



# Datenschutzkonzept

LDA Legal Data Analytics GmbH

Stand: 25.09.2026

Version: 1.0

# Inhaltsverzeichnis

|                                                                                            |           |
|--------------------------------------------------------------------------------------------|-----------|
| Inhaltsverzeichnis.....                                                                    | 2         |
| Definitionen.....                                                                          | 9         |
| <b>A. Allgemeiner Teil .....</b>                                                           | <b>12</b> |
| I.    Zweck und Hintergrund des Datenschutzkonzepts.....                                   | 12        |
| II.   Aufbau und Funktionsweise des Datenschutzkonzepts .....                              | 12        |
| III.  Beschreibung des LDA-Tools .....                                                     | 12        |
| IV.  Technische Infrastruktur.....                                                         | 13        |
| V.    Rollen .....                                                                         | 14        |
| 1.    Rolle des Kunden .....                                                               | 14        |
| 2.    Rolle der LDA .....                                                                  | 14        |
| 3.    Beziehung zu den Nutzern.....                                                        | 15        |
| 4.    Rolle von Partnern mit eigener Drittapplikation .....                                | 15        |
| <b>B. Besonderer Teil .....</b>                                                            | <b>16</b> |
| I.    Verarbeitungsvorgänge bei der Nutzung des LDA-Tools .....                            | 16        |
| 1.    Indexierung von Verlags- bzw. Kundenfachinhalten (Vorbereitung der Datenbasis) ..... | 16        |
| 1.1.    Beschreibung des Verarbeitungsvorgangs .....                                       | 16        |
| 1.2.    Art der personenbezogenen Daten .....                                              | 17        |
| 1.3.    Kategorien betroffener Personen .....                                              | 17        |
| 1.4.    Empfänger der Daten.....                                                           | 17        |
| 1.5.    Regelfristen für die Löschung der Daten .....                                      | 17        |
| 1.6.    Übermittlung der Daten in Drittländer .....                                        | 17        |
| 1.7.    Einhaltung der Datenschutzgrundsätze .....                                         | 18        |
| 1.7.1.    Rechtmäßigkeit der Verarbeitung.....                                             | 18        |
| a)        Perspektive des Kunden .....                                                     | 18        |
| b)        Perspektive von LDA .....                                                        | 18        |
| 1.7.2.    Transparenz .....                                                                | 18        |
| 1.7.3.    Zweckbindung.....                                                                | 18        |
| 1.7.4.    Datenminimierung .....                                                           | 18        |
| 1.7.5.    Richtigkeit.....                                                                 | 18        |
| 1.7.6.    Integrität und Vertraulichkeit.....                                              | 19        |
| 1.7.7.    Rechenschaftspflicht.....                                                        | 19        |
| 2.    Infrastruktur und Anwendungsbetrieb .....                                            | 19        |
| 2.1.    Beschreibung des Verarbeitungsvorgangs .....                                       | 19        |
| 2.2.    Art der personenbezogenen Daten .....                                              | 19        |

|        |                                               |    |
|--------|-----------------------------------------------|----|
| 2.3.   | Kategorien betroffener Personen .....         | 20 |
| 2.4.   | Empfänger der Daten .....                     | 20 |
| 2.5.   | Regelfristen für die Löschung der Daten ..... | 20 |
| 2.6.   | Datenübermittlung in Drittländer .....        | 20 |
| 2.7.   | Einhaltung der Datenschutzgrundsätze .....    | 20 |
| 2.7.1. | Rechtmäßigkeit der Verarbeitung.....          | 20 |
| a)     | Perspektive des Kunden .....                  | 20 |
| b)     | Perspektive LDA .....                         | 20 |
| 2.7.2. | Transparenz .....                             | 21 |
| 2.7.3. | Zweckbindung.....                             | 21 |
| 2.7.4. | Datenminimierung .....                        | 21 |
| 2.7.5. | Richtigkeit.....                              | 21 |
| 2.7.6. | Rechenschaftspflicht.....                     | 21 |
| 3.     | Authentifizierung und Autorisierung.....      | 21 |
| 3.1.   | Beschreibung der Verarbeitungstätigkeit ..... | 21 |
| 3.1.1. | Modell 1 – Identity Provider des Kunden ..... | 21 |
| 3.1.2. | Modell 2 – Identity Provider der LDA.....     | 21 |
| 3.2.   | Art der personenbezogenen Daten .....         | 22 |
| 3.3.   | Kategorien betroffener Personen .....         | 22 |
| 3.4.   | Empfänger der Daten .....                     | 22 |
| 3.4.1. | Modell 1 – Identity Provider des Kunden ..... | 22 |
| 3.4.2. | Modell 2 – Identity Provider der LDA.....     | 22 |
| 3.5.   | Regelfristen für die Löschung der Daten ..... | 22 |
| 3.5.1. | Modell 1 – Identity Provider des Kunden ..... | 22 |
| 3.5.2. | Modell 2 – Identity Provider der LDA.....     | 23 |
| 3.6.   | Datenübermittlung in Drittländer .....        | 23 |
| 3.7.   | Einhaltung der Datenschutzgrundsätze .....    | 23 |
| 3.7.1. | Rechtmäßigkeit der Verarbeitung.....          | 23 |
| a)     | Perspektive des Kunden .....                  | 23 |
| b)     | Perspektive LDA .....                         | 23 |
| 3.7.2. | Transparenz .....                             | 24 |
| 3.7.3. | Zweckbindung.....                             | 24 |
| 3.7.4. | Datenminimierung .....                        | 24 |
| 3.7.5. | Richtigkeit.....                              | 24 |
| 3.7.6. | Integrität und Vertraulichkeit.....           | 24 |
| 3.7.7. | Rechenschaftspflicht.....                     | 24 |
| 4.     | Eingabeprozess.....                           | 25 |

