Rotmonten Wirtschaftsprüfung AG

Aktuell

Oktober 2026 – Nr. 28

Stark in die Zukunft

Veränderungen gehören zum Leben – privat wie geschäftlich. Entscheidend ist, wie wir mit ihnen umgehen. Wir sind überzeugt: Wer frühzeitig plant, Bewährtes erhält und neue Möglichkeiten gemeinsam nutzt, schafft eine gute Grundlage für die Zukunft. Genau diesen Weg möchten wir in den kommenden Jahren gehen.

Die Anforderungen an Treuhand, Beratung und Wirtschaftsprüfung verändern sich laufend. Gleichzeitig bleibt etwas unverändert: Gute Beratung lebt von Menschen, von Vertrauen und von langjährigen persönlichen Beziehungen.

Gemeinsam stärker
Vor diesem Hintergrund wird Martin Juen seine Firmen (Juen Treuhand GmbH, Bleichenbacher + Steiger Treuhand AG, H. Keller Revision und Treuhand AG) und sein Team in den kommenden Jahren schrittweise in die Rotmonten Treuhand AG beziehungsweise die Rotmonten Wirtschaftsprüfung AG integrieren.

Bereits heute arbeiten unsere Unternehmen eng zusammen: Wir befinden uns auf demselben Stockwerk, teilen die Infrastruktur und pflegen einen unkomplizierten Austausch. Die geplante Zusammenführung ist deshalb der logische letzte Schritt einer Zusammenarbeit, die im Alltag bereits gelebt wird.

Bewährtes bleibt
Besonders wichtig ist uns die Kontinuität in der persönlichen Betreuung. Martin Juen und sein Team werden diesen Weg in den kommenden Jahren gemeinsam mit uns gehen und weiterhin aktiv mitwirken. Die langjährige Erfahrung, das grosse Know-how und die persönlichen Beziehungen zu den Kundinnen und Kunden bleiben bestehen und sind auch künftig ein wichtiger Teil unserer gemeinsamen Organisation.

Auch die vertrauten Ansprechpartner bleiben erhalten. Gleichzeitig rücken unsere Teams noch näher zusammen und können ihre Erfahrungen und ihr Wissen verstärkt miteinander teilen. So lassen sich Stellvertretungen langfristig gut organisieren und die Betreuung verlässlich sicherstellen. Wir verbinden Bewährtes mit neuen Möglichkeiten – ohne die persönliche Nähe zu verlieren.

Mit Weitsicht planen
Als Treuhänder und Wirtschaftsprüfer begleiten wir unsere Kundinnen und Kunden regelmässig bei Nachfolgeregelungen und langfristigen unternehmerischen Entscheiden. Dabei empfehlen wir, Veränderungen frühzeitig vorzubereiten. Diesen Anspruch stellen wir auch an uns selbst.

Der geplante Schritt eröffnet auch unseren Firmen Chancen. Unser Team wird mit zusätzlicher Fachkompetenz ergänzt und Synergien können genutzt werden. An unserer grundsätzlichen Organisation ändert sich aber nichts, Ihre Ansprechpartner bleiben unverändert.

Wir freuen uns darauf, Bewährtes weiterzuführen, Erfahrungen zusammenzubringen und gemeinsam stark in die Zukunft zu gehen.

Rotmonten Wirtschaftsprüfung AG

Rotmonten Wirtschaftsprüfung AG
Schuppisstrasse 8, 9016 St. Gallen, Tel. +41-71-243 00 18, www.rotmonten-wp.ch,

Business Continuity – wenn Schlüsselpersonen ausfallen

Ein Unternehmen kann technisch bestens aufgestellt sein – und trotzdem können Prozesse plötzlich ins Stocken geraten. Gerade bei kleineren und mittleren Unternehmen konzentrieren sich Wissen, Berechtigungen und Verantwortung oft auf wenige Personen oder gar nur eine Person. Fällt eine Schlüsselperson unerwartet aus, ist in den Ferien oder kurzfristig nicht erreichbar, zeigt sich rasch, wie gut die Organisation tatsächlich vorbereitet ist.

