößen sowie die Ableitung und Umsetzung von Abhilfemaßnahmen. Der Prozess folgt dabei stets den Grundprämissen des Vieraugenprinzips sowie der Vertraulichkeit.

Um der gesellschaftsrechtlichen Gesamtverantwortung gerecht zu werden, fungiert Corporate Legal & Compliance als unabhängige Meldestelle zur Bewertung und Untersuchung von Hinweisen. Es wurden spezielle Verfahrensweisen zur Vermeidung von Interessenkonflikten definiert, falls Vorstandsmitglieder oder Corporate Legal & Compliance selbst Gegenstand von Hinweisen sind. Sollte ein solches Szenario eintreten, wurden alternative Verantwortlichkeiten und Berichtswege für die Bearbeitung dieser Hinweise definiert und mittels Prozessbeschreibung kommuniziert. Die Ergebnisse interner Untersuchungen werden dem Vorstand und dem Aufsichtsrat im Rahmen der quartalsweisen Berichterstattung in verkürzter und abstrakter Form gemeldet. Dabei werden unter anderem gesetzliche Vorgaben zur Vertraulichkeit der Identität von Hinweisgebern und datenschutzrechtliche Bestimmungen in angemessener Weise berücksichtigt. Neben der turnusmäßigen Berichterstattung erfolgt nach Bedarf eine anlassbezogene Ad-hoc-Berichterstattung.

Konzernrichtlinien, darunter die Antikorruptionsrichtlinie, entfalten besondere Bedeutung im Rahmen der Prävention. Sie tragen dazu bei, die Mitarbeiter-Compliance in wichtigen Themenfeldern,



wie die Verhinderung und Aufdeckung von Korruption und Bestechung, sicherzustellen. Dabei schützen sie sowohl die Mitarbeiter als auch das Unternehmen und tragen so zu einer nachhaltigen Entwicklung bei. Daher folgt die Kommunikation und Umsetzung von Konzernrichtlinien bei der Nemetschek Group einem standardisierten Prozess, um sicherzustellen, dass alle relevanten Interessengruppen in allen lokalen Einheiten die Richtlinien erhalten und angemessen über deren Inhalt informiert werden.

Die Konzernfunktion Legal & Compliance stellt sicher, dass jede Compliance-Richtlinie auf globaler Vorstandsebene unterstützt („Tone from the Top“) und dazu ein formell dokumentierter Beschluss des Gremiums erwirkt wird. Anschließend kommuniziert Corporate Legal & Compliance Richtlinien wie die konzernweite Antikorruptionsrichtlinie über das Intranet und per E-Mail. Um sicherzustellen, dass die Richtlinie auch in allen relevanten lokalen Einheiten kommuniziert und umgesetzt wird, leitet Corporate Legal & Compliance die Richtlinien an alle Geschäftsführer der Marken weiter und nutzt das global bestehende Compliance-Netzwerk, das aus benannten Compliance-Koordinatoren besteht, die für jede Marke innerhalb der Nemetschek Group verantwortlich sind. Die Compliance-Koordinatoren sind dafür verantwortlich, interne Genehmigungen auf Markenebene einzuholen und die Unterstützung des lokalen Managements für die jeweiligen Richtlinien zu sichern („Tone from the Top“). Anschließend kommunizieren die Compliance-Koordinatoren die Richtlinieninhalte an alle Mitarbeiter und bieten entsprechende Schulungen an.

