

KI-Use-Cases & Datenregeln — was darf rein, was darf die KI tun?

DATENSCHUTZ & KI-RECHT — Schutz der Menschen hinter den Daten				zuständig: Datenschutzbeauftragter (extern): John Maik Ryssel, clever datenschutz GmbH	
Gemeint sind Kunden, Ansprechpartner, Eigentümer, Mieter und Mitarbeitende. Rechtlicher Rahmen: DSGVO (Umgang mit personenbezogenen Daten) und AI Act — die EU-KI-Verordnung verlangt u. a. Schulung der Nutzer, geprüfte Veröffentlichungen und einen Hinweis, wenn Kunden direkt mit einer KI sprechen.					
G1 — Gebäudedaten ohne Personenbezug, keine Stufen Regel: erlaubt — Kennwerte, Pläne, Abrechnungen, Anlagentechnik. Einfach grün. Versteckte Personendaten: z.B. Eigentümernamen und Wohnadressen in Plänen/Unterlagen vorher raus — sonst gilt K2.		K1–K3 — Personendaten jede Datenart im Detail: Seite 2 K1 berufliche Kontaktdaten: Name, berufl. Mail/Telefon, Funktion, Firmenanschrift — erlaubt. K2 privat & sensibel: private Wohnadresse, Gebäudeeigentum, private IBAN/Steuernr., Konditionen — nur wenn nötig, vorher aufräumen. K3 höchste Stufe: Gesundheit, Mieter-/Bewohnerdaten, besondere Kategorien — gesperrt, nur komplett anonym.		M1 / M2 — Mitarbeiterdaten M1 erlaubt · M2 gesperrt M1: Name, berufliche E-Mail, Benutzer-ID + technische Nutzungsdaten der KI-Systeme — erlaubt. M2 — alle sonstigen Mitarbeiterdaten: gesperrt. Auffangregel: Was nicht ausdrücklich M1 ist, ist M2. Ausnahmen: Personalvorgänge nur als komplett anonyme Fallbeschreibung; interne Aufzeichnungen nur mit Einwilligung.	
erlaubt nur unter Auflage erlaubt (Rechtsgrundlage nach DSGVO — z. B. berechtigtes Interesse oder Einwilligung — und/oder Bedingung wie Aufräumen, menschliche Prüfung, IT-Freigabe) nicht erlaubt (nach DSGVO gesperrt oder aus Systemschutz-Gründen verboten)					
Grundprinzip Datenminimierung: Immer nur die Daten hinein, die der Zweck wirklich braucht — die DSGVO gibt Betroffenen Anspruch auf minimalste Daten. Ganze, ungeprüfte Ordner sind deshalb regelmäßig unzulässig.					
Nr	Use Case — Beispiel	Daten	Zugriffsweg	Regel / Auflage	Status
A	Beratung & Berichte				
A1	Berichte & Inhalte für Beratungsprojekte Energieberatungsbericht T2	G1 · K1 (K2)	Chat / Skill	Ergebnis wird fachlich geprüft, bevor es zum Kunden geht. Keine Fotos mit erkennbaren Gesichtern von Mietern oder Kunden in den Bericht nehmen. Bei Privatkunden (K2), Namen erst am Ende einfügen.	Erlaubt
A2	Berichte aus eigener KI-WebApp GEKO-Bericht T3	G1 · K1	eigene App	Unterschied zu A1: Daten liegen vorübergehend in der App. App über IT-Freigabeprozess; Berichte menschlich geprüft.	Mit Auflage auch Systemschutz
A3	Auswertung Gebäudepläne & Abrechnungen DIN 276 T3	G1 · K1	Chat / Ordner	Nur G1- und K1-Daten — erlaubt. Gegebenenfalls müssen versteckte personenbezogene Daten entfernt werden (z.B. private Wohnadresse)	Erlaubt
A4	Angebotsvergleich Fachunternehmer Heizung / PV, Cowork	G1 · K1 (K2)	aufgeräumter Ordner	Anbieter-Kontaktdaten sind in der Regeln beruflich = K1 (auch Firmenadresse und Bezahldaten); bei Firmenkunden ebenfalls K1, bei Privatkunden Anschrift (K2) okay, weitere K2-Daten ggf. schwärzen	Erlaubt
B	Kommunikation & Vertrieb				
B1	Kundenmails beantworten 1:1 einfügen im Chat, Vertrieb	K1	Chat	Generell K1 — enthält der Text K2/K3 (z. B. Krankheitsthemen): nicht einfügen, manuell prüfen. Gesendet wird immer von Menschen.	Erlaubt
B2	Agent im geteilten Postfach energieberatung@ in T2	G1 · K1 (K2)	Agent	Agent ok — sortiert & entwirft, versendet nie (Systemschutz-Regel). Unbekannter Posteingang bleibt Restrisiko; K2 Daten nur nutzen, wenn für den Zweck erforderlich.	Mit Auflage auch Systemschutz
B3	Pipeline-Scoring im Vertrieb Wochenpriorisierung T3	G1 · K1	Chat / KI-Konto	Bewertet werden Verkaufschancen, nicht Personen — kein Profiling.	Erlaubt
B4	Meeting-Transkription & Zusammenfassung Kundentermine	K1	Tool / Chat	Nur mit vorheriger Einwilligung (Strafrecht!). Extern: dokumentiert (schriftlich oder Chat-Abfrage). Intern: Team-Einverständnis abfragen. Keine Meeting-Transkription für M2-Themen.	Mit Auflage
C	Interne Prozesse & HR				
C1	Mitarbeitergespräche vorbereiten Denkpartner, alle Teams	M2	Chat	Nur als komplett anonyme Fallbeschreibung — keine Namen, keine Rollen/Teams, keine erkennbaren Umstände. Sonst gesperrt.	Mit Auflage
C2	Mitarbeiterprofile mit persönlichen Daten Personio, Gesundheit	M2	Chat	Besondere Kategorien, keine Rechtsgrundlage — gesperrt.	Gesperrt
C3	Qualitätssicherung Fördervorgänge T4	G1 · K2	aufgeräumter Ordner	Ganze Ordner nein — Datenminimierung: nur nötige Unterlagen, private IBAN/Steuernummern immer raus, sofern diese nicht direct benötigt werden (berechtigtes Interesse).	Mit Auflage
C4	Recruiting & Bewerbungsunterlagen	M2	alle	Bis auf Weiteres gesperrt — Beschäftigtendatenschutz, Diskriminierungsrisiko.	Gesperrt
C5	Interne Meetings aufzeichnen & transkribieren Teammeetings, Besprechungen	M2	Tool / Chat	Nur mit Einwilligung der Teilnehmenden (vorab informieren) — nie zur Leistungs- oder Verhaltensbewertung.	Mit Auflage
D	Marketing & Veröffentlichung				
D1	Fachcontent erstellen Blog, LinkedIn, Förderthemen — Team 3	—	Chat	Redaktionelle Prüfung + verantwortliche Person (zentrale Kanäle: Marketingleitung; Team-Content: Teamleitung) — nie ungeprüft veröffentlichen.	Mit Auflage
D2	Referenzprojekte mit Kundennennung Case Studies	K1	Chat	Nur mit dokumentierter Kundenfreigabe + Redaktionsprüfung.	Mit Auflage

