



Managed-Services-Rahmenbedingungen

B2B-Standard · Kennung MS-RB - Version 1.2 - Stand 4. August 2026

B2B-Standard; für Verbraucher nur mit den ausdrücklichen B2C-Ausnahmen

1. Geltungsbereich

1.1 Diese Bedingungen gelten für alle als Managed Service, Managed Tarif, Betreuungspauschale, Hosting-, Cloud-, Lizenz-, Domain- oder laufende technische Betreuung bezeichneten Leistungen des Anbieters, insbesondere Managed WLAN, Firewall, Backup, Endpoint, Microsoft 365, Server, Monitoring, Telefonie, 3CX, Ansagenverwaltung, Domains und Webhosting.

1.2 Das Tarifblatt bestimmt nur Leistung, Menge, Preis, Hardware, gespeicherte Daten, Drittanbieter und gebuchte Optionen. Allgemeine Regeln werden nicht im Tarifblatt wiederholt.

1.3 Der Anbieter kann je nach Produkt und Kundenanforderung unterschiedliche Hersteller, Plattformen, Speicherorte und Hostinganbieter einsetzen. Die für den konkreten Dienst maßgeblichen Angaben werden im Angebot, Tarifblatt oder - bei Auftragsverarbeitung - in der AVV beziehungsweise der dazu bereitgestellten Unterauftragsverarbeiterliste bezeichnet.

2. Leistungsumfang und Grenzen

2.1 Nur im Tarifblatt bezeichnete Leistungen sind in der Pauschale enthalten. Mehrmengen, Projekte, Migrationen, Datenrettung, Neuaufbau nach Angriff, Umzug, Verkabelung, Fremdanbieterkoordination und Vor-Ort-Arbeit werden gesondert berechnet, soweit nicht eingeschlossen.

2.2 Die standardisierte Erstimplementierung vereinbarter Agenten und Managementkomponenten ist nur bei entsprechender Einführungsposition enthalten. Atypische, veraltete oder nicht dokumentierte Bestandskonfigurationen werden nach Hinweis nach Aufwand bearbeitet.

2.3 Hersteller-, Lizenz-, Cloud-, Domain-, Telekommunikations-, Hardware- und Ersatzteilkosten sind nur enthalten, wenn ausgewiesen.

2.4 Pauschalen gelten nur für die im Tarif vereinbarten Benutzer, Geräte, Datenmengen, Standorte und Systeme. Mehrmengen können ab Aktivierung oder dem folgenden Abrechnungszeitraum berechnet werden. Der Kunde meldet Änderungen unverzüglich.

2.5 Je Tarif auswählbar sind insbesondere Inventarisierung, Ereignismonitoring, Patchmanagement unterstützter Systeme und Drittsoftware, Verwaltung des Endpoint-Schutzes, Backup-Statusprüfung, Helpdesk-Inklusivzeit, Vor-Ort-Leistung, Dokumentation und Regelberichte. Nicht ausdrücklich bezeichnete Punkte sind nicht enthalten.

2.6 Patch- und Automationsmaßnahmen können Neustarts, Funktionsänderungen oder Inkompatibilitäten verursachen. Wartungsfenster und zulässige Automationen werden im Tarif festgelegt. Lehnt der Kunde eine empfohlene Sicherheitsmaßnahme ab, darf der Anbieter Entscheidung und Risiko dokumentieren.

2.7 Eine Prüfung, Zertifizierung oder Garantie von DSGVO-, NIS2-, DORA-, KRITIS- oder branchenspezifischer Compliance ist nur bei ausdrücklichem gesondertem Prüfauftrag geschuldet.

3. Service, Monitoring und SLA

3.1 Reguläre Servicezeiten sind Mo-Do 09:00-18:00 Uhr und Fr 09:00-12:00 Uhr, ausgenommen Feiertage in Bayern. Monitoring ist ohne gesonderte Bereitschaft keine 24/7-Sicherheitsleitstelle.

3.2 Ohne ausdrücklich gebuchtes SLA wird nach Best Effort priorisiert. Reaktionszeit ist qualifizierte Aufnahme und Bearbeitungsbeginn, nicht Behebung. Verbindliche Werte gelten nur nach SLA-Modul.

3.3 Wartungsfenster, Neustarts und zulässige Automationen stehen im Tarifblatt. Kritische Sicherheitsmaßnahmen dürfen nach dokumentierter Risikobewertung beschleunigt erfolgen.

4. Anbieterhardware

4.1 Als Anbieterhardware bezeichnete Geräte bleiben Eigentum des Anbieters. Der Kunde schützt sie vor Verlust, Beschädigung und unbefugtem Zugriff und meldet Standortänderungen.

4.2 Der Anbieter darf Hardware gegen technisch vergleichbare Geräte austauschen, wenn die vereinbarte Funktion nicht wesentlich verschlechtert wird.

4.3 Der Kunde ermöglicht nach Terminvereinbarung Zugang. Ein angebotener Termin darf grundsätzlich höchstens sieben Werktage in der Zukunft liegen, sofern kein sachlicher Grund entgegensteht. Wiederholt veränderter Zugang berechtigt nach zwei konkreten Terminen und Nachfrist zur Abrechnung tatsächlichen Mehraufwands und Aussetzung betroffener Leistungen.