Business Continuity bedeutet deshalb nicht nur Datensicherung, IT-Systeme und Notfallpläne. Ebenso wichtig ist die menschliche und organisatorische Absicherung der zentralen Prozesse. Besonders im Finanz- und Rechnungswesen können fehlende Stellvertretungen schnell weitreichende Folgen haben: Zahlungen bleiben liegen, Löhne können nicht verarbeitet werden, wichtige Dokumente können wegen fehlender Unterschriftsregelung nicht unterzeichnet werden oder Fristen werden verpasst usw.

Abhängigkeiten bewusst reduzieren
Ein wirksames Vier-Augen-Prinzip gehört zu den einfachsten und wichtigsten Kontrollen und zu einem Wissenstransfer. Wesentliche Zahlungen, Änderungen von Bankverbindungen oder andere sensible Vorgänge sollten nicht vollständig durch eine einzelne Person abgewickelt werden können. Entscheidend ist, dass die zweite Person den Vorgang tatsächlich beurteilen kann und nicht nur formell freigibt.

Gerade deshalb ist eine funktionierende Stellvertretung wichtig. Es genügt nicht, auf einem Organigramm festzuhalten, wer wen vertritt. Die Stellvertretung muss die Abläufe kennen, über die notwendigen Kompetenzen verfügen und auf die relevanten Systeme zugreifen können. Eine gut durchdachte Passwortverwaltung ist hilfreich. Gerade bei kleineren Unternehmen sind aber die internen Möglichkeiten dafür manchmal begrenzt. In solchen Fällen kann es sinnvoll sein, einzelne Stellvertretungsfunktionen extern abzusichern - beispielsweise über den Treuhänder. Mit klar definierten Zuständigkeiten und angemessen begrenzten Berechtigungen kann so sichergestellt werden, dass wichtige Aufgaben auch bei einem personellen Ausfall weitergeführt werden können. Die Unterschriftshoheit soll aber jederzeit beim Kunden verbleiben.

Ferien als Praxistest
Geplante Ferien sind eine gute Gelegenheit, die eigene Organisation zu testen. Sind Pendenzen, Fristen und Zuständigkeiten sauber übergeben? Kann die Stellvertretung Zahlungen freigeben und auf die notwendigen Unterlagen zugreifen? Läuft der Betrieb normal weiter und notwendige Unterschriften können geleistet werden? Oder zeigt sich erst während der Abwesenheit, dass entscheidendes Wissen bei einer einzigen Person liegt? Wer Ferienübergaben bewusst nutzt, erkennt solche Abhängigkeiten frühzeitig.

Auch Passwörter und Zugriffsrechte gehören zu diesem Thema. Gemeinsam verwendete Passwörter oder Zugangsdaten, die nur eine Person kennt, schaffen gleichzeitig Sicherheitsrisiken und Abhängigkeiten. Sinnvoller sind persönliche Benutzerkonten, Mehrfaktor-Authentifizierung und geregelte Notfallzugriffe. Bei Funktionswechseln oder Austritten sollten Berechtigungen zudem konsequent überprüft und angepasst werden.

Ein einfacher Selbsttest
Stellen Sie sich für einen Moment vor, eine zentrale Person wäre ab morgen für zwei Wochen nicht verfügbar: Können Zahlungen und Löhne weiterhin korrekt verarbeitet werden? Sind Fristen, Pendenzen und wiederkehrende Aufgaben dokumentiert? Verfügt die Stellvertretung über die notwendigen Zugriffe? Und ist klar, wer im Ausnahmefall entscheiden darf?

Wenn einzelne dieser Fragen nicht eindeutig mit Ja beantwortet werden können, besteht Handlungsbedarf. Oft sind keine grossen Projekte nötig. Dokumentierte Abläufe, klare Stellvertretungen, konsequente Doppelkontrollen und ein geregeltes Berechtigungsmanagement erhöhen die Widerstandsfähigkeit der Unternehmung bereits deutlich.

Die Prüfung von personellen Abhängigkeiten und kritischen Abläufen soll ein wiederkehrender Prozess in jedem Unternehmen sein.

Cyberkriminalität: Warum gerade KMU im Finanz- und Rechnungswesen besonders wachsam sein müssen

Die Digitalisierung vereinfacht den Geschäftsalltag – gleichzeitig eröffnet sie Cyberkriminellen neue Möglichkeiten. Während spektakuläre Hackerangriffe auf internationale Konzerne die Schlagzeilen dominieren, sind es in der Praxis vor allem kleine und mittlere Unternehmen (KMU), die zunehmend Opfer von Cyberbetrug werden.