SYSTEMSCHUTZ — Schutz unserer Systeme & Ablagen			
Unser SharePoint, Postfächer und Rechner sollen geschützt werden. Risiken: KI verändert oder löscht Dateien, schafft Wildwuchs, lädt Schadsoftware, bekommt zu weite Rechte. Zuständig: IT (Jonas Hofheinz).			
Die fünf Wege, wie KI an unsere Daten kommt Von oben nach unten sieht die KI mehr und darf mehr selbst tun — deshalb werden die Regeln strenger. 1 Chat-Eingabe Du fügst Inhalte selbst in den Chat ein — die KI sieht genau das, nicht mehr. Regel: frei — beachte nur die Datenregeln links. 2 Aufgeräumter Ordner Du stellst einen Ordner zusammen und gibst diesen für die KI frei; die KI liest nur diese Dateien. Regel: erlaubt — vorher aufräumen: nur die Dateien hineinlegen, die für die Aufgabe gebraucht werden; es gelten die Datenregeln links. 3 Eingeschränktes KI-Konto Die KI bekommt ein eigenes M365-Konto, das nur festgelegte Postfächer oder Ablagen sehen kann. Regel: unser Standardweg, wenn die KI dauerhaft Zugriff braucht. Die IT richtet das Konto ein; was es sehen darf, wird nur nach Freigabe durch IT, Datenschutzbeauftragten und Geschäftsführung geändert. 4 Agent Die KI arbeitet länger selbstständig, im agentischen Modus. Regel: nur mit eng umrissenem Auftrag und IT-Freigabe — sie sortiert und entwirft, versendet aber nie selbst. Sie hat nie übergordnet Schreibrecht auf unserem Sharepoint. 5 Vollzugriff-Connector Die KI wird direkt mit dem ganzen Postfach oder dem ganzen SharePoint verbunden. Regel: verboten. Neue Verbindungen (Connectoren) beantragt man bei der IT — genehmigt wird höchstens die eingeschränkte Variante über Weg 3. In jedem Fall gilt: keine Schreibrechte auf SharePoint, kein Mailversand durch Agents — Ergebnisse legt ein Mensch ab. Beide Sperren werden von der IT technisch erzwungen und dokumentiert, nicht nur als Regel aufgeschrieben.			
S	Technik & Zugriffe		
Nr	Use Case — Zugriffsweg	Regel / Auflage	Status
S1	Cowork mit freigegebenen Projektordnern Weg 2: Ordner — Standardweg	Auf dem SharePoint darf die KI nichts verändern oder speichern — Ihr arbeitet mit lokalen Kopien, das Ergebnis legt Ihr dann wieder im Sharepoint ab.	Mit Auflage
S2	Claude-Plugins & Erweiterungen pptx / Word / Excel ...	Die eingebauten Anthropic-Funktionen (Word-, Excel-, PowerPoint-Dateien erstellen) sind frei — es gelten die normalen Datenregeln; keine K3-/M2-Daten, K2 vorher aufräumen. Weitere Plugins nur nach IT-Freigabe. Browser nicht freigegeben.	Mit Auflage
S3	App-Entwicklung mit Claude Code Code — Datenaufnahme-App T3	Bevor entwickelt wird, prüft die IT das Setup und gibt es frei. Entwickelt wird nur im Firmennetz — keine private Umgebung.	Mit Auflage
S4	Connector: persönliches Outlook-Postfach Weg 5: Vollzugriff	Nicht erlaubt: Das private Postfach enthält auch private Mails (M2). Die IT sperrt diese Verbindung technisch.	Gesperrt auch DS
S5	Connector: SharePoint (Vollzugriff) Weg 5: Vollzugriff	Nicht erlaubt: Nutze stattdessen S1 (freigegebener Projektordner). Neue Connectoren nur per Antrag bei der IT.	Gesperrt auch DS
Unser Standard: Die KI bekommt breite Zugriffe nie direkt, sondern nur über eigene, eingeschränkte M365-Konten, die die IT verwaltet. Wer einen neuen Connector oder ein neues Plugin braucht, stellt einen Antrag bei der IT; IT und Datenschutzbeauftragter prüfen, die Geschäftsführung gibt frei. So bleibt jederzeit nachvollziehbar, worauf KI zugreifen kann.			
Erlaubt Mit Auflage Gesperrt (Farblogik: siehe Legende links oben) Datenkürzel: G1 Gebäudedaten (ohne Personenbezug) · K1 berufliche Kontaktdaten · K2 privat & sensibel · K3 höchste Stufe · M1 Mitarbeiter-Basisdaten (erlaubt) · M2 sonstige Mitarbeiterdaten (gesperrt) — jede Datenart im Detail: Seite 2			