|        |                                               |    |
|--------|-----------------------------------------------|----|
| 4.1.   | Beschreibung des Verarbeitungsvorgangs .....  | 25 |
| 4.2.   | Art der personenbezogenen Daten .....         | 25 |
| 4.3.   | Kategorien betroffener Personen .....         | 25 |
| 4.4.   | Empfänger der Daten .....                     | 25 |
| 4.5.   | Regelfristen für die Löschung der Daten ..... | 25 |
| 4.6.   | Datenübermittlung in Drittländer .....        | 26 |
| 4.7.   | Einhaltung der Datenschutzgrundsätze .....    | 26 |
| 4.7.1. | Rechtmäßigkeit der Verarbeitung.....          | 26 |
| a)     | Perspektive des Kunden .....                  | 26 |
| b)     | Perspektive LDA .....                         | 26 |
| 4.7.2. | Transparenz .....                             | 26 |
| 4.7.3. | Zweckbindung.....                             | 26 |
| 4.7.4. | Datenminimierung .....                        | 26 |
| 4.7.5. | Richtigkeit.....                              | 27 |
| 4.7.6. | Integrität und Vertraulichkeit.....           | 27 |
| 4.7.7. | Rechenschaftspflicht.....                     | 27 |
| 5.     | Verarbeitung der Eingabe .....                | 27 |
| 5.1.   | Beschreibung des Verarbeitungsvorgangs .....  | 27 |
| 5.2.   | Art der verarbeiteten Daten .....             | 28 |
| 5.3.   | Kategorien betroffener Personen .....         | 28 |
| 5.4.   | Empfänger der Daten.....                      | 28 |
| 5.5.   | Regelfristen für die Löschung der Daten ..... | 28 |
| 5.6.   | Datenübermittlung in Drittländer .....        | 28 |
| 5.7.   | Einhaltung der Datenschutzgrundsätze .....    | 28 |
| 5.7.1. | Rechtmäßigkeit der Verarbeitung.....          | 28 |
| a)     | Perspektive des Kunden .....                  | 28 |
| b)     | Perspektive LDA .....                         | 28 |
| 5.7.2. | Transparenz .....                             | 28 |
| 5.7.3. | Zweckbindung.....                             | 29 |
| 5.7.4. | Datenminimierung .....                        | 29 |
| 5.7.5. | Richtigkeit.....                              | 29 |
| 5.7.6. | Integrität und Vertraulichkeit.....           | 29 |
| 5.7.7. | Rechenschaftspflicht.....                     | 29 |
| 6.     | Suche nach relevanten Inhalten .....          | 29 |
| 6.1.   | Beschreibung des Verarbeitungsvorgangs .....  | 29 |
| 6.2.   | Art der personenbezogenen Daten .....         | 30 |
| 6.3.   | Kategorien betroffener Personen .....         | 30 |

