

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 1.1 · Stand 14.10.2026

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. Sie ist ein Auswertungswerkzeug (Nutzungsbedingungen § 4 Abs. 1).
2. Bezogen wird die Plattform ausschließlich über Partner des Anbieters; Preise und Bedingungen des Bezugs regelt der Vertrag mit dem Partner. Auftrag ist die vom Anbieter bestätigte Bestellung des Partners für den Endkunden.
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 und wird der Bestand nicht verringert, gilt für den Rest des Nutzungszeitraums die nächsthöhere Klasse.

3. Grundleistung – die Bereiche

Die Grundleistung umfasst die folgenden Bereiche. Berechtigte Nutzer des Endkunden sehen sie nach Rolle und Freigabe.

Bereich	Inhalt
Lizenzen und Kosten	Lizenzen und Dienstpläne je Identität, Bestand und Zuweisung je Lizenz, doppelt gehaltene Ansprüche, Konten ohne Nutzung, Empfehlungen zur Lizenzierung, Kosten und Kostenstellen

Bereich	Inhalt
Nutzung	Nutzung von Exchange, OneDrive, SharePoint, Teams, Office-Anwendungen und Copilot je Identität und Organisation, Inaktivität, Speicherbelegung
Sicherheit	Anmeldeverfahren und zweiter Faktor je Konto, riskante Benutzer, Vorfälle und Warnungen aus Defender, Richtlinien für den bedingten Zugriff, Administratorrollen, Postfach-Konfiguration
Geräte	Geräte des Verzeichnisses mit Zuordnung, Betriebssystem, Konformität, Richtlinien und Schwachstellen
Compliance	Übersicht der Regelwerke; die Abgleiche selbst sind Zusatzmodule (Abschnitt 4)
Verwaltung	Mandant anbinden und trennen, Erhebungen starten und einsehen, Aufbewahrung, Nutzer, Rollen und Freigaben, Prüfprotokoll der Organisation, Katalog der Zusatzmodule

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, DSGVO Art. 32
Sicherheit	Sicherheitslage im Vergleich: Auswertung von Bedrohungen (Threat Hunting), kein Vergleich mit anderen Organisationen · Postfach-Abfluss & Altprotokolle · App- & Consent-Governance: Anwendungen und Zustimmungen · Anmelde-Hygiene: Anmeldungen ohne zweiten Faktor
Speicher und Zusammenarbeit	Speicher & Kollaboration: Speicherbelegung und Aufräum-Kandidaten in SharePoint, OneDrive und Postfächern · Gruppen-Governance: Gruppen ohne Eigentümer und öffentliche Gruppen
Lizenzen und Planung	Lizenz-Planung mit Beschlussvorlage · Copilot: Voraussetzungen, Datenzugriffs-Risiken und Lizenz-Fit für Microsoft 365 Copilot · Telefonie & Audiokonferenz · Power-BI-Lizenz-Fit

Setzt ein Modul im Mandanten eine Lizenz, einen Dienst oder eine Berechtigung voraus — etwa Microsoft Defender XDR, Teams Phone oder den Power-BI-Zugang nach Abschnitt 6 —, liefert es ohne sie keine Werte.

5. Erhebung

- 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.
- 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.
- Gelesen wird, was die Berechtigungen nach Abschnitt 6 zulassen. Nicht gelesen werden Inhalte von E-Mails, Dateien, Chats und Kalendern sowie Kennwörter.
- Quelle aller Angaben sind die Schnittstellen von Microsoft. 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. Berechtigungen im Mandanten des Endkunden

Die Plattform fordert Berechtigungen für die folgenden Schnittstellen an. Jede einzelne Berechtigung zeigt sie dem Administrator vor der Zustimmung mit ihrem Zweck an.

Schnittstelle	Zweck
Microsoft Graph (Anwendungsrollen)	Benutzer, Gruppen, Lizenzen, Anwendungen und Stammdaten des Mandanten; Nutzungsberichte und Anmeldungen; Administratorrollen und PIM; Sicherheitsbewertung, Vorfälle, Warnungen, Risiken, Threat Hunting, Angriffssimulation und Sensoren von Defender for Identity; Richtlinien für bedingten Zugriff, Vertraulichkeit und Aufbewahrung, eDiscovery, Zugriffsüberprüfungen, Berechtigungsverwaltung, Lebenszyklus-Workflows und Zustimmungsanfragen; Speicher und Freigabeeinstellungen von SharePoint und OneDrive; Geräte, Gerätekonfiguration und App-Schutz aus Intune, Zeitpunkt der letzten LAPS-Rotation; Telefonie, Audiokonferenz und Webinare als Zahlungen; Raum-Ressourcen; Teams-Richtlinien
Microsoft Defender for Endpoint (Anwendungsrollen)	Onboarding-Status der Geräte, Schwachstellen
Exchange Online und Security & Compliance (Anwendungsrolle Exchange.ManageAsApp)	Postfächer, Posteingangsregeln, Delegierungen, Organisationskonfiguration und Purview-Richtlinien — ausschließlich mit lesenden Befehlen
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

Die Anwendungsrollen für Microsoft Graph und Defender for Endpoint sind Leserollen — mit einer Ausnahme: 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.

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, und im Mandanten entsteht der Eintrag der Anmelde-Anwendung des Anbieters

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

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.
2. **Im Erhebungslauf:** Der Lauf ändert im Mandanten nichts und legt dort nur zweierlei an, beides Aufträge an Microsoft, die er zum Lesen braucht. (a) Für die Teams-Richtlinien einen Auftrag für eine Konfigurations-Momentaufnahme. Der Lauf liest sie aus und löscht den Auftrag wieder; ist sie am Ende seiner Wartezeit noch nicht fertig, bleibt der Auftrag stehen, und der nächste Lauf versucht erneut, ihn zu löschen. Unabhängig davon entfernt Microsoft ihn nach eigener Angabe nach sieben Tagen. Die Momentaufnahme zählt auf ein Kontingent, das Microsoft je Mandant vorgibt. (b) Für einzelne Intune-Berichte einen Exportauftrag, dessen Datei der Lauf lädt. Wie lange Microsoft den Auftrag aufbewahrt, bestimmt Microsoft.
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.

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

Jeder Nutzer meldet sich mit eigenem Konto und zweitem Faktor an. Rollen und Freigaben verwaltet der Endkunde in der Plattform; die Sicht des Partners regeln die Nutzungsbedingungen (§ 5), die Sicherheit der Verarbeitung der Vertrag zur Auftragsverarbeitung.

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.
4. **Reaktionszeiten:** Verbindliche Reaktions- und Wiederherstellungszeiten gelten nur, wenn sie gesondert vereinbart sind.

12. Vorschau-Funktionen, unentgeltliche Leistungen

Vorschau-Funktionen und unentgeltliche Leistungen regeln die Nutzungsbedingungen (§ 4 Abs. 2).

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.

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 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).
- 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.

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 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, Übergangszeitraum, Abruf und Löschung regeln die Nutzungsbedingungen (§ 6 Abs. 4 bis 8);

Wechsel und Export sind unentgeltlich.

2. Daten und Formate.

Daten	Format	Weg
Erhebungsberichte (Momentaufnahmen des Mandanten)	JSON (RFC 8259)	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)	auf Anforderung in Textform
Prüfprotokoll der Organisation	JSON (RFC 8259) oder CSV (RFC 4180)	auf Anforderung in Textform

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. 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.