Leistungsbeschreibung

mit den Angaben zu Anbieterwechsel, Datenexport und internationalem Zugriff (Art. 26 und 28 der Verordnung (EU) 2023/2854)

Bauer365 GmbH · Im Grund 4, 74199 Untergruppenbach · Amtsgericht Stuttgart, HRB 807588
Fassung 1.14 · Stand 18.11.2026

1. Gegenstand, Bezugsweg, Lizenzarten

1. Die Plattform ist eine über das Internet bereitgestellte Anwendung. Sie liest Bestands-, Lizenz-, Nutzungs-, Konfigurations- und Sicherheitsdaten eines Microsoft-365-Mandanten über die Schnittstellen von Microsoft und wertet sie zu Berichten, Kennzahlen, Empfehlungen und Dokumenten aus; auf Anforderung auch die Copilot-Lizenzen einer GitHub-Organisation. Sie ist ein Auswertungswerkzeug (Nutzungsbedingungen § 4 Abs. 1).
2. Bezogen wird die Plattform über einen Partner des Anbieters oder unmittelbar beim Anbieter (Direktbezug). Über einen Partner regelt der Vertrag mit ihm Preise und Bedingungen des Bezugs; im Direktbezug regeln sie die Nutzungsbedingungen (§ 6a) und die Auftragsbestätigung. Im Direktbezug ist der Anbieter zugleich der betreuende Partner des Endkunden: Angebot, Auftrag, Rechnung und Support kommen von ihm, und wo diese Beschreibung vom Partner spricht, ist er in dieser Rolle gemeint. Auftrag ist die vom Anbieter bestätigte Bestellung des Partners für den Endkunden oder, im Direktbezug, des Endkunden selbst.
3. Eine Lizenz gilt für einen Endkunden und einen Microsoft-365-Mandanten über einen Nutzungszeitraum von einem, zwei oder drei Vertragsjahren ab der Freischaltung, ohne automatische Verlängerung.
4. Der Leistungsumfang ergibt sich abschließend aus der Größenklasse (Abschnitt 2), der Grundleistung (Abschnitt 3) und den bestellten Zusatzmodulen (Abschnitt 4).

2. Größenklassen

Die Größenklasse richtet sich nach der Zahl der lizenzierten Benutzer im Mandanten des Endkunden: Benutzerkonten im Entra-Verzeichnis mit mindestens einer zugewiesenen Microsoft-365-Lizenz, wie die Plattform sie bei der Erhebung zählt. Gastkonten und Konten ohne zugewiesene Lizenz zählen nicht. Nennt der Auftrag nichts anderes, gelten diese Klassen:

Größenklasse	Lizenzierte Benutzer
XS	bis 79
S	80 bis 249
M	250 bis 2 499
L	2 500 bis 5 999
XL	6 000 bis 14 999
XXL	ab 15 000

Überschreitet die Zahl der lizenzierten Benutzer die gebuchte Klasse bei zwei aufeinanderfolgenden Erhebungen, teilt der Anbieter das mit; ist der Bestand 14 Tage danach nicht auf die gebuchte Klasse verringert, gilt für den Rest des Nutzungszeitraums die nächsthöhere Klasse zum zeitanteiligen Mehrpreis.

3. Grundleistung — die Bereiche

Die Grundleistung (Grundpaket) umfasst alle Auswertungen der Plattform außer den Zusatzmodulen nach Abschnitt 4 (Regelwerke und Copilot); die folgenden Themen beschreiben sie. Berechtigte Nutzer des Endkunden sehen sie nach Rolle und Freigabe. Vereinbart sind die Themen, nicht Aufbau, Darstellung und Bezeichnung der einzelnen Ansichten (Abschnitt 11 Nr. 2); jede Auswertung zeigt, was die Daten des Mandanten hergeben (Abschnitt 5 Nr. 4).

Bereich	Themen
Lizenzen und Kosten	Bestand, Zuweisung und Nutzung der Microsoft-Lizenzen je Konto und für die Organisation, Kosten und Kostenstellen, Hinweise auf ungenutzte oder mehrfach gehaltene Lizenzen, Empfehlungen zur Lizenzierung — auch für Telefonie und Power BI
Nutzung und Zusammenarbeit	Nutzung der Microsoft-365-Dienste je Konto und für die Organisation, Inaktivität, Speicherbelegung und Kandidaten zum Aufräumen, Gruppen und ihre Verwaltung
Sicherheit	Anmeldung und Zugriffsschutz, privilegierte Zugänge, Gäste und Freigaben nach außen, Anwendungen und ihre Zustimmungen, Konfiguration der Postfächer, Vorfälle, Warnungen und Bedrohungen aus Microsoft Defender
Geräte	Geräte mit Zuordnung, Betriebssystem, Konformität, Richtlinien und Schwachstellen
Compliance	Übersicht der Regelwerke und Speicherorte der Daten des Mandanten; die Abgleiche mit einzelnen Regelwerken sind Zusatzmodule (Abschnitt 4)
Verwaltung	Mandant anbinden und trennen, Erhebungen starten, planen und einsehen, Aufbewahrung, Pseudonymisierung personenbezogener Angaben, Nutzer, Rollen, Anmeldung und Freigaben, Beauftragung des Partners mit der Verwaltung (Abschnitt 10), Katalog der Module, Prüfprotokoll der Organisation

4. Zusatzmodule

Zusatzmodule werden je Endkunde zu einer Lizenz bestellt und enden mit ihr (Nutzungsbedingungen § 6 Abs. 1). Geschuldet ist ein Modul nur, wenn der Auftrag es nennt.

