

KI-Nutzungsrichtlinie (Acceptable Use Policy)

MUSTER — kein Rechtsrat. Vor Verwendung durch DSB/Fachanwalt prüfen lassen.
Betreiber: [Firma] · Stand: [Datum] · Version: 1.0 · Freigegeben von: [Name/Funktion]

1. Zweck und Geltungsbereich

Diese Richtlinie regelt die Nutzung von KI-Diensten (z. B. Chat-Assistenten, Text-/Code-Generatoren) durch alle Beschäftigten, Auszubildenden und externen Mitarbeitenden von [Firma]. Sie gilt für alle betrieblich genutzten Geräte und für jede dienstliche Verarbeitung von Unternehmens- oder personenbezogenen Daten.

2. Grundsatz — KI-Zugriff nur über das Gateway

- KI-Dienste dürfen **ausschließlich über das bereitgestellte AISecurityGateway** genutzt werden. Das Gateway filtert personenbezogene Daten heraus, bevor sie an externe KI-Anbieter gelangen.
- Die **direkte** Nutzung von KI-Web-Frontends (z. B. über den Browser) oder von KI-APIs **am Gateway vorbei** ist untersagt. Technische Sperren (DNS-Filter) dürfen nicht umgangen werden.
- Das Einrichten eigener DNS-Resolver, VPNs oder Proxys zur Umgehung der Schutzmaßnahmen ist untersagt.

3. Verbotene Eingaben

Auch über das Gateway gilt: In KI-Dienste dürfen **nicht** eingegeben werden, soweit nicht ausdrücklich freigegeben:

- Klar erkennbare personenbezogene Daten Dritter (Kunden, Kolleg:innen, Bewerber:innen),
- besondere Kategorien personenbezogener Daten (Art. 9 DSGVO: Gesundheit, u. Ä.),
- Zugangsdaten, Schlüssel, Passwörter,
- vertrauliche Geschäftsgeheimnisse, soweit nicht durch die Blacklist abgedeckt.

Im Zweifel gilt: **nicht eingeben** und [zuständige Stelle] fragen.

4. Zulässige Nutzung

Freigegeben ist die Nutzung für [z. B. Recherche, Entwurfstexte, Code-Hilfe, Zusammenfassungen] im Rahmen der dienstlichen Aufgaben. Ergebnisse sind vor Verwendung fachlich zu prüfen (keine ungeprüfte Übernahme).

5. Home-Office und mobile Geräte

Bei Tätigkeit außerhalb des Betriebs gelten zusätzlich der **Home-Office-Datenschutz-Zusatz** und die **Mobile-/BYOD-Richtlinie**. Insbesondere ist im Home-Office das Unternehmens-[VPN] zu nutzen, damit die Schutzmaßnahmen greifen.

6. Protokollierung

Die Nutzung wird zu Sicherheits- und Nachweiszwecken protokolliert (nur Metadaten, keine Klartext-Inhalte). Näheres regeln die Datenschutzinformation und ggf. die Betriebsvereinbarung.

7. Folgen bei Verstoß

Verstöße können [arbeitsrechtliche Maßnahmen nach Maßgabe von Gesetz und Betriebsvereinbarung] nach sich ziehen.

8. Inkrafttreten

Diese Richtlinie tritt am [Datum] in Kraft.

Ich habe die Richtlinie erhalten und zur Kenntnis genommen:

Name: _____ Datum: _____ Unterschrift: _____