Ein Bestandteil des Präventionsmaßnahmenportfolios, das die Nemetschek Group zur Verhinderung von Verstößen gegen Antikorruptions- und Antibestechungsgesetze vorhält, ist das verpflichtende computerbasierte Compliance-Training, das in verschiedenen Formaten angeboten wird. Diese Schulungen zielen auf die Förderung einer Unternehmenskultur ab, in der alle Mitarbeiter für potenzielle Compliance-Probleme sensibilisiert werden. Die Nemetschek Group nutzt ein modernes Compliance-Schulungstool, um Wissen zu den Themen Antikorruption und Bestechungsbekämpfung effizient und nachhaltig im gesamten Konzern zu vermitteln. Das E-Learning ist flächendeckend in allen Tochtergesellschaften der Nemetschek Group ausgerollt und ist für die gesamte Belegschaft, inklusive der Führungskräfte, verpflichtend zu absolvieren. Das Training ist zu Beginn des Arbeitsverhältnisses abzuschließen und je nach Tochtergesellschaft regelmäßig, überwiegend mindestens zweijährlich, zu wiederholen. Es enthält sowohl theoretische Informationen als auch Praxisbeispiele im Bereich Antikorruption und Bestechungsbekämpfung. Weitere Schulungen werden regelmäßig von Corporate Legal & Compliance für die Compliance-Koordinatoren angeboten, die als lokale Multiplikatoren in ihren Marken fungieren („Train-the-Trainer-Prinzip“).

Korruption und Bestechung stellen ein grundsätzliches Risiko für die Nemetschek Group dar. Die Nemetschek Group wendet daher die eingeführten Maßnahmen gegen Korruption und Bestechung auf alle Mitarbeiter gleichermaßen an, um ein möglichst

umfassendes Bewusstsein für diese Risiken zu schaffen. Dabei ist sich die Nemetschek Group bewusst, dass vor allem Funktionen mit Schnittstellen zu externen Geschäftspartnern wie Einkaufs- und Vertriebsabteilungen sowie der Vorstand Risikoszenarien durch Korruption und Bestechung ausgesetzt sind. Der Vorstand steht in regelmäßigem Dialog mit der Konzernfunktion Legal & Compliance, um sicherzustellen, dass das Compliance-Managementsystem der Nemetschek Group stets den sich konstant weiterentwickelnden externen und internen regulatorischen Anforderungen entspricht. Um diesen Standard zu erreichen, unterstützt der Vorstand die Einrichtung, Aufrechterhaltung und Verbesserung neuer und bestehender Compliance-Maßnahmen. Dazu gehören unter anderem die Etablierung und Beibehaltung einer konsequenten „Tone from the Top“-Kultur und die gelebte Vorbildfunktion für die Mitarbeiter in Bezug auf Compliance-Verpflichtungen und -Schulungen („Walk the Talk“). Vorstandsmitglieder nehmen daher an den gleichen Antikorruptionsschulungen teil wie normale Mitarbeiter. Unter Berücksichtigung ihrer besonders risikoexponierten Position in Bezug auf Korruptions- und Bestechungsszenarien haben Vorstandsmitglieder sowie Mitglieder des Aufsichtsrats ergänzendes Schulungsmaterial von Corporate Legal & Compliance bereitgestellt bekommen, das Bestechungs- und Antikorruptionsrisiken aufzeigt und Lösungen sowie angemessenes Verhalten in kritischen Szenarien bietet.

Über die eingerichteten Meldekanäle der Nemetschek Group wurden innerhalb des Berichtszeitraums keine Hinweise oder Beschwerden über Verstöße gegen Antikorruptions- oder Antibestechungsgesetze gemeldet. Des Weiteren sind der Nemetschek Group für den Berichtszeitraum keine laufenden Verfahren, daraus resultierende Verurteilungen oder Bußgelder aufgrund von Verstößen gegen Antikorruptions- oder Antibestechungsgesetze, die in Verbindung mit den Tochtergesellschaften der Nemetschek Group stehen, bekannt.

Im Berichtsjahr 2024 wurden gruppenweit insgesamt 3.846 Mitarbeiter im Rahmen des Compliance-Trainings als geschult erfasst, was einem Prozentsatz von 86,2 % entspricht. Die Kennzahlen beinhalten auch geschulte Mitarbeiter, die die Nemetschek Group innerhalb des markenspezifischen Trainingsturnus verlassen haben.