Gruppe	Inhalt
Regelwerke	Abgleich der im Mandanten messbaren technischen Anforderungen eines Regelwerks als Selbstauskunft (Abschnitt 14), mit Nachweisdokument; je Regelwerk ein Modul: NIS2 (BSIG), TISAX® (VDA ISA), ISO/IEC 27001, CIS Controls, DORA, SOC 2, BSI IT-Grundschutz, BSI C5:2026, DSGVO Art. 32
Copilot	Microsoft 365 Copilot und Agents: Voraussetzungen für die Einführung, Datenzugriffs-Risiken, vorhandene Agents und ihre Reichweite, Nutzung und Lizenz-Fit; dazu eine Übersicht zur KI-Verordnung (Verordnung (EU) 2024/1689) als Selbstauskunft (Abschnitt 14). Auf Anforderung (Abschnitt 6): Nutzung von KI-Diensten außerhalb von Copilot, Verbrauch der Copilot-Credits je Abteilung mit Notbremse (Abschnitt 6a) und die Copilot-Lizenzen einer GitHub-Organisation

Setzt eine Auswertung der Grundleistung oder ein Zusatzmodul im Mandanten eine Lizenz, einen Dienst oder eine Berechtigung voraus — etwa Microsoft Defender XDR, Teams Phone, Microsoft 365 Copilot, Global Secure Access oder eine Erweiterung nach Abschnitt 6 —, liefert sie ohne diese Voraussetzung keine Werte.

5. Erhebung

1. Ein Administrator des Endkunden bindet den Mandanten durch seine Zustimmung an. Danach greift die Plattform als Anwendung mit einem Zertifikat zu, ohne Nutzerkonto und Kennwort des Endkunden.
2. Eine Erhebung lösen berechtigte Nutzer des Endkunden oder ein in der Plattform eingestellter Zeitplan aus. Jede Erhebung ist eine Momentaufnahme des Mandanten zum Zeitpunkt ihres Laufs; ihre Dauer hängt von der Größe des Mandanten und von Microsoft ab und ist nicht zugesagt.

3. Gelesen wird, was die Berechtigungen nach Abschnitt 6 zulassen. Nicht gelesen werden Inhalte von E-Mails, Dateien, Chats, Kalendern und Besprechungen, Kennwörter sowie aus GitHub Code, Repositories, Prompts und Vorschläge.
4. Quelle aller Angaben sind die Schnittstellen von Microsoft, bei der GitHub-Anbindung die von GitHub. Fehlt im Mandanten eine Berechtigung, eine Lizenz oder ein Dienst, den ein Wert voraussetzt, oder liefert Microsoft ihn nicht, fehlt der Wert; die Plattform kennzeichnet ihn in der Regel als „nicht erhoben“.
5. Microsoft stellt Daten teils verzögert oder lückenhaft bereit, drosselt Abrufe und ändert Schnittstellen, Bezeichnungen und Preise. Ergebnisse können deshalb von den Verhältnissen im Mandanten abweichen; ihre Richtigkeit, Vollständigkeit und Aktualität im Einzelfall ist nicht zugesagt. Vor einer Entscheidung auf Grundlage eines Ergebnisses ist es mit dem Mandanten abzugleichen (Nutzungsbedingungen § 4 Abs. 4 bis 6).
6. Der Endkunde wirkt mit: Für die Anbindung braucht es einen Administrator mit dem Recht, Anwendungen und Rollen im Verzeichnis zuzustimmen. Fordert eine neue Fassung der Plattform eine weitere Berechtigung an, zeigt die Plattform das an; bis der Endkunde erneut zustimmt, fehlen die Werte, die sie voraussetzen.
7. Auf ausdrückliche Anforderung meldet sich ein Administrator des Endkunden zusätzlich für die Kostenverwaltung an (Abschnitt 6). Dann greift die Plattform für den Saldo der Copilot-Credits, den Verbrauch je Abteilung und die Notbremse im Namen dieses Administrators zu. Sie bewahrt dafür ein Aktualisierungs-Token verschlüsselt auf; Microsoft macht es nach 90 Tagen ohne Nutzung ungültig, die Plattform löscht es beim Trennen.