Als Geschäftspartner unserer Kunden erleben wir, dass insbesondere die Bereiche **Finanzen, Buchhaltung und Lohnwesen** im Fokus der Täter stehen. Denn dort befinden sich die Zahlungsströme und die sensiblen Unternehmensdaten.

Die Finanzabteilung ist für Cyberkriminelle besonders attraktiv, weil dort:
- Zahlungen ausgelöst werden,
- Lieferantenstammdaten gepflegt werden,
- Bankverbindungen hinterlegt sind,
- vertrauliche Unternehmensdaten gespeichert werden.

Die Täter müssen keine Computersysteme «hacken». Oft genügt es, das Vertrauen eines Mitarbeitenden zu gewinnen oder eine täuschend echte E-Mail zu versenden.

Cyberkriminalität ist längst kein Randthema der IT mehr. Sie gehört zu den zentralen Unternehmensrisiken jedes Schweizer KMU.

Ein **wirksames Schutzkonzept** basiert auf drei sich ergänzenden Säulen:

Vorsorgen durch ein modernes Internes Kontrollsystem, geschulte Mitarbeitende und klar definierte Prozesse.

Verhindern durch technische Sicherheitsmassnahmen, konsequente Kontrollen und eine gelebte Sicherheitskultur.

Versichern durch eine Cyberversicherung, welche die finanziellen Folgen eines erfolgreichen Angriffs abfedert. Viele Versicherer setzen heute voraus, dass grundlegende Sicherheitsmassnahmen bereits umgesetzt wurden. Gute Prävention verbessert deshalb nicht nur die Sicherheit, sondern oft auch die Versicherbarkeit und die Prämien.

Unternehmen, die diese drei Bereiche miteinander verbinden, stärken ihre Widerstandsfähigkeit nachhaltig und schaffen Vertrauen – bei Kunden, Mitarbeitenden und Geschäftspartnern. Cybersicherheit ist keine einmalige Investition, sondern ein fortlaufender Prozess – und ein wesentlicher Erfolgsfaktor für eine sichere und zukunftsfähige Unternehmensführung.

Unsere Empfehlung als Ihr Geschäftspartner
Wer **vorsorgt, klare Prozesse etabliert** und **das verbleibende Risiko sinnvoll versichert**, schützt nicht nur sein Unternehmen, sondern auch Mitarbeitende, Kunden und Geschäftspartner.

Wir empfehlen Ihnen, die internen Abläufe regelmässig zu überprüfen und insbesondere folgende Fragen zu beantworten:
- Sind unsere Zahlungsprozesse klar geregelt?
- Werden Änderungen von Bankverbindungen kontrolliert?
- Sind unsere Mitarbeitenden regelmässig geschult?
- Verfügen wir über funktionierende Datensicherungen?
- Besteht ein aktueller Notfallplan?
- Entspricht unsere Cyberversicherung den heutigen Risiken?

Praxis-Check: Wie sicher ist Ihr Unternehmen?
Beantworten Sie die folgenden Fragen mit **Ja** oder **Nein**:
- Gibt es für wesentliche Zahlungen ein verbindliches Vier-Augen-Prinzip?
- Werden Änderungen von Lieferanten-IBANs immer telefonisch verifiziert?
- Ist die Mehrfaktor-Authentifizierung für E-Banking und Microsoft 365 aktiviert?
- Werden Datensicherungen regelmässig getestet?
- Haben Ihre Mitarbeitenden in den letzten 12 Monaten eine Schulung zu Phishing und Cyberbetrug besucht?
- Besteht eine Cyberversicherung mit aktueller Deckung?
- Ist Cyberkriminalität Bestandteil Ihres Internen Kontrollsystems (IKS)?

Auswertung: Wenn Sie mehr als zwei Fragen mit «Nein» beantworten, lohnt sich eine Überprüfung Ihrer Prozesse. Bereits kleine organisatorische Anpassungen können das Risiko eines erfolgreichen Cyberangriffs erheblich reduzieren.

Haben Sie Fragen zu Ihren internen Kontrollprozessen oder möchten Sie Ihre Abläufe im Finanz- und Rechnungswesen überprüfen? Wir unterstützen Sie gerne mit einer praxisnahen Standortbestimmung und konkreten Handlungsempfehlungen.