### **Zahlungspraktiken**

Als globales Softwareunternehmen hat die Nemetschek Group sich verpflichtet, faire Zahlungsbedingungen für alle Lieferanten zu gewährleisten. Für alle Lieferanten wird ein Zahlungsziel von 30 Tagen ab Rechnungsdatum zugelassen. Längere Zahlungsziele, zum Beispiel mit größeren Unternehmen, werden individuell vereinbart, solange diese nicht grob benachteiligend sind. Innerhalb des Berichtszeitraums sind der Nemetschek Group keine ausstehenden Gerichtsverfahren aufgrund von Zahlungen, die durch eine Tochtergesellschaft der Nemetschek Group nicht geleistet wurden, bekannt geworden.

## Cyber- und Informationssicherheit

Für das unternehmensspezifische Thema Cyber- und Informationssicherheit berichtet die Nemetschek Group in ihrer Nachhaltigkeitserklärung zusätzliche wesentliche Informationen und relevante Kennzahlen, die der Bewertung der Leistung und Wirksamkeit in Bezug auf Informationssicherheit dienen. Im Risk Committee der Nemetschek Group werden neben Risiken und Chancen seit dem Geschäftsjahr 2024 auch Auswirkungen im Bereich Informationssicherheit quartalsweise mit dem Vorstand diskutiert und in einem Quartalsbericht für den Aufsichtsrat festgehalten.

Die Security-Strategie der Nemetschek Group ist auf einem dreischichtigen Sicherheitsmodell aufgebaut. Dieses Modell besteht aus einem „Brand Layer“, der sich auf die lokale Implementierung und das Sicherheitsmanagement in den Marken konzentriert, einem „Group Layer“, der für alle Marken verpflichtend ist und grundlegende Standards sicherstellen soll, sowie einem „Flexible Layer“, der optionale Services beinhaltet, die für die Marken auf Anfrage verfügbar sind. Der „Group Layer“, der von der gruppenweiten und zentral gesteuerten Information Security Funktion verwaltet wird und der durch das Security Operation Center (SOC) betriebene Shared Services beinhaltet, umfasst mehrere obligatorische Dienste. Diese umfassen die Implementierung der Standardtechnologie, Bestandsverwaltung, Schwachstellenmanagement, Bedrohungswarnung, 24/7-Sicherheits-Monitoring und 24/7-Reaktion auf Sicherheitsvorfälle. Die Sicherheit von Webanwendungen soll durch den Einsatz von Web-App-Scannern und anderen Sicherheits-Audit-Tools gewährleistet werden. Das Sicherheitsbewusstsein der Mitarbeiter wird durch Phishing-Kampagnen und Schulungsprogramme gestärkt. Regelmäßige Penetrationstests werden durchgeführt, um Schwachstellen zu identifizieren. Der „Group Layer“ umfasst auch standardisierte Marken-Sicherheitsberichte und technische Reaktionsdienste auf Sicherheitsvorfälle. Der „Flexible Layer“, der in erster Linie von der Nemetschek SE verwaltet wird, einschließlich des SOC, bietet erweiterte Dienste. Dazu gehören ein „Managed Detection and Response“ (MDR)-Service (Erkennung und Reaktion auf Sicherheitsbedrohungen und -angriffe) für ein verbessertes Monitoring, bestandsbasierte und markenindividuelle Lösungen mit Ergebnisanalyse sowie administrative Unterstützungsleistungen für den gesamten Konzern. Die Marken haben die Verantwortung für das Vertragsmanagement sowie die Implementierung der konzernweiten Sicherheitsmaßnahmen auf lokaler Ebene. Die Strategie beinhaltet die Bereitstellung von Härtingrichtlinien und umfassenden Schulungsprogrammen zur Unterstützung dieser Bemühungen. Dieser mehrschichtige Ansatz zielt darauf ab, ein angemessenes, skalierbares und flexibles Sicherheitssystem zu schaffen, das auf die spezifischen Bedürfnisse der einzelnen Marken zugeschnitten werden kann und gleichzeitig eine solide Basissicherheit für den gesamten Konzern gewährleistet.