6. Berechtigungen im Mandanten des Endkunden

Die Plattform fordert Berechtigungen für die folgenden Schnittstellen an. Die vollständige Liste der einzelnen Berechtigungen mit ihrem Zweck erhält der Endkunde mit seinem Auftrag; sie ist Teil dieser Leistungsbeschreibung und wie die technischen und organisatorischen Maßnahmen vertraulich (Nutzungsbedingungen § 8). Die Plattform zeigt sie dem Administrator außerdem vor der Zustimmung an. Im Standard sind es Leserechte. Ein schreibendes Recht richtet die Plattform nur auf ausdrückliche Anforderung des Endkunden ein, nach einem Hinweis auf seine Wirkung, den der Endkunde annimmt, und mit einer Anleitung zum Rückbau. Welche Berechtigungen erteilt sind, kann der Endkunde jederzeit in seinem Mandanten nachprüfen: in Microsoft Entra ID bei den Unternehmensanwendungen des Anbieters, unter deren Berechtigungen.

Schnittstelle	Wofür
Microsoft Graph (Anwendungsrollen)	Verzeichnis-, Lizenz-, Nutzungs-, Konfigurations-, Geräte-, Sicherheits- und Compliance-Daten des Mandanten — lesend, ausser den Aufträgen nach Abschnitt 7 Nr. 2; Einstellungen ändert die Plattform darüber allein mit dem Schalter nach Abschnitt 6b Nr. 2 und nur mit dem Recht, das der Endkunde dafür eigens erteilt
Microsoft Defender for Endpoint (Anwendungsrollen)	Geräte- und Schwachstellendaten
Exchange Online und Security & Compliance (Exchange.ManageAsApp)	Konfiguration von Postfächern, Organisation und Compliance — mit lesenden Befehlen; geschrieben wird darüber allein für den Schalter nach Abschnitt 6b Nr. 1 und nur mit der Rolle, die der Endkunde dafür selbst einrichtet
Verzeichnisrollen Security Reader und Global Reader	Lesezugriff für die Abfragen von Exchange Online und Purview
Verzeichnisrolle Teams Reader für den Dienstprinzipal „Tenant Configuration Management“ von Microsoft	Lesen der Teams-Richtlinien

Zwei Klarstellungen:

- Für die Teams-Richtlinien bietet Microsoft keine Leserolle. Die Plattform fordert dafür die Rolle ConfigurationMonitoring.ReadWrite.All an, die nur für die Konfigurationsüberwachung von Microsoft gilt, und nutzt sie allein für die Momentaufnahme nach Abschnitt 7 Nr. 2.

- Einzelne Leserollen erlauben nach der Beschreibung von Microsoft mehr, als die Plattform liest — etwa die Rolle für SharePoint- und OneDrive-Websites auch das Lesen von Dateien. Die Plattform liest mit ihnen nur Angaben über Inhalte, etwa Namen, Struktur, Größe und Freigaben, nicht die Inhalte selbst (Abschnitt 5 Nr. 3). Ebenso erlaubt das Recht der Erweiterung „Besprechungs-Transkripte“ das Lesen des Textes; die Plattform ruft nur die Liste der Transkripte ab und speichert ihre Zahl.

Nur auf ausdrückliche Anforderung des Endkunden richtet die Plattform ein:

Erweiterung	Was sie ist
Schreibrolle „Compliance Administrator“	Verzeichnisrolle für den Dienstprinzipal, mit der Microsoft weitere Purview-Angaben herausgibt; die Plattform liest auch mit ihr nur
Power-BI-Zugang	Eigene App-Registrierung mit Zertifikat und Dienstprinzipal sowie die Sicherheitsgruppe „PureTenant Power BI Reader“; den Zugang gibt der Endkunde in seiner Power-BI-Verwaltung frei
Anmeldung über Microsoft (Single Sign-on)	Nutzer des Endkunden melden sich mit ihrem Microsoft-Konto an; die Plattform erhält Kennung, Name und E-Mail-Adresse, gleicht die so angemeldeten Konten regelmäßig mit dem Verzeichnis ab, und im Mandanten entsteht der Eintrag der Anmelde-Anwendung des Anbieters
Audit-Suche (AuditLogsQuery.Read.All)	Copilot- und Agent-Aktivität sowie der Start von Power-Apps-Anwendungen aus dem Prüfprotokoll von Microsoft 365; gespeichert werden nur Zählungen je Vorgang und Tag, ohne Konten, Adressen, Dateien und Pfade. Je Erhebungslauf entsteht dafür im Mandanten eine gespeicherte Suche (Abschnitt 7 Nr. 2)
Besprechungs-Transkripte (OnlineMeetingTranscript.Read.All)	Zahl der Teams-Besprechungen mit Transkript, je Organisator abgefragt und zusammengezählt gespeichert; der Text wird nicht abgerufen. Microsoft gibt Transkripte über die Schnittstelle erst frei, wenn der Endkunde dies im Teams Admin Center einschaltet; diese Einstellung gilt für alle Anwendungen seines Mandanten
KI-Verkehr über Global Secure Access (NetworkAccess-Reports.Read.All)	Aufrufe von KI-Diensten im Verkehrsprotokoll von Global Secure Access; gespeichert werden nur Zählungen je Dienst, ohne Konto, Gerät, Adresse oder Anmeldename
Schatten-KI aus Cloud Discovery (CloudApp-Discovery.Read.All)	Entdeckte Cloud-Anwendungen der Kategorie generative KI aus Defender for Cloud Apps mit Freigabestatus und Anzahlen; die Listen der Nutzer, Geräte und Adressen werden nicht abgerufen
Admin-Anmeldung Kostenverwaltung	Ein Administrator des Endkunden meldet sich bei der App-Registrierung „PureTenant Kostenverwaltung“ des Anbieters an. Die Plattform liest damit den Saldo der Copilot-Credits und den Verbrauch je Person, den sie sofort je Abteilung zusammenzählt — sobald dort mindestens fünf Konten Credits verbraucht haben; kleinere Abteilungen zusammengefasst und, bleibt auch die Sammlung darunter, ohne Zahl — und nicht je Person speichert, und schaltet auf Anforderung die Notbremse (Abschnitt 6a). Delegierte Berechtigungen: CopilotCostManagement.Read.All, CopilotCostManagementPolicy.ReadWrite.All, CopilotCostManagement-UserData.Read.All (Microsoft Graph); für Copilot Studio zusätzlich Licensing.BillingPolicies.ReadWrite und EnvironmentManagement.Environments.Read (Power Platform API)