4.4 Nach Vertragsende wird Anbieterhardware innerhalb 14 Kalendertagen zurückgegeben oder zur Abholung zugänglich gemacht. Nach erfolgloser Nachfrist wird tatsächlicher Geräte-, Beschaffungs- und Abwicklungswert ersetzt; eine Tarifpauschale gilt nur, wenn transparent vereinbart und der Nachweis fehlenden oder geringeren Schadens zugelassen ist.

5. Fernzugriff, Daten und Sicherheit

5.1 Dauerhafte Management-Agenten und unbeaufsichtigter Zugriff erfordern Freigabe. Rechte werden beschränkt, MFA und personengebundene Konten soweit möglich eingesetzt sowie administrative Zugriffe technisch protokolliert.

5.2 Kundeneigene Tenant-, Domain-, Zertifikats- und Adminzugänge bleiben dem Kunden zugeordnet. Interne Anbieterwerkzeuge und -lizenzen müssen nicht herausgegeben werden. Kundenänderungen beeinflussen Haftung nur bei Ursächlichkeit.

5.3 Bei unmittelbar drohender erheblicher Sicherheits- oder Datenverlustgefahr darf der Anbieter nach erteilter Freigabe angemessene Sofortmaßnahmen wie Isolation, Kontosperre oder Blockierung schädlicher Verbindung treffen und informiert unverzüglich.

5.4 Ohne beauftragtes Managed Backup bleibt der Kunde für getrennte, getestete Sicherungen verantwortlich. Speicherung ist keine gesetzliche/revisions sichere Archivierung, sofern nicht vereinbart.

6. Zahlungsrückstand - Stufe 1

6.1 Nach Fälligkeit darf der Anbieter mit der ersten Mahnung bei B2B sofort neue Bestellungen, Projekte, Erweiterungen, Vor-Ort-Termine, neue Lizenzen, Konfigurationsänderungen, kostenlosen Support und nicht sicherheitsnotwendige Verwaltungsfunktionen zurückhalten. Die Mahnung nennt Forderung, Verzugsfolgen, betroffene Dienste und eine Zahlungsfrist von fünf Kalendertagen.

6.2 Nach erfolglosem Ablauf darf eine im Tarifblatt definierte technische Teilsperre erfolgen. Sie wird auf betroffene Leistungen begrenzt und zuvor auf Sicherheits-, Datenverlust- und Verhältnismäßigkeitsrisiken geprüft. Berechtigt bestrittene Forderungen bleiben außer Betracht.

6.3 Sicherheitskritische Kernfunktionen wie Firewall-Basischutz, bestehende Backupdaten oder Endpoint-Schutz werden nicht unbemerkt automatisiert abgeschaltet. Zunächst werden Support, Änderungen, Verwaltung oder neue Sicherungspunkte nach besonderer Warnung beschränkt.

7. Zahlungsrückstand - Stufe 2 und Kündigung

7.1 Bleibt Zahlung aus, erhält der B2B-Kunde eine zweite und letzte Mahnung mit sieben Kalendertagen Nachfrist, Kündigungsandrohung, geplantem Beendigungsdatum, betroffenen Modulen, Herstellerrestkosten, Export-, Rückgabe- und Löschhinweisen.

7.2 Nach fruchtlosem Ablauf darf der Anbieter betroffene Dauerschuldverhältnisse außerordentlich kündigen, kontrolliert deaktivieren und die Forderung an Rechtsanwalt oder registrierten Inkassodienstleister übergeben. Vollständig bezahlte, trennbare Module werden nicht automatisch mitgekündigt.

7.3 Der Vergütungsanspruch bleibt während einer vom Kunden verursachten Sperre bestehen, soweit der Anbieter leistungsbereit war. Angemessene tatsächliche Wiederfreischaltungskosten dürfen nach Preisblatt berechnet werden.

7.4 Bei Verbrauchern und öffentlich zugänglichen Telekommunikationsdiensten gelten ausschließlich zwingende Sonderregeln. Insbesondere werden TKG-Schwellen, Androhungsfristen und Mindestversorgung nicht durch diesen B2B-Prozess verkürzt.

8. Drittanbieter, nicht stornierbare Kosten und Preisänderungen

8.1 Die Kündigung/Sperre des Managementdienstes beseitigt nicht die Zahlungspflicht für vor Bestellung offengelegte, verbindlich bestellte und beim Hersteller nicht stornierbare Lizenzen, Domains, Abos oder Mindestmengen bis zum nächstmöglichen Herstellerende.

8.2 Klar ausgewiesene Fremdkosten werden nach nachgewiesener Herstelleränderung im gleichen Umfang angepasst; Senkungen werden im gleichen Maßstab weitergegeben. Soweit vorher bekannt, erfolgt sechs Wochen Vorankündigung. Ein Sonderkündigungsrecht des betroffenen Bestandteils besteht, soweit keine offengelegte Herstellerbindung entgegensteht.