Die Nemetschek Group sieht sich in der Verantwortung, Informationssicherheit kontinuierlich zu verbessern und damit einen

Mehrwert für interne und externe Stakeholder, darunter Kunden, Geschäftspartner und Mitarbeiter, zu schaffen. Das Unternehmen berücksichtigt die Bedürfnisse verschiedener interessierter Parteien, sowohl intern als auch extern, und behandelt relevante Themen in Bezug auf Informationssicherheit innerhalb des Konzerns. Die Interessen und Perspektiven der zentralen Stakeholder im Bereich Informationssicherheit stellen sich wie folgt dar:

- › Mitarbeiter (intern): Implementierung von ISMS-Kontrollen zum Schutz der Unternehmensinformationen, Sicherung der Arbeitsumgebung und Verbesserung der Fähigkeiten durch Schulungen
- › Management (intern): Minimierung von Betriebsunterbrechungen und Sicherheitsvorfällen, um den Markenwert und die Reputation zu erhalten und eine kosteneffiziente Informationssicherheit zu gewährleisten
- › Aktionäre (extern): Vermeidung von Schadensfällen durch kosteneffiziente Informationssicherheit und Einhaltung gesetzlicher Anforderungen
- › Kunden (extern): Sicherstellung des Schutzes von Kundeninformationen und der Verfügbarkeit von Dienstleistungen, wobei Vertraulichkeit, Integrität und Verfügbarkeit gewahrt bleiben
- › Lieferanten (extern): Implementierung von Kontrollen zur Erfüllung der Sicherheitsanforderungen der Lieferanten und Gewährleistung eines sicheren Betriebs
- › Behörden/Auditoren (extern): Sicherstellung der Einhaltung gesetzlicher Anforderungen und Bereitstellung von Nachweisen für ein funktionierendes ISMS
- › Cyber-Versicherung (extern): Vermeidung von Schadensfällen durch starke Cyber-Abwehr

Für einen global agierenden Konzern in der AEC/O- sowie der Medien- und Unterhaltungsindustrie wie die Nemetschek Group ist ein umfassendes und verlässliches Informationssicherheitsmanagement von zentraler Bedeutung. Um die Softwarelösungen des Konzerns sowie die eigenen IT-Systeme und Netzwerke bestmöglich vor Cyberangriffen zu schützen, werden Investitionen in die eigene Sicherheitsinfrastruktur getätigt sowie eine Vielzahl von Maßnahmen zur Verbesserung des Schutzniveaus umgesetzt. Im Rahmen der konzernweiten Business-Enablement-Initiative soll auch im Bereich Informationssicherheit die operative Exzellenz durch höhere organisatorische Effizienz und Effektivität sowie harmonisierte Prozesse gesteigert werden. Das zentral gesteuerte ISMS, das auf alle Segmente des Konzerns, den eigenen Betrieb sowie die Wertschöpfungskette der Nemetschek Group ausgerichtet ist, soll das Vertrauen in die Nemetschek Group als verlässlichen Partner am Markt stärken und einen zentralen Beitrag zur Umsetzung der Konzernwachstumsstrategie leisten.

Der Prozess zur Ermittlung und Bewertung der wesentlichen Auswirkungen, Risiken und Chancen im Bereich Informationssicherheit folgt dem Prozess der doppelten Wesentlichkeitsana-