|        |                                               |    |
|--------|-----------------------------------------------|----|
| 6.4.   | Empfänger der Daten .....                     | 30 |
| 6.5.   | Regelfristen für die Löschung der Daten ..... | 30 |
| 6.6.   | Datenübermittlung in Drittländer .....        | 30 |
| 6.7.   | Einhaltung der Datenschutzgrundsätze .....    | 30 |
| 6.7.1. | Rechtmäßigkeit der Verarbeitung.....          | 30 |
| a)     | Perspektive des Kunden .....                  | 30 |
| b)     | Perspektive LDA .....                         | 30 |
| 6.7.2. | Transparenz .....                             | 30 |
| 6.7.3. | Zweckbindung.....                             | 31 |
| 6.7.4. | Datenminimierung .....                        | 31 |
| 6.7.5. | Richtigkeit.....                              | 31 |
| 6.7.6. | Integrität und Vertraulichkeit.....           | 31 |
| 6.7.7. | Rechenschaftspflicht.....                     | 31 |
| 7.     | Antwortgenerierung.....                       | 31 |
| 7.1.   | Beschreibung des Verarbeitungsvorgangs .....  | 31 |
| 7.2.   | Art der personenbezogenen Daten .....         | 31 |
| 7.3.   | Kategorien betroffener Personen .....         | 32 |
| 7.4.   | Empfänger der Daten.....                      | 32 |
| 7.5.   | Regelfristen für die Löschung der Daten ..... | 32 |
| 7.6.   | Datenübermittlung in Drittländer .....        | 32 |
| 7.7.   | Einhaltung der Datenschutzgrundsätze .....    | 32 |
| 7.7.1. | Rechtmäßigkeit der Verarbeitung.....          | 32 |
| a)     | Perspektive des Kunden .....                  | 32 |
| b)     | Perspektive LDA .....                         | 32 |
| 7.7.2. | Transparenz .....                             | 33 |
| 7.7.3. | Zweckbindung.....                             | 33 |
| 7.7.4. | Datenminimierung .....                        | 33 |
| 7.7.5. | Richtigkeit.....                              | 33 |
| 7.7.6. | Integrität und Vertraulichkeit.....           | 33 |
| 7.7.7. | Rechenschaftspflicht.....                     | 33 |
| 8.     | Datenhaltung für Suchfunktionen.....          | 33 |
| 8.1.   | Beschreibung der Verarbeitung.....            | 33 |
| 8.2.   | Art der personenbezogenen Daten .....         | 34 |
| 8.3.   | Kategorien betroffener Personen .....         | 34 |
| 8.4.   | Empfänger der Daten.....                      | 34 |
| 8.5.   | Regelfristen für die Löschung der Daten ..... | 34 |
| 8.6.   | Datenübermittlung in Drittländer .....        | 34 |

|         |                                                    |    |
|---------|----------------------------------------------------|----|
| 8.7.    | Einhaltung der Datenschutzgrundsätze .....         | 34 |
| 8.7.1.  | Rechtmäßigkeit der Verarbeitung.....               | 34 |
| a)      | Perspektive des Kunden .....                       | 34 |
| b)      | Perspektive LDA .....                              | 35 |
| 8.7.2.  | Transparenz .....                                  | 35 |
| 8.7.3.  | Zweckbindung.....                                  | 35 |
| 8.7.4.  | Datenminimierung .....                             | 35 |
| 8.7.5.  | Richtigkeit.....                                   | 35 |
| 8.7.6.  | Integrität und Vertraulichkeit.....                | 35 |
| 8.7.7.  | Rechenschaftspflicht.....                          | 35 |
| 9.      | Qualitätssicherung/Produktverbesserung .....       | 35 |
| 9.1.    | Beschreibung des Verarbeitungsvorgangs .....       | 35 |
| 9.2.    | Art der personenbezogenen Daten .....              | 36 |
| 9.3.    | Kategorien betroffener Personen .....              | 36 |
| 9.4.    | Empfänger der Daten .....                          | 36 |
| 9.5.    | Regelfristen für die Löschung der Daten .....      | 36 |
| 9.6.    | Datenübermittlung in Drittländer .....             | 36 |
| 9.7.    | Einhaltung der Datenschutzgrundsätze .....         | 37 |
| 9.7.1.  | Rechtmäßigkeit der Verarbeitung.....               | 37 |
| a)      | Perspektive des Kunden .....                       | 37 |
| b)      | Perspektive LDA .....                              | 37 |
| 9.7.2.  | Transparenz .....                                  | 37 |
| 9.7.3.  | Zweckbindung.....                                  | 37 |
| 9.7.4.  | Datenminimierung .....                             | 37 |
| 9.7.5.  | Richtigkeit.....                                   | 37 |
| 9.7.6.  | Integrität und Vertraulichkeit.....                | 37 |
| 9.7.7.  | Rechenschaftspflicht.....                          | 37 |
| 10.     | Protokollierung und Monitoring zur Sicherheit..... | 38 |
| 10.1.   | Beschreibung des Verarbeitungsvorgangs .....       | 38 |
| 10.2.   | Art der personenbezogenen Daten .....              | 38 |
| 10.3.   | Kategorien betroffener Personen .....              | 38 |
| 10.4.   | Empfänger der Daten .....                          | 39 |
| 10.5.   | Regelfristen für die Löschung der Daten .....      | 39 |
| 10.6.   | Datenübermittlung in Drittländer .....             | 39 |
| 10.7.   | Einhaltung der Datenschutzgrundsätze .....         | 39 |
| 10.7.1. | Rechtmäßigkeit der Verarbeitung.....               | 39 |
| c)      | Perspektive des Kunden .....                       | 39 |

