

ANHANG II

Beschreibung der Verarbeitung

I. Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- ☒ Studierende
- ☒ Beschäftigte
- ☒ Weitere berechnigte Nutzende

☐ Sonstige Personen:

II. Kategorien einfacher Daten, die verarbeitet werden:

Es werden einfache Daten verarbeitet, die nicht der DS-GVO unterfallen. Dies sind:

- a. Eingabedaten der Nutzenden (insb. sog. Prompts);
- b. Ausgabedaten der KI-Modelle (insb. sog. Completions);
- c. anonyme Identifikationsnummer (ID) der Konversation;
- d. anonyme Identifikationsnummer (ID) eines Konversationselements (insb. Eingabedaten und Ausgabedaten);
- e. genutztes KI-Modell;
- f. Zeitstempel eines Konversationselements;
- g. übertragene Tokenzahl der Eingabedaten und der Ausgabedaten;
- h. anonyme Identifikationsnummer (ID) des Kostenelements;
- i. Kosten.

III. Kategorien personenbezogener Daten, die verarbeitet werden:

Es werden personenbezogene Daten gem. Art. 4 Abs. 1 DS-GVO verarbeitet. Dies sind:

Kategorie 1: Daten, die im Rahmen der **Shibboleth-Anbindung** übertragen werden. Diese sind:

- a. Die Identity Provider (IDP)-spezifische, eindeutige, persistierende ID zur Person (vom IDP generiert);
- b. Rollen bzw. Gruppen der Person (die Bezeichnung richtet sich nach der Benennung durch die Auftraggeberin);
- c. Art der Zugehörigkeit zur eigenen Organisation;
- d. Zugehörige Domain der eigenen Organisation.

Kategorie 2: Ferner werden Daten als Teil der **Browsersession** übertragen. Diese sind:

- a. Von der Person festgelegter Rufname;
- b. Nachnamen;
- c. Dienstliche E-Mail-Adresse.

Kategorie 3: Ferner wird bei der Nutzung der Webseite ein **Authentifizierungs-Cookie** gesetzt. Dieser enthält:

- a. Shibboleth Session-ID;
- b. Einstellungen zur Cookie-Policy;
- c. IP-Adresse des Endgeräts der Person;
- d. ID des Dienstes KI:connect.nrw.

Es werden keine besonders sensiblen personenbezogene Daten gem. Art. 9 Abs. 1 DS-GVO verarbeitet.

Es werden keine personenbezogene Daten gem. Art. 10 DS-GVO verarbeitet.

Die drei Kategorien personenbezogener Daten werden zu keiner Zeit zwischen den Kategorien verknüpft. Insbesondere wird die Identity Provider (IDP)-spezifische, eindeutige, persistierende ID zur Person nicht mit Daten aus den Kategorien 2 und 3 verknüpft.

IV. Art der Verarbeitung der personenbezogenen Daten:

Für die Kategorien 1 und 2 werden Daten transportverschlüsselt übertragen und als Datenbankeinträge bei der Auftragnehmerin gespeichert.

Für die Kategorie 3 werden Daten als Hash-Werte auf dem Endgerät der Nutzenden gespeichert.

V. Zwecke, für die die Daten im Auftrag der Auftraggeberin verarbeitet werden:

1. Beschreibung der Verarbeitungszwecke einfacher Daten:

Die einfachen Daten werden für folgende Zwecke verarbeitet:

- a. Anlegen von persistierenden Konversationen zwischen Nutzenden und KI-Modellen;
- b. Kostenzuordnung der Konversation zu Kostenelementen.

2. Beschreibung der Verarbeitungszwecke personenbezogener Daten:

Die *pseudonymisierte ID der Nutzenden* gemäß Kategorie 1.a wird für folgende Zwecke verarbeitet:

- a. Eindeutige Zuordnung von Konversationen zu Nutzenden.

Die *Rolle bzw. Gruppe der Nutzenden* gemäß Kategorie 1.b wird für folgende Zwecke verarbeitet:

- a. Feststellung der Berechtigung der Nutzenden zur Verwendung bestimmter Funktionen (insb. Nutzung bestimmter KI-Modelle);
- b. Bestimmung des Kostenelements, dem eine Konversation zugeordnet ist.

Die *Art der Zugehörigkeit zur Organisation* gemäß Kategorie 1.c wird für folgende Zwecke verarbeitet:

- a. Feststellung der Berechtigung der Nutzenden zur Nutzung des Dienstes und Ausschluss nicht-berechtigter Nutzender von der Nutzung des Dienstes;
- b. Bestimmung des Kostenelements, dem eine Konversation zugeordnet ist.

Die *Domain zur Organisation* gemäß Kategorie 1.d wird für folgende Zwecke verarbeitet:

- a. Rückmeldung der Berechtigungsprüfung an die Nutzenden.