lyse sowie der Steuerung wesentlicher Auswirkungen, Risiken und Chancen im Konzern. Bei der Durchführung der doppelten Wesentlichkeitsanalyse wurde die Konzernfunktion Information Security eng in die Ermittlung und Bewertung nachhaltigkeitsbezogener Auswirkungen, Risiken und Chancen im Bereich Informationssicherheit miteinbezogen. Das Management der wesentlichen Auswirkungen sowie damit verbundene getroffene Maßnahmen und deren Wirkung liegen in der Verantwortung des Corporate Information Security Officer (CISO). Im Rahmen der doppelten Wesentlichkeitsanalyse wurden tatsächliche oder potenzielle positive oder negative Auswirkungen, Risiken und Chancen im Bereich Informationssicherheit identifiziert, die unmittelbar mit dem Geschäftsmodell, der Strategie und der Wertschöpfungskette der Nemetschek Group in Verbindung stehen. Die Bewertung der Auswirkungen, Risiken und Chancen im Bereich Informationssicherheit hat ergeben, dass die tatsächlichen positiven Auswirkungen, die sich auf die Sicherheitsinfrastruktur der Nemetschek Group beziehen, über der definierten Wesentlichkeitsschwelle liegen und damit relevant für die vorliegende Berichterstattung der Nemetschek Group sind.

Die Nemetschek Group kommt ihrer gesellschaftlichen Verantwortung nach und verpflichtet sich konzernweit zum sorgfältigen Umgang mit den Informationen der Mitarbeiter, Kunden und Geschäftspartner. Die Konzernfunktion Information Security steuert gruppenweite Informationssicherheitsaktivitäten mit dem Ziel, jederzeit angemessene organisatorische und technische Maßnahmen auf Konzernebene sowie auf Segment- und Markenebene sicherzustellen. Die Funktion wird durch den CISO verantwortet, der eine direkte Berichtslinie zum CFO und somit dem Vorstand der Nemetschek SE hat. Organisiert wird die Informationssicherheit durch ein in den jeweiligen Marken eingesetztes gruppenweites ISMS. Zum Ende des Berichtsjahres 2024 wurde das ISMS aller Marken, bis auf GoCanvas (und SiteDocs), gemäß ISO/IEC 27001 zertifiziert. Die Unternehmensstruktur der Nemetschek Group ermöglicht eine zentrale Steuerung und das Monitoring auf Konzernebene, während die Marken die Verantwortung im Bereich Informationssicherheit behalten.

Der Ansatz der Nemetschek Group zur Steuerung von Informationssicherheit beinhaltet detaillierte Richtlinien und Verfahren, die mit internationalen Standards und regulatorischen Anforderungen im Einklang stehen. Die konzernweit geltenden Informationssicherheitsrichtlinien, darunter die „Group Information Security Guideline“ sowie die „Group Information Security Policies“, sind darauf ausgerichtet, IT-Systeme und Daten sowie die Sicherheit der Produkte, Mitarbeiter und Bürostandorte im gesamten Konzern zu schützen. Die Konzepte basieren auf dem konzernweiten ISMS, das den ISO/IEC-27001-Standards entspricht, und zielen auf die Verhinderung von Sicherheitsvorfällen, deren frühzeitige Erkennung und die Gewährleistung einer angemessenen Reaktion ab. Die Konzepte umfassen technische und organisatorische Maßnahmen, die der Umsetzung und dem Monitoring von Informationssicherheit dienen. Die Wirksamkeit der Maßnahmen wird

mindestens jährlich durch unabhängige Stellen und interne Audits überprüft. Die Richtlinien gelten für alle Einheiten innerhalb der Nemetschek Group und decken Aktivitäten der Managementprozesse, Kernprozesse sowie unterstützende Prozesse ab. Die „Group Information Security Guideline“ sowie die „Group Information Security Policies“ wurden vom CISO der Nemetschek Group verabschiedet und vom Vorstand der Nemetschek Group genehmigt und freigegeben. Die Richtlinien werden bei Bedarf, in der Regel mindestens einmal im Jahr, aktualisiert.