8.3 Drittanbieter bleiben für ihre Direktleistung verantwortlich; der Anbieter bleibt für eigene Beratung, Konfiguration, Integration und eingesetzte Erfüllungshelfen verantwortlich.

8.4 Soweit eine Auftragsverarbeitung vorliegt, werden die für den jeweiligen Dienst eingesetzten Unterauftragsverarbeiter dem Kunden im Rahmen der AVV oder auf einem vereinbarten elektronischen Weg zugänglich gemacht. Änderungen richten sich nach dem dort geregelten Informations- und Widerspruchsverfahren. Eine öffentliche Bekanntgabe interner Lieferanten- und Systemlisten ist nicht geschuldet.

9. Produktbezogene Sperrgrundsätze

Produktart	Erste Mahnung	Nach erster Frist	Nach zweiter Frist
WLAN/Firewall	Änderungen und Support stoppen	nicht sicherheitsnotwendige Cloudverwaltung beschränken; letzte sichere Konfiguration bleibt	kontrollierte Kündigung, Hardware zurück
Backup	Restore-/Änderungsaufträge stoppen	neue Sicherungspunkte nur nach spezieller Warnung aussetzen	Export-/Abruffrist, danach Löschung
Ansagen/Portale	Änderungen und Portal sperren	Aktivierung neuer Inhalte/Zeitpläne sperren	Export, Kündigung, spätere Löschung
Hosting/E-Mail	Änderungen, Support, Neuanlagen sperren	Website/Hosting/E-Mail nach ausdrücklicher Verlustwarnung teilweise oder vollständig sperren	Datenabruf, Kündigung, Löschung

Produktart	Erste Mahnung	Nach erster Frist	Nach zweiter Frist
Domains	Änderungen/Neuregistrierungen sperren	Domain bleibt registriert	Transferfrist; Registrarleistung zum angekündigten Termin beenden
M365/3CX/Lizenzen	Support, Änderungen, neue Seats stoppen	nur technisch/vertraglich zulässige Zugriffsbeschränkung	Managementvertrag beenden; Herstellerrestkosten bleiben
Endpoint/RMM	Änderungen und Standardsupport stoppen	nicht notwendige Verwaltung beschränken	kontrollierte Entfernung; Schutz nicht unbemerkt abschalten

10. Datenabruf, Löschung und Exit

10.1 Sperre ist keine Löschung. Nach Vertragsende bleiben exportierbare Kundendaten grundsätzlich mindestens 30 Kalendertage abrufbar, soweit Plattform, Vertrag und Recht dies ermöglichen. Eine zweite Löschankündigung erfolgt mindestens sieben Kalendertage vorher.

10.2 Export wird technisch möglich und gegen vereinbarte Vergütung bereitgestellt. Zwingende Data-Act-Rechte, insbesondere Wechsel-, Übergangs-, Abruf- und Entgeltregeln, bleiben unberührt.

10.3 Nach Abruffrist werden Daten und Backups datenschutzgerecht nach Löschzyklus gelöscht, sofern keine gesetzliche Aufbewahrung oder dokumentierte Weisung entgegensteht. Löschung wird dokumentiert.

10.4 Beim Offboarding werden kundeneigene Zugänge übergeben, delegierte Anbieterzugänge deaktiviert, Agenten kontrolliert entfernt, Anbieterhardware zurückgeführt und Herstellerlaufzeiten dokumentiert.

10.5 Gesetzliche Aufbewahrungspflichten für Vertrags-, Buchführungs-, Steuer- und Abrechnungsunterlagen bleiben unberührt. Sie rechtfertigen keine pauschale Aufbewahrung technischer Kundeninhalte, Postfächer oder Backups. Solche Daten werden nach Vertrags-, Abruf- und produktspezifischen Löschrufen sowie den technisch dokumentierten Löschzyklen behandelt.

11. Domains, Hosting und E-Mail

11.1 Domain und Hosting sind getrennte Leistungen. Die Sperre einer Website führt nicht automatisch zur Freigabe/Löschung der Domain.

11.2 Vor Beendigung der Domainverwaltung werden Ablauf-/Renewal-Datum und Transferfrist mitgeteilt. Der Kunde erhält nach Identitätsprüfung notwendige Transferinformationen. Erfolgt weder Zahlung noch Transfer, darf die Registrarleistung zum angekündigten Zeitpunkt enden; auf mögliches Freiwerden der Domain wird deutlich hingewiesen.

11.3 Vor E-Mail-Sperre wird ausdrücklich auf mögliche Abweisung oder Verlust eingehender Nachrichten hingewiesen. Web-, Datenbank-, Postfach- und Backupdaten werden erst nach Abruffrist gelöscht.

12. Vertragsänderungen

Neue Tarif- oder Modulversionen gelten nicht automatisch für Bestandsverträge. Wesentliche Leistungs-, Preis- oder Rechtsänderungen erfordern eine wirksame Vertragsgrundlage oder ausdrückliche Vereinbarung. Redaktionelle und zwingend rechtliche Änderungen ohne wirtschaftliche Verschlechterung können angekündigt werden.