Künstliche Intelligenz braucht menschliche Verantwortung

Künstliche Intelligenz ist Teil unseres Alltags. Sie formuliert Texte, wertet Daten aus, erstellt Bilder und unterstützt Entscheidungen. Richtig eingesetzt, spart sie Zeit und eröffnet Möglichkeiten. Doch KI ist weder neutral noch unfehlbar. Wer sie nutzt, überträgt ihr nicht die Verantwortung für das Ergebnis.

Eine der grössten Gefahren liegt in der scheinbaren Sicherheit ihrer Antworten. KI formuliert überzeugend, auch wenn Aussagen unvollständig, verzerrt oder falsch sind. Besonders bei rechtlichen, medizinischen, finanziellen oder personellen Fragen dürfen Informationen nie ungeprüft übernommen werden. KI kann Grundlagen aufbereiten, ersetzt aber weder Fachwissen noch das persönliche Urteil.

Auch rechtlich ist Vorsicht geboten. Sobald Personendaten verarbeitet werden, gilt in der Schweiz das Datenschutzgesetz – auch bei KI-Anwendungen. Zudem können Urheberrecht, Persönlichkeitsschutz, Geschäftsgeheimnisse und Haftungsfragen betroffen sein. International tätige Unternehmen müssen die Anwendbarkeit des EU AI Act prüfen. Vertrauliche Kundeninformationen, Mitarbeiterdaten, Verträge, Gesundheitsangaben oder interne Geschäftszahlen gehören nicht in frei zugängliche KI-Systeme. Oft bleibt unklar, wo Eingaben gespeichert und wie sie weiterverwendet werden.

Ebenso wichtig sind die emotionalen und menschlichen Risiken. KI kann Einfühlungsvermögen überzeugend nachahmen, empfindet jedoch weder Mitgefühl noch Verantwortung. Sie darf menschliche Beziehungen oder professionelle Hilfe nicht ersetzen. In Unternehmen dürfen Mitarbeitende nicht auf Datenprofile reduziert werden. Entscheide über Anstellung, Beförderung, Entlöhnung oder Kündigung müssen nachvollziehbar bleiben und von Menschen verantwortet werden.

Ethisch stellt sich nicht nur die Frage, was technisch möglich, sondern auch, was vertretbar ist. KI kann Vorurteile aus Trainingsdaten übernehmen und Personen oder Gruppen benachteiligen. Manipulierte Bilder, Stimmen und Videos verwischen die Grenze zwischen Wahrheit und Täuschung. Wer KI-Inhalte verbreitet, muss deren Richtigkeit prüfen, die Herkunft offenlegen und Irreführung vermeiden.

Gesellschaftlich droht ein Verlust an Vertrauen, wenn nicht mehr erkennbar ist, ob Inhalte echt sind. Der ungleiche Zugang zur Technologie kann zudem bestehende Unterschiede verstärken. Auch die Arbeitswelt verändert sich. Deshalb müssen Menschen rechtzeitig weitergebildet und einbezogen werden.

Unternehmen brauchen klare organisatorische Regeln: eine verbindliche KI-Richtlinie, freigegebene Anwendungen, geregelte Zuständigkeiten sowie Vorgaben zum Datenschutz und zur Kontrolle. Mitarbeitende müssen wissen, welche Informationen sie eingeben dürfen, wann eine fachliche Prüfung nötig ist und wer Entscheide freigibt. Sensible Anwendungen sollten vor der Einführung rechtlich, technisch und ethisch beurteilt und regelmässig überprüft werden.

Für Privatpersonen gilt im Kleinen dasselbe: keine sensiblen Daten preisgeben, Aussagen hinterfragen, Quellen prüfen und bei wichtigen Fragen Fach- oder Vertrauenspersonen beiziehen. KI ist ein Werkzeug – keine Autorität und kein Ersatz für das eigene Denken.

Die entscheidende Frage lautet nicht, ob wir KI einsetzen, sondern wie. Ein verantwortungsvoller Umgang verbindet ihre Möglichkeiten mit Datenschutz, Transparenz, Fairness und menschlicher Urteilskraft. KI kann vieles beschleunigen. Verantwortung, Empathie und Gewissen bleiben Aufgaben des Menschen.