Die Umsetzung der Konzepte im Bereich Informationssicherheit umfasst eine Reihe von Maßnahmen, die für die Nemetschek Group besonders relevant sind, darunter:

- » ISO/IEC-27001-Zertifizierung: Im Geschäftsjahr 2024 wurde eine erfolgreiche Zertifizierung aller Marken, bis auf GoCanvas (und SiteDocs), nach ISO/IEC 27001 durchgeführt. Die Zertifizierung ist bis zum Jahr 2027 gültig. GoCanvas (und SiteDocs) sollen im Laufe des Jahres 2025 durch eine Scope-Erweiterung in das Nemetschek ISMS integriert werden.
- » SOC: Im Geschäftsjahr 2023 wurde eine gruppenweit standardisierte Informationssicherheitsarchitektur aufgebaut und in den Marken und deren IT-Systemen eingerichtet. Eine zentrale Überwachung, die Auswertung sowie die Reaktion auf identifizierte Sicherheitsvorfälle erfolgen in einem neu aufgebauten SOC. Das SOC verfügt über eine 24/7-Angriffserkennung, um Sicherheitsangriffe gegen Mitarbeiter oder IT-Systeme zu erkennen und abzuwehren. Das SOC ermöglicht eine Echtzeit-Erkennung und eine entsprechend schnelle Reaktionsfähigkeit auf Bedrohungen. Relevante Sicherheitsvorfälle werden in einen definierten Security-Incident-Prozess überführt.
- » Training und Sensibilisierung: Ein zusätzlicher Schwerpunkt im Bereich Informationssicherheit liegt in der regelmäßigen Schulung aller Mitarbeiter durch webbasierte Trainings, Phishing-Mail-Simulationen und anlassbezogene Kommunikation, um das Bewusstsein der Mitarbeiter für Informationssicherheit zu schärfen. Das konzernweit verbindliche E-Learning-Training zum Thema Informationssicherheit wird außerdem auf jährlicher Basis aktualisiert. Dank einer geschulten Belegschaft sieht sich die Nemetschek Group in der Lage, Sicherheitsbedrohungen frühzeitig zu erkennen und zu entschärfen. Regelmäßige Weiterbildung ist ein wesentlicher Bestandteil unserer Engagements für Informationssicherheit.
- » Cyber-Security-Versicherung: Zur weiteren Absicherung gegen Informationssicherheitsrisiken verfügt die Nemetschek Group zudem über eine konzernweite Cyber-Security-Versicherung, die über eine der Größe des Konzerns angemessene Deckung verfügt.

Weitere Maßnahmen, wie eine verbesserte Reporting-Struktur, ergeben sich aus potenziellen neuen regulatorischen Anforderungen, wie der Netzwerk- und Informationssicherheitsrichtlinie (NIS2). Gleichzeitig bereitet sich die Nemetschek Group auf den

europäischen Cyber Resilience Act (CRA) vor, der ein erweitertes Schwachstellen-Programm für Softwareprodukte vorsieht. Die Nemetschek Group zielt mit ihren Maßnahmen im Bereich Informationssicherheit darauf ab, die Sicherheit und Resilienz der Produkte mit digitalen Elementen zu gewährleisten, um auf zukünftige gesetzliche Verpflichtungen vorbereitet zu sein.

Das interne Security-Kontrollsystem der Nemetschek Group verfolgt die Wirksamkeit der Konzepte und Maßnahmen in Bezug auf wesentliche Auswirkungen, Risiken und Chancen im Bereich Informationssicherheit. Die Anzahl der Sicherheitsvorfälle nach Schweregrad, Time to Detect (TTD: Zeit, die benötigt wird, um einen Vorfall oder eine Sicherheitsbedrohung zu erkennen) und Time to Respond (TTR: Zeit, die benötigt wird, um einen Vorfall oder eine Sicherheitsbedrohung zu kontrollieren und zu beheben) sind fachspezifische Steuerungsgrößen, die Rückschlüsse auf die Wirksamkeit bestehender Konzepte und Maßnahmen im Bereich Informationssicherheit zulassen. Interne und externe Informationssicherheitsaudits sowie Penetrationstests liefern zusätzliche Erkenntnisse zur Effektivität des ISMS.