Die Audit-Suche, die Besprechungs-Transkripte, der KI-Verkehr und die Schatten-KI legen je eine eigene App-Registrierung mit Zertifikat und Dienstprinzipal an, die genau das genannte Anwendungsrecht für Microsoft Graph trägt. Der Endkunde kann sie einzeln widerrufen; der Widerruf löscht das Schlüsselmaterial sofort und nach einer Anmeldung des Administrators die App samt Recht.

GitHub-Anbindung (auf Anforderung). Für Copilot › GitHub legt ein Inhaber der GitHub-Organisation des Endkunden dort eine eigene, private GitHub-App an und installiert sie. Sie trägt diese Rechte:

Recht in GitHub	Zweck
GitHub Copilot Business: Read-only	Copilot-Sitze mit Konto, letzter Aktivität, Editor und vorgemerkter Kündigung; Kopfzahlen der Abrechnung — keine Prompts, keine Vorschläge, kein Code

Recht in GitHub	Zweck
Administration: Read-only	AI-Credit-Verbrauch je Modell und die Budgets der Organisation. Das Recht öffnet weitere Einstellungen der Organisation lesend; die Plattform ruft nur die beiden Abrechnungswege ab — kein Code, keine Repositories
GitHub Copilot Business: Read and write (nur nach gesonderter Erteilung)	Notbremse: Sitze zum Ende des Abrechnungszyklus kündigen und die Kündigung zurücknehmen, jeweils nach ausdrücklicher Bestätigung; jede Aktion im Prüfprotokoll.

Das Schreibrecht erteilt der Endkunde in GitHub selbst; die Plattform nutzt es erst, nachdem sie es an der Installation gemessen hat, und nur für die Notbremse.

Zwei weitere Freigaben kann nur der Endkunde selbst setzen, per PowerShell in seinem Mandanten. Die Plattform zeigt ihm dafür die Befehle mit den Kennungen seiner Verbindung, auch die zum Rückgängigmachen:

Freigabe	Was sie ist
eDiscovery-Rollengruppen	Aufnahme des Dienstprinzipals in die Rollengruppe „eDiscovery-Manager“ über Security & Compliance PowerShell. Nach der Beschreibung von Microsoft erlaubt diese Rolle auch Durchsuchen, Vorschau und Export von Inhalten in den Fällen, in denen die Anwendung Mitglied ist; die Plattform liest damit nur die Liste dieser Fälle und ihre Datenverwalter
Webinare und Town Halls	Eine Teams-Anwendungszugriffsrichtlinie für die Anwendung, mandantenweit zugewiesen; die Plattform liest damit, wer im Mandanten Webinare und Town Halls veranstaltet

6a. Notbremse

Neben den Schaltern nach Abschnitt 6b ist die Notbremse die einzige Handlung der Plattform, die im Mandanten eine Einstellung ändert. Sie setzt (a) die Monatsgrenze einer Ausgabenrichtlinie für Copilot-Credits auf 0, (b) löst eine Umgebung der Power Platform von ihrer Abrechnungsrichtlinie (Pay-as-you-go über Azure) oder (c) kündigt mit der GitHub-Anbindung Copilot-Sitze zum Ende des Abrechnungszyklus. Auslösen kann sie ein Nutzer des Endkunden, der die Organisation verwaltet oder die Bereichsrolle „Kosten verantworten“ trägt, oder ein Partner mit Verwaltungsauftrag (Abschnitt 10 Nr. 3), jeweils nur nach ausdrücklicher Bestätigung. Die Plattform speichert die vorherige Einstellung, zeigt die gezogene Notbremse an und stellt die Einstellung auf Anforderung wieder her, sofern sie im Mandanten nicht inzwischen anders geändert wurde; dann ändert sie nichts. Jede Handlung steht im Prüfprotokoll. Die Wirkung bestimmt Microsoft beziehungsweise GitHub: Laufende Aufgaben können noch enden, die Sperre kann verzögert greifen, und eine gelöste Umgebung zieht nur noch aus gekaufter Kapazität, bei deren Überschreitung Microsoft ihre Agents abschaltet.