Datenkatalog — jede Datenart im Detail

Frei / K1 / M1	erlaubt	K2	nur wenn für den Zweck nötig — vorher aufräumen, im Zweifel raus/schwärzen	K3	gesperrt — nur komplett anonymisiert	M2	gesperrt — Ausnahmen stehen in der Tabelle	Gesperrt	nie eingeben
Grundprinzip Datenminimierung: Immer nur die Daten hinein, die der Zweck wirklich braucht — ganze, ungeprüfte Ordner sind regelmäßig unzulässig. Rechtsgrundlagen je Eintrag: KI-Nutzungsrichtlinie, Anlage 3 (erstellt unter Beratung vom Datenschutzbeauftragten).									

Gebäudedaten (G1)			
1	Gebäudekennwerte Fläche, Baujahr, Zustand, U-Werte, DIN-Berechnungen	Frei	Sachdaten — kein Personenbezug
2	Baupläne & Grundrisse ohne Eigentümer-/Bewohnerangaben	Frei	Achtung: Pläne enthalten oft Eigentümernamen und Wohnadressen → vorher entfernen, sonst gilt K2
3	Energieabrechnungen auf Gebäudeebene Gesamtverbrauch ohne Haushaltszuordnung	Frei	einzelne Haushalte erkennbar → K2 (private Energiedaten)
4	Anlagentechnik Heizung, PV, Lüftung, hydraulischer Abgleich	Frei	
5	Objektadresse reine Gebäudeadresse ohne Personenzuordnung	Frei	Grenzfall: kombiniert mit Eigentümer-/Bewohnernamen → K2
6	Förder- und Programmdaten BEG, iSFP-Inhalte ohne Personendaten	Frei	