Es werden *keine* Accounts für die Nutzenden bei der Auftragnehmerin angelegt.

Die ID zur Person gemäß Kategorie 1.a wird ausschließlich als Teil einer Konversation gespeichert. Die Rollen bzw. Gruppen der Person gemäß Kategorie 1.b sowie die Zugehörigkeit und Domain zur eigenen Organisation gemäß Kategorien 1.c und 1.d dienen zur Bestimmung des anonymen Kostenelements für die Konversation. Es findet keine weitere Verarbeitung statt.

Der *Rufname, Nachnamen* und *dienstliche E-Mail Adresse* gemäß Kategorie 2.a bis 2.c werden für folgende Zwecke verarbeitet:

- a.. Anzeige von Personeninformationen in der Benutzeroberfläche im Bereich „Einstellungen“.

Die *Cookie-Daten* gemäß Kategorie 3.a bis 3.d werden für folgende Zwecke verarbeitet:

- a. Ermöglichung der zur Anzeige der Webseite des Dienstes technisch notwendigen Funktionen.

VI. Dauer der Verarbeitung der personenbezogenen Daten:

Personenbezogene Daten werden ausschließlich als Teil einer Konversation gespeichert (s. Abs. V). Für diese gibt es drei Arten von Löschanlässen:

1. *Löschersuchen gemäß Art. 17 DS-GVO*: Die Nutzenden verlangen die unverzügliche Löschung ihrer personenbezogenen Daten.
2. *Manuelle Löschung durch die Nutzenden*: Die Nutzenden veranlassen die Löschung von Daten durch eine Interaktion mit dem Dienst (z.B. Klicken eines Löschsymbols).
3. *Automatische Löschung*: Die eigene Organisation kann Löschzeiträume für Daten festlegen. Nach deren Ablauf wird die Löschung der Daten automatisch veranlasst.

Der Zugriff auf den Dienst ist an den qualifizierenden Status als Mitglied oder Angehörige bzw. Angehöriger der Auftraggeberin gebunden. Der Verlust des qualifizierenden Status wird technisch analog zum Löschersuchen gemäß Art. 17 DS-GVO behandelt.

Kategorien einfacher Daten a und b (Eingabedaten und Ausgabedaten) werden bei einem Löschauftrag der Art 1 unverzüglich gelöscht. Bei einem Löschauftrag der Arten b und c werden sie nach 14 Tagen gelöscht, um eine vorherige Wiederherstellung durch die Nutzenden zu ermöglichen.

Kategorien einfacher Daten c bis i werden bis zum Ende der laufenden Abrechnungsperiode, höchstens aber für 386 Tage gespeichert. Die Speicherung erfolgt zur Ermöglichung der Kostenrechnung.

Personenbezogene Daten der Kategorie 1 werden bei einem Löschauftrag der Art 1 unverzüglich anonymisiert. Bei einem Löschauftrag der Arten b und c werden sie nach 14 Tagen anonymisiert, um eine vorherige Wiederherstellung durch die Nutzenden zu ermöglichen.

Personenbezogene Daten der Kategorie 2 werden für die Dauer der Browsersession gespeichert.

Personenbezogene Daten der Kategorie 3 werden entweder bis zur Löschung des Cookies oder für die Gültigkeitsdauer des Cookies von höchstens 24h gespeichert.

VII. Datenzugriff

Der *Zugriff auf Daten durch Dritte oder betroffene Personen* ist in Klausel 8 Buchstabe a) in Verbindung mit Klausel 7 Abs. 4 Buchstabe b) und Klausel 11 Abs. 2 des Auftragsverarbeitungsvertrags geregelt.

Der *Zugriff auf eigene Daten* ist ferner wie folgt geregelt:

1. Nutzende haben ausschließlich Zugriff auf die Daten, die sie selbst eingegeben haben bzw. die für die Erbringung der Dienstleistung notwendig sind.
2. Natürliche Personen, denen die Auftraggeberin ausdrücklich die Berechtigung erteilt hat, haben ausschließlich Zugriff auf einfache Daten der Kategorien c bis i.
3. Von den Nutzenden aktiv zugelassene Dritte können über eine Freigabe- oder Einladungsfunktion Zugriff auf Daten erhalten, die die Nutzenden selbst eingegeben haben bzw. die für die Erbringung der Dienstleistung notwendig sind. Die Zugriffsberechtigung erfolgt ausschließlich auf Basis der von den Nutzenden erteilten Einwilligung oder Anweisung.

VIII. Fernwartung

Räumlich getrennte Zugriffe der Auftragnehmerin auf IT-Systeme der Auftraggeberin zu Wartungs- oder Reparaturzwecken (Fernwartung) finden nicht statt.

IX. Drittlandtransfer

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union statt.