|         |                                               |    |
|---------|-----------------------------------------------|----|
| d)      | Perspektive LDA .....                         | 39 |
| 10.7.2. | Transparenz .....                             | 39 |
| 10.7.3. | Zweckbindung.....                             | 39 |
| 10.7.4. | Datenminimierung .....                        | 40 |
| 10.7.5. | Richtigkeit.....                              | 40 |
| 10.7.6. | Integrität und Vertraulichkeit.....           | 40 |
| 10.7.7. | Rechenschaftspflicht.....                     | 40 |
| 11.     | Abrechnung .....                              | 40 |
| 11.1.   | Beschreibung des Verarbeitungsvorgangs .....  | 40 |
| 11.2.   | Art der personenbezogenen Daten .....         | 40 |
| 11.3.   | Kategorien betroffener Personen .....         | 41 |
| 11.4.   | Empfänger der Daten.....                      | 41 |
| 11.5.   | Regelfristen für die Löschung der Daten ..... | 41 |
| 11.6.   | Datenübermittlung in Drittländer .....        | 41 |
| 11.7.   | Einhaltung der Datenschutzgrundsätze .....    | 41 |
| 11.7.1. | Rechtmäßigkeit der Verarbeitung.....          | 41 |
| a)      | Perspektive des Kunden .....                  | 41 |
| b)      | Perspektive LDA .....                         | 41 |
| 11.7.2. | Transparenz .....                             | 42 |
| 11.7.3. | Zweckbindung.....                             | 42 |
| 11.7.4. | Datenminimierung .....                        | 42 |
| 11.7.5. | Richtigkeit.....                              | 42 |
| 11.7.6. | Integrität und Vertraulichkeit.....           | 42 |
| 11.7.7. | Rechenschaftspflicht.....                     | 42 |
| 12.     | Support.....                                  | 42 |
| 12.1.   | Beschreibung der Verarbeitung.....            | 42 |
| 12.2.   | Art der personenbezogenen Daten .....         | 43 |
| 12.3.   | Kategorien betroffener Personen .....         | 43 |
| 12.4.   | Empfänger der Daten.....                      | 43 |
| 12.5.   | Regelfristen für die Löschung der Daten ..... | 43 |
| 12.6.   | Datenübermittlung in Drittländer .....        | 43 |
| 12.7.   | Einhaltung der Datenschutzgrundsätze .....    | 44 |
| 12.7.1. | Rechtmäßigkeit der Verarbeitung.....          | 44 |
| a)      | Perspektive des Kunde .....                   | 44 |
| b)      | Perspektive LDA .....                         | 44 |
| 12.7.2. | Transparenz .....                             | 44 |
| 12.7.3. | Zweckbindung.....                             | 44 |