Person — geschäftlich			
7	Name + berufliche Funktion Ansprechpartner einer Firma/Kommune	K1	berufliche Kontaktdaten
8	Berufliche E-Mail / Telefonnummer vorname.name@firma.de, Durchwahl	K1	
9	Firmenanschrift Anschrift des Unternehmens/der Kommune	K1	Anschrift natürlicher Personen (privat) → K2
10	E-Mail-Signatur (geschäftlich) Name, Funktion, Firmendaten	K1	
11	Inhalt geschäftlicher E-Mails Sachthemen, Projektabsprachen	K1	enthält der Text private/sensible Angaben (z. B. Krankheit) → K2/K3: nicht einfügen, manuell prüfen
12	Vertragskonditionen & Angebotspreise Preise, Rabatte, Zahlungsziele	K2	zugleich Geschäftsgeheimnis (eigenes und fremdes)
13	Bankverbindung / UST-ID einer Firma IBAN, Steuernummern juristischer Personen	K2	bei juristischen Personen nicht personenbezogen, aber vertraulich; bei Einzelunternehmern personenbezogen
14	Meeting-Aufzeichnung & KI-Transkription (Kunden) Aufzeichnung/Transkription von Kundenterminen	K2	nur mit vorheriger Einwilligung — zu Beginn auf Aufzeichnung, KI und Zweck hinweisen; nicht Nötiges aus Transkripten entfernen
15	Foto im beruflichen Kontext Website-Porträt, Teamfoto	K2	Nutzung/Veröffentlichung nur mit Einwilligung; Redaktionsregel beachten

Person — privat			
16	Private Wohnadresse auch aus Plänen, Grundbuch, Verträgen	K2	
17	Gebäudeeigentum / Eigentümerstellung wem ein Gebäude gehört, Eigentümerlisten (WEG)	K2	
18	Private Telefonnummer / E-Mail	K2	
19	Private IBAN / Bankverbindung z. B. in Förderanträgen	K2	kritisch — im Zweifel raus oder schwärzen
20	Private Steuernummer / Steuer-ID z. B. in Förderanträgen	K2	kritisch — wie private IBAN
21	Private Energie-/Verbrauchsdaten Verbrauch eines identifizierbaren Haushalts	K2	berechtigtes Interesse — dokumentieren
22	Geburtsdatum	K2	
23	Foto/Bild einer Person (privat) Bewohnerfotos, Personen auf Baustellen	K2	Veröffentlichung nur mit Einwilligung; biometrische Auswertung → K3
24	Unterschriften auf gescannten Dokumenten	K2	schwärzen, wenn nicht nötig

Person — besonders geschützt			
25	Mieter-/Bewohnerdaten Namen, Wohneinheiten, Mietverhältnisse	K3	häufigster Risikofall bei Wohnungswirtschafts-Kunden

Person — besonders geschützt (Fortsetzung)			
26	Gesundheitsdaten auch beiläufig, z. B. Krankheit in einer Kundenmail	K3	besondere Kategorie (Art. 9 DSGVO)
27	Religion, Gewerkschaft, Sozial-/Härtefalldaten z. B. Härtefallanträge	K3	besondere Kategorie (Art. 9 DSGVO)

Mitarbeitende — M1 (erlaubt)			
28	Name und berufliche E-Mail-Adresse inkl. technischer Benutzer-ID für Accounts	M1	nur erforderliche Identifikations- und Accountdaten
29	Nutzungs- & Protokolldaten der KI-Systeme Logins, Nutzungszeiten, Audit-Logs, Mengendaten	M1	keine Prompt-Inhalte, keine Leistungsbewertung — sonst M2

Mitarbeitende — M2 (gesperrt)			
30	Meeting-Aufzeichnung & KI-Transkription (intern) interne Meetings, Besprechungen	M2	Sonderfall: nur mit Einwilligung der Teilnehmenden — nie zur Leistungs- oder Verhaltensbewertung
31	Mitarbeiter-Gesprächsdaten / Personalvorgänge MA-Gespräche, Konflikte, Leistung, Feedback	M2	Ausnahme: komplett anonyme Fallbeschreibung — keine Namen, Rollen, Teams oder erkennbaren Umstände
32	Bewerbungsunterlagen Lebensläufe, Zeugnisse, Bewertungen	M2	KI-gestützte Bewerberauswahl kann Hochrisiko nach AI Act sein
33	Personio-/HR-Daten alle Exporte und Auszüge	M2	keine HR-Exporte, keine Connector-Zugriffe
34	Private E-Mails & private Kommunikation private Inhalte im dienstlichen Postfach	M2	Grund für die Sperre des Outlook-Connectors
35	Inhaltsdaten der eigenen KI-Nutzung eigene Angaben im Chat über sich selbst	M2	erlaubt nur, soweit für die eigene Nutzung nötig — keine Auswertung durch andere
36	Sonstige Beschäftigtendaten Gehalt, Arbeitszeiten, Urlaub, Krankheit, Bewertungen ...	M2	Auffangregel: Was nicht ausdrücklich M1 ist, ist M2

Sicherheit			
37	Passwörter & Zugangsdaten API-Schlüssel, TAN, PINs, Tokens	Gesperrt	gilt immer — Systemschutz