6b. Schalter für Einstellungen des Mandanten

Einzelne Einstellungen des Mandanten kann der Endkunde in der Plattform mit einem Schalter ein- und ausschalten. Derzeit sind das zwei Einstellungen:

1. die Einstellung von Exchange Online, mit der Postfächer von ihren Aliasadressen senden und antworten können (SendFromAliasEnabled). Eingeschaltet schreibt Exchange diese Adressen nicht mehr auf die primäre Adresse um; die Einstellung gilt für alle Postfächer des Mandanten;
2. die Einstellung der Microsoft-365-Nutzungsberichte, ob Benutzer-, Gruppen- und Websitenamen verborgen werden (displayConcealedNames). Ausgeschaltet zeigen alle Nutzungsberichte des Mandanten die Namen, auch im Microsoft 365 Admin Center und für jede Anwendung, die diese Berichte lesen darf; die Plattform ordnet die Nutzungsdaten dann den Konten zu. Ob der Endkunde die Namen zeigen darf, etwa nach einer Vereinbarung mit seiner Arbeitnehmervertretung, klärt er selbst.

Weitere Einstellungen nimmt der Anbieter nur mit einer neuen Fassung dieser Beschreibung auf.

Die Plattform liest den aktuellen Wert mit den Leserechten nach Abschnitt 6 und zeigt ihn neben dem Schalter an; kann sie ihn nicht lesen, zeigt sie das und nicht „aus“. Umschalten kann ein Nutzer des Endkunden, der die Organisation verwaltet, oder ein Partner mit Verwaltungsauftrag (Abschnitt 10 Nr. 3), jeweils nur nach ausdrücklicher Bestätigung. Geschrieben wird mit dem Zertifikat der Anwendung des Anbieters im Mandanten, ohne Anmeldung einer Person. Das Recht dazu gibt der Endkunde selbst, für jede Einstellung gesondert:

1. für die Einstellung von Exchange Online: Ein Exchange-Administrator des Endkunden legt mit Befehlen, die die Plattform anzeigt, in Exchange Online eine eigene Rolle „PureTenant Tenant-Schalter“ an, die allein die Änderung der Einstellungen von Exchange Online nach diesem Abschnitt erlaubt, und weist sie über eine gleichnamige Rollengruppe nur dieser Anwendung zu;
2. für die Einstellung der Nutzungsberichte: Ein Administrator für privilegierte Rollen oder ein Globaler Administrator des Endkunden erteilt dieser Anwendung mit Befehlen, die die Plattform anzeigt, das Recht ReportSettings.ReadWrite.All. Es erlaubt nach der Beschreibung von Microsoft allein das Lesen und Ändern der Einstellungen der Nutzungsberichte.

Ohne das jeweilige Recht weist Microsoft jede Änderung ab. Der Endkunde kann es jederzeit wieder entziehen — mit den ebenfalls angezeigten Befehlen, das Recht für die Nutzungsberichte auch in Microsoft Entra ID bei den Unternehmensanwendungen des Anbieters; das Lesen bleibt davon unberührt. Die Plattform ändert genau die gewählte Einstellung, liest sie danach zurück und zeigt das Ergebnis; lässt es sich nicht bestätigen, sagt sie das. Antrag und Ergebnis stehen im Prüfprotokoll. Zurückgestellt wird mit demselben Schalter. Die Wirkung bestimmt Microsoft; eine Änderung kann verzögert greifen.

