

MCP-Zugriffsmatrix: Welche Systeme, welche Rechte

Je System eine Zeile, drei Fragen: lesen, schreiben, Freigabe. Ausgefüllt ist das Blatt die Grundlage für AV-Vertrag, Betriebsrat und den ersten Server.

BETRIEB / BEREICH	DATUM	AUSGEFÜLLT VON
-------------------	-------	----------------

01 SYSTEM-INVENTAR ☐ System 1 · Eigentümer · Datenart · Zahl der Nutzer ☐ System 2 · Eigentümer · Datenart · Zahl der Nutzer ☐ System 3 · Eigentümer · Datenart · Zahl der Nutzer ☐ System 4 · Eigentümer · Datenart · Zahl der Nutzer ☐ System 5 · Eigentümer · Datenart · Zahl der Nutzer	02 ZUGRIFFSART JE SYSTEM ☐ System 1 · Lesen () · Schreiben () · Freigabe nötig () ☐ System 2 · Lesen () · Schreiben () · Freigabe nötig () ☐ System 3 · Lesen () · Schreiben () · Freigabe nötig () ☐ System 4 · Lesen () · Schreiben () · Freigabe nötig () ☐ System 5 · Lesen () · Schreiben () · Freigabe nötig ()
03 RECHTEQUELLE ☐ Zugriff im Namen des Nutzers (OAuth 2) () oder technisches Konto () ☐ Rechte kommen aus dem Quellsystem () Begründung bei Nein ☐ Personendaten enthalten? () DSFA nötig (DSGVO Art. 35)? () ☐ MCP-Server: Hersteller / Open Source / Eigenbau · geprüft von	04 PROTOKOLL UND BETRIEB ☐ Ablageort des Zugriffsprotokolls · Aufbewahrung ☐ Wer wertet wöchentlich aus? ☐ Betriebsrat informiert (BetrVG § 87) () Datum ☐ AV-Vertrag mit Anbieter (DSGVO Art. 28) () Datum
05 FREIGABEREGEL FÜR SCHREIBZUGRIFFE ☐ Frühester Termin für ersten Schreibzugriff (nach Protokollauswertung) ☐ Wer gibt eine Schreibaktion frei? (Rolle, Kanal) ☐ Welche Aktionen bleiben dauerhaft ausgeschlossen?	

REIHENFOLGE

1 Inventar	2 Lesezugriff	3 Rechte prüfen	4 Protokolle auswerten	5 Schreibzugriff einzeln
------------	---------------	-----------------	------------------------	--------------------------



TIPPS VOM BYTE

- Ein Protokoll ändert nichts an Berechtigungen. Was der Nutzer im ERP nicht darf, darf der Agent auch nicht.
- Starten Sie mit Lesezugriff auf zwei Systeme. Schreibzugriff kommt, wenn der Lesezugriff vier Wochen sauber lief.
- Fragen Sie den Anbieter, wo die Anbindung läuft und was das Modell zu sehen bekommt. Beides gehört in den AVV.

GEGENZEICHNUNG

Fachbereich	IT	Geschäftsführung
-------------	----	------------------

Regel: Kein Schreibzugriff, bevor vier Wochen Leseprotokolle ausgewertet sind und eine Freigaberegul steht.