Kennzahlen im Bereich Informationssicherheit werden durch eine regelmäßige Datenerfassung zu Performance, Risikoindikatoren und Governance-Praktiken gemessen. In regelmäßigen Abständen bewertet die Konzernfunktion Information Security die Performance anhand von internen Zielvorgaben, analysiert Trends und vergleicht diese mit Daten der Technologiebranche, die über Plattformanbieter anhand anonymisierter Kundendaten generiert werden. Auf der Grundlage dieser Bewertungen werden Initiativen zur kontinuierlichen Verbesserung des ISMS eingeführt, um die konzernweiten Konzepte und Prozesse kurz- bis mittelfristig zu verbessern. Die Nemetschek Group legt ihre Leistung im Bereich Informationssicherheit durch regelmäßige mündliche und schriftliche Berichte an das ELT sowie externe Interessengruppen (zum Beispiel mittels Kundenfragebögen zu Informationssicherheit oder Zertifizierungsaudits) offen. Der systematische Informationssicherheitsansatz der Nemetschek Group trägt dazu bei, die Anstrengungen zum Schutz von IT-Systemen, Daten, Produkten, Mitarbeitern und Bürostandorten mit den Zielen des Konzerns und den Erwartungen der internen und externen Interessengruppen in Einklang zu bringen und somit eine wirkungsvolle Steuerung von Auswirkungen, Risiken und Chancen zu ermöglichen.

Um die Performance im Bereich Informationssicherheit zu beurteilen, führt die Nemetschek Group regelmäßige interne und externe Audits inklusive Lieferantenaudits sowie Penetrationstests durch. Relevante Erkenntnisse werden regelmäßig an das Management der Nemetschek SE oder das der jeweiligen Marke berichtet. Die Strategie im Bereich Informationssicherheit zielt auf eine kontinuierliche Verbesserung bestehender Prozesse ab und sieht sowohl eine regelmäßige Aktualisierung von Richtlinien als auch interne Korrekturmaßnahmen vor. Die Konzernfunktion Information Security ist bestrebt, eine transparente Berichterstattung zur Wirksamkeit der Konzepte und Maßnahmen für interne

und externe Stakeholdergruppen in Übereinstimmung mit ISO/IEC 27001 offenzulegen.

Die Nemetschek Group strebt eine Anzahl von null Sicherheitsvorfällen an. Sicherheitsvorfälle sind als einzelne oder eine Reihe unerwünschter beziehungsweise unerwarteter Informationssicherheitsereignisse zu verstehen, die den Geschäftsbetrieb des Konzerns mit hoher Wahrscheinlichkeit beeinträchtigen und die Informationssicherheit gefährden könnten. Die Zeitspannen der TTD und TTR bei Sicherheitsvorfällen sollen möglichst gering gehalten werden. Im Falle von Sicherheitsvorfällen werden diese nach Behebung eingehend untersucht und entsprechende Maßnahmen ergriffen, um einen erneuten Vorfall dieser Art zu verhindern. Die Kennzahlen im Bereich Cyber- und Informationssicherheit werden im vorliegenden Berichtsjahr erstmalig berichtet und dienen als Basis für zukünftige Berichtsperioden.

Die Nemetschek Group erfasst Sicherheitsvorfälle sowie die zugehörigen TTD und TTR für alle Marken bis auf Maxon und GoCanvas über eine SaaS-basierte „Managed-Security-Service-Provider“(MSSP)-Plattform. Die Kennzahlen für Maxon und GoCanvas werden separat erfasst. Die Konzernfunktion Information Security validiert und konsolidiert die Sicherheitsvorfälle, TTD und TTR auf Konzernebene.

Die Sicherheitsvorfälle der Nemetschek Group werden in drei Kategorien eingestuft („medium“, „high“ oder „critical“). Die Basis für die Kategorisierung ist eine Bewertung nach finanziellen sowie reputationsbezogenen Auswirkungen. Im Geschäftsjahr 2024 haben sich insgesamt 9 Vorfälle in der Kategorie „medium“ ereignet. Es gab keine Vorfälle in den Kategorien „high“ und „critical“. Die durchschnittliche TTD erfolgt nahezu in Echtzeit, die durchschnittliche TTR liegt bei etwa 26 Minuten.