7. Was im Mandanten entsteht

1. **Bei der Anbindung:** Mit der Zustimmung des Administrators legt die Einrichtungs-Anwendung des Anbieters einmalig die App-Registrierung „PureTenant M365 License Insights“ mit Zertifikat und Dienstprinzipal an, weist die Rollen nach Abschnitt 6 zu und richtet den Dienstprinzipal „Tenant Configuration Management“ von Microsoft mit der Rolle Teams Reader ein. Ihre Schreibrechte auf Anwendungen und Rollen des Verzeichnisses nutzt sie nur dafür; das Zugriffstoken des Administrators wird danach verworfen. Mit der Zustimmung entsteht auch der Eintrag der Einrichtungs-Anwendung unter den Unternehmensanwendungen. Eine Erweiterung nach Abschnitt 6 legt zusätzlich an, was dort genannt ist. Mit der Admin-Anmeldung Kostenverwaltung entsteht die Zustimmung zur Unternehmensanwendung „PureTenant Kostenverwaltung“, mit Copilot Studio zusätzlich die Zustimmung zur Power Platform API. Bei der GitHub-Anbindung entsteht in der GitHub-Organisation des Endkunden eine private GitHub-App mit den Rechten nach Abschnitt 6 und ihre Installation. Für die Schalter nach Abschnitt 6b richtet der Endkunde selbst ein, was der jeweilige Schalter braucht: für Exchange Online die Rolle und die Rollengruppe „PureTenant Tenant-Schalter“, in der er die Anwendung des Anbieters als Dienstprinzipal bekannt macht, und für die Nutzungsberichte die Zuweisung des Rechts ReportSettings.ReadWrite.All an diese Anwendung.
2. **Im Erhebungslauf:** Der Lauf ändert im Mandanten keine Einstellung. Für einzelne Abfragen — etwa die Teams-Richtlinien und Berichte aus Intune — legt er bei Microsoft Lese- oder Exportaufträge an, die er wieder löscht oder die Microsoft nach eigener Frist entfernt. Solche Aufträge können auf Kontingente zählen, die Microsoft je Mandant vorgibt. Mit der Erweiterung „Audit-Suche“ legt er je Lauf eine gespeicherte Suche im Prüfprotokoll mit dem Namen „PureTenant Erhebung *Zeitpunkt* UTC" an; Microsoft lässt sie über die Schnittstelle nicht löschen, und wie lange sie stehen bleibt, bestimmt Microsoft. Ein unterbrochener und fortgesetzter Lauf legt keine zweite an.
3. **Bei der Trennung:** Die Plattform löscht ihr Schlüsselmaterial und beendet die Erhebung. Was im Mandanten angelegt wurde, bleibt dort, bis der Endkunde es entfernt; beim vollständigen Rückbau werden auch die Apps der Erweiterungen gelöscht. Beim Trennen der Admin-Anmeldung löscht die Plattform das Aktualisierungs-Token; die Zustimmung bleibt, bis der Endkunde die Unternehmensanwendung entfernt. Eine gezogene Notbremse bleibt bestehen, bis sie freigegeben oder im Mandanten geändert wird — nach dem Trennen nur noch im Mandanten. Bei der Trennung der GitHub-Anbindung entfernt die Plattform die Installation und löscht den Schlüssel; die App selbst löscht der Endkunde in GitHub.

8. Ergebnisse, Dokumente, Export

Für Ergebnisse gelten die Nutzungsbedingungen (§ 2 Abs. 4); Daten, Formate und Wege des Exports nennt der Abschnitt „Anbieterwechsel, Datenexport und internationaler Zugriff“.

9. Aufbewahrung und Löschung

Wie viele Erhebungen aufbewahrt werden, stellt der Endkunde ein; die Fristen nennt der Vertrag zur Auftragsverarbeitung (Anlage 1 Abschnitt 6). Was ohne gültige Lizenz gilt, regeln die Nutzungsbedingungen (§ 6).

10. Nutzerkonten, Rollen, Sicherheit der Nutzung

1. Jeder Nutzer meldet sich mit eigenem Konto an: mit Kennwort und zweitem Faktor in der Plattform oder, wenn der Endkunde die Anmeldung über Microsoft eingerichtet hat, mit seinem Microsoft-Konto. Im zweiten Fall gelten für Anmeldung und zweiten Faktor die Richtlinien des Mandanten; sie festzulegen und durchzusetzen ist Sache des Endkunden. Die Plattform lässt dabei nur Anmeldungen zu, für die Microsoft einen zweiten Faktor bestätigt.
2. Rollen und Freigaben verwaltet der Endkunde in der Plattform: Verwalter der Organisation und Mitglieder mit Rechten je Bereich.
3. Der Endkunde kann seinen Partner in der Plattform mit der Verwaltung seiner Organisation beauftragen. Der Partner handelt dann in der Organisation im Umfang, den die Plattform für die Verwaltung vorsieht; Rechte, die nur eine Person des Endkunden ausüben kann — etwa Freigaben an den Partner oder die Löschung der Organisation, solange ihr Konten des Endkunden angehören —, gehören nicht dazu; die Notbremse (Abschnitt 6a) darf der Partner in der Verwaltung auslösen und die Schalter nach Abschnitt 6b bedienen. Legt der Partner den Endkunden mit dessen Vollmacht an, entsteht der Auftrag damit (Nutzungsbedingungen § 5 Abs. 4). Jede Handlung in der Verwaltung steht mit Person und Partner im Prüfprotokoll der Organisation. Der Endkunde kann den Auftrag jederzeit beenden.
4. Die Sicht des Partners regeln im Übrigen die Nutzungsbedingungen (§ 5), die Sicherheit der Verarbeitung der Vertrag zur Auftragsverarbeitung. Das gilt auch für den Anbieter in der Rolle des Partners: Auch er sieht Auswertungen nur mit Freigabe des Endkunden.

11. Verfügbarkeit, Wartung, Support

1. **Verfügbarkeit** am Übergabepunkt (Routerausgang des Rechenzentrums): 98,5 % im Mittel eines Kalendermonats. Nicht als Ausfall gelten angekündigte Wartungsfenster, Nichtverfügbarkeit, Drosselung oder Änderungen der Dienste und Schnittstellen von Microsoft, Störungen im Verantwortungsbereich des Partners oder des Endkunden, höhere Gewalt und Maßnahmen, die zur Abwehr eines Angriffs unverzüglich erforderlich sind.
2. **Wartungsfenster** kündigt der Anbieter mindestens 48 Stunden vorher an. Sie liegen in der Regel außerhalb von 08:00 bis 18:00 Uhr an Werktagen und dauern zusammen höchstens acht Stunden je Kalendermonat. Neue Fassungen der Plattform liefert der Anbieter ohne Ankündigung aus; Funktionen, Aufbau und Bezeichnungen der Bereiche können sich dabei ändern (Nutzungsbedingungen § 4 Abs. 6).
3. **Support:** Der Endkunde erhält Support von seinem Partner (erste Stufe). Der Anbieter unterstützt den Partner (zweite Stufe) per E-Mail an info@bauer365.de, an Werktagen (Montag bis Freitag, ausgenommen gesetzliche Feiertage in Baden-Württemberg) von 09:00 bis 17:00 Uhr, in deutscher und englischer Sprache. Im Direktbezug unterstützt der Anbieter den Endkunden auf demselben Weg und zu denselben Zeiten unmittelbar.
4. **Reaktionszeit:** Auf eine Meldung nach Nr. 3 antwortet der Anbieter innerhalb von vier Stunden innerhalb der Supportzeit mit einer ersten fachlichen Rückmeldung. Wiederherstellungszeiten gelten nur, wenn sie gesondert vereinbart sind.

12. Vorschau-Funktionen, unentgeltliche Leistungen

Vorschau-Funktionen und unentgeltliche Leistungen regeln die Nutzungsbedingungen (§ 4 Abs. 2). Bevor eine Erhebung vorliegt, kann die Plattform Beispieldaten zeigen; sie sind als solche gekennzeichnet und betreffen nicht den Mandanten des Endkunden. Auswertungen und Funktionen, die auf Schnittstellen beruhen, die Microsoft oder GitHub nur als Beta oder Vorschau anbieten, sind in der Plattform als Vorschau gekennzeichnet. Sie können jederzeit eingeschränkt sein oder keine Ergebnisse liefern, etwa weil der Anbieter der Schnittstelle sie ändert oder abschaltet.

13. Sprachen und Zugang

- Die Oberfläche lässt sich auf Deutsch, Englisch oder Französisch einstellen; einzelne Inhalte, Vertragstexte und erzeugte Dokumente sind deutsch.
- Der Zugang erfolgt über einen aktuellen Webbrowser unter puretenant.de; beim Endkunden wird nichts installiert.
- Die Oberfläche kann Logo und Farbe des betreuenden Partners tragen, sonst die Marke PureTenant. Anbieter der Plattform bleibt der Anbieter.

14. Nicht Gegenstand der Leistung

- Rechts-, Steuer- oder Lizenzberatung im Einzelfall; Sicherheitsüberwachung (Security Operations); Managed-Security- oder Managed-Service-Leistungen.
- Zertifizierung, Prüfung durch eine Prüfstelle oder Bestätigung der Rechtskonformität — ein Abgleich mit einem Regelwerk oder eine Übersicht zur KI-Verordnung ist eine Selbstauskunft auf gemessenen Werten und Angaben des Endkunden.
- Die Umsetzung von Empfehlungen im Mandanten des Endkunden (Lizenzen zuweisen oder entziehen, Richtlinien setzen, Konten ändern) — ausgenommen die Notbremse nach Abschnitt 6a und die Schalter nach Abschnitt 6b.
- Verfügbarkeit, Vollständigkeit und Richtigkeit der Daten, Dienste und Schnittstellen von Microsoft; Preise und Produktnamen Dritter; die Internet-Anbindung von Endkunde und Partner.
- Richtigkeit, Vollständigkeit und Aktualität der Ergebnisse im Einzelfall (Abschnitt 5 Nr. 5); ein wirtschaftlicher oder rechtlicher Erfolg, insbesondere eine bestimmte Einsparung.
- Archivierung oder Sicherung der Daten des Endkunden über die Aufbewahrung nach Abschnitt 9 hinaus.
- Einrichtung, Schulung, Beratung und Migration beim Endkunden; was der Partner im Rahmen einer Verwaltung nach Abschnitt 10 Nr. 3 tut.

15. Änderungen dieser Beschreibung

Welche Fassung dieser Beschreibung gilt, bestimmen der Auftrag und die Nutzungsbedingungen (§ 4 Abs. 1, § 9 Abs. 2). In einem laufenden Nutzungszeitraum ändert der Anbieter sie nur unter den Voraussetzungen, die die Nutzungsbedingungen für ihre eigene Änderung nennen (§ 9 Abs. 2); sein Recht, die Plattform weiterzuentwickeln (dort § 4 Abs. 6), bleibt unberührt.

Anbieterwechsel, Datenexport und internationaler Zugriff

Angaben nach Art. 26 und Art. 28 der Verordnung (EU) 2023/2854 zur Plattform „PureTenant – M365 License Insights“. Ihre aktuelle Fassung steht auf der Website des Anbieters, puretenant.de.

1. Verfahren. Der Endkunde — oder sein Partner mit Verwaltungsauftrag, wenn der Endkunde ihm dafür in Textform zugestimmt hat — erklärt in Textform an privacy@bauer365.de, ob der Endkunde zu einem anderen Anbieter wechseln, seine Daten in eine eigene IT-Umgebung übernehmen oder sie löschen lassen will. Fristen, Über-

gangszeitraum, Abruf und Löschung regeln die Nutzungsbedingungen (§ 6 Abs. 4 bis 8); Wechsel und Export sind unentgeltlich. Den Export erstellt die Verwaltung des Endkunden — oder sein Partner mit Verwaltungsauftrag — auch selbst in der Anwendung (Einstellungen › Datenexport) als ZIP-Archiv, bestätigt mit dem zweiten Faktor; jeder Export steht im Prüfprotokoll der Organisation.

2. Daten und Formate.

Daten	Format	Weg
Erhebungsberichte (Momentaufnahmen des Mandanten)	JSON (RFC 8259)	Datenexport in der Anwendung, auch nach dem Ende des Nutzungszeitraums; sonst auf Anforderung in Textform
Tabellen der Auswertungen	CSV (RFC 4180), XLSX (ISO/IEC 29500)	Export in der Anwendung
Erzeugte Dokumente	PDF (ISO 32000)	Download in der Anwendung
Einstellungen und Entscheidungen des Endkunden	JSON (RFC 8259), XLSX (ISO/IEC 29500)	Datenexport in der Anwendung
Prüfprotokoll der Organisation	JSON (RFC 8259), XLSX (ISO/IEC 29500)	Datenexport in der Anwendung

Das Archiv des Datenexports beschreibt sich selbst: Ein Verzeichnis nennt jede Datei mit Prüfsumme und was fehlt, ein JSON Schema die Struktur der Einstellungen und Entscheidungen.

Was auf Anforderung bereitgestellt wird, erhält der Endkunde als Datei innerhalb des Übergangszeitraums, zusammen mit einer Beschreibung der Datenstruktur. Was nicht exportierbar ist, nennen die Nutzungsbedingungen (§ 6 Abs. 6).

3. Einschränkungen. Der Export erfolgt als Datei an eine berechtigte Person des Endkunden. Eine Programmierschnittstelle für den Export oder für die Übertragung an einen anderen Anbieter besteht nicht. Daten aus einem anderen Dienst übernimmt die Plattform nicht; sie erhebt ihre Daten aus dem Mandanten des Endkunden.

4. Ort der Infrastruktur (Art. 28 Abs. 1 lit. a). Die Plattform speichert und verarbeitet die Daten aus den Mandanten der Kunden auf Servern in Deutschland; diese unterliegen deutschem Recht. Der Abruf durch die Nutzer läuft über ein vorgeschaltetes Auslieferungs- und Schutznetz, dessen Betreiber seinen Sitz in Slowenien hat und dem Recht der Europäischen Union unterliegt. E-Mails der Plattform versendet Microsoft Ireland Operations Limited über Exchange Online; die Postfächer liegen in Deutschland, verarbeitet wird innerhalb der EU-Datengrenze von Microsoft. Die eingesetzten Dienstleister nennt der Vertrag zur Auftragsverarbeitung (Anlage 3).

5. Schutz vor Zugriff von Behörden aus Drittländern (Art. 28 Abs. 1 lit. b). Vertraglich: Der Anbieter setzt Dienstleister nur nach dem Vertrag zur Auftragsverarbeitung ein und übermittelt Daten nicht ohne Weisung des Endkunden in ein Drittland (dort § 7 und § 8). Technisch: Übertragung und Speicherung sind in dem Umfang verschlüsselt, den der Vertrag zur Auftragsverarbeitung nennt (dort § 5 und Anlage 2); die Schlüssel der gespeicherten Daten verwaltet der Anbieter selbst. Organisatorisch: Ersuchen von Behörden eines Drittlands prüft der Anbieter nach Art. 32 der Verordnung; er gibt Daten nur in dem danach zulässigen Umfang heraus und unterrichtet den Endkunden, soweit das zulässig ist.

6. Kontakt. Bauer365 GmbH, Im Grund 4, 74199 Untergruppenbach, privacy@bauer365.de.