|         |                                                               |    |
|---------|---------------------------------------------------------------|----|
| 12.7.4. | Datenminimierung .....                                        | 44 |
| 12.7.5. | Richtigkeit.....                                              | 44 |
| 12.7.6. | Integrität und Vertraulichkeit.....                           | 44 |
| 12.7.7. | Rechenschaftspflicht.....                                     | 44 |
| II.     | Rechte der betroffenen Personen .....                         | 45 |
| 1.      | Recht auf Auskunft (Art. 15 DSGVO).....                       | 45 |
| 2.      | Recht auf Berichtigung (Art. 16 DSGVO).....                   | 45 |
| 3.      | Recht auf Löschung (Art. 17 DSGVO) .....                      | 46 |
| 4.      | Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)..... | 46 |
| 5.      | Recht auf Datenübertragbarkeit (Art. 20 DSGVO) .....          | 47 |
| 6.      | Recht auf Widerspruch (Art. 21 DSGVO) .....                   | 47 |
| III.    | Technische und organisatorische Maßnahmen .....               | 48 |
| 1.      | Zutrittskontrolle (physische Sicherheit) .....                | 48 |
| 2.      | Zugangskontrolle (Systemzugang).....                          | 48 |
| 3.      | Zugriffskontrolle (Berechtigungskonzept) .....                | 48 |
| 4.      | Authentifizierung und Autorisierung von API-Zugriffen.....    | 48 |
| 5.      | Verschlüsselung.....                                          | 49 |
| 6.      | Pseudonymisierung und Datenminimierung .....                  | 49 |
| 7.      | Weitergabekontrolle .....                                     | 49 |
| 8.      | Eingabekontrolle / Protokollierung .....                      | 49 |
| 9.      | Verfügbarkeitskontrolle .....                                 | 49 |
| 10.     | Integritätskontrolle .....                                    | 49 |
| 11.     | Datentrennung .....                                           | 50 |
| 12.     | Lösch- und Aufbewahrungskonzept .....                         | 50 |
| 13.     | Vertraulichkeit und Verpflichtung der Mitarbeiter .....       | 50 |
| 14.     | Sicherheit bei mobiler Arbeit / Telearbeit.....               | 50 |
| 15.     | Incident-Response-Management.....                             | 50 |
| 16.     | Datenschutzmanagement und Compliance .....                    | 50 |
| IV.     | Verletzungen des Schutzes personenbezogener Daten .....       | 51 |
| V.      | Datenschutz-Folgenabschätzung.....                            | 51 |
| VI.     | Berufsgeheimnis und § 203 StGB .....                          | 51 |

## Definitionen

Für die Zwecke dieses Datenschutzkonzepts gelten die nachfolgenden Begriffsbestimmungen:

„**Anonymisierung**“ ist die Veränderung personenbezogener Daten derart, dass ein Personenbezug nicht oder nur mit einem unverhältnismäßigen Aufwand wiederhergestellt werden kann; anonymisierte Daten unterliegen nicht der DSGVO (ErwGr. 26 DSGVO).

„**Antwort (Ausgabe)**“ ist die auf eine Eingabe hin von der Anwendung mittels KI generierte Ausgabe.

„**API**“ (Application Programming Interface – API) ist die Programmierschnittstelle, über die andere Systeme auf die Funktionen der Anwendung zugreifen.

„**Auftragsverarbeiter**“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DSGVO).

„**Betroffene Person**“ ist eine durch Informationen identifizierte oder identifizierbare natürliche Person (Art. 4 Nr. 1 DSGVO).

„**Chunking**“ ist die Aufteilung längerer Texte in kleinere, inhaltlich zusammenhängende Segmente.

„**Drittapplikation**“ ist eine von einem Kunden oder Partner bereitgestellte Endanwendung, die über die API auf die Anwendung zugreift und von natürlichen Personen genutzt wird.

„**Einbettungen (Embeddings)**“ sind numerische Repräsentationen nicht-numerischer Daten, die von Large Language Models (LLMs) zur Erfassung semantischer Bedeutung verwendet werden. Sie ermöglichen es KI-Modellen, Beziehungen zwischen Konzepten zu identifizieren und die Bedeutung von Eingaben zu verstehen.

„**Eingabe (Prompt)**“ ist die Eingabe, die der Nutzer in der Anwendung vornimmt oder veranlasst, gleich in welcher Form (Frage, Anweisung, hochgeladenes Dokument).

„**Eingabedaten**“ im Sinne der KI-VO sind Daten, die in ein KI-System eingespeist oder von diesem direkt erfasst werden, auf deren Grundlage das System eine Ausgabe hervorbringt (Art. 3 Nr. 33 KI-VO).

„**Endkunde**“ ist die Organisation oder natürliche Person, die mit dem Kunden einen Nutzungsvertrag über die Nutzung der Anwendung geschlossen hat. Handelt es sich um eine Organisation, sind dies typischerweise Kanzleien, Steuerberatungsgesellschaften, Rechtsabteilungen oder sonstige Unternehmen. Setzt der Kunde das LDA-Tool unmittelbar für eigene Zwecke ein, fallen Kunde und Endkunde zusammen.

„**Identity Provider**“ ist der Dienst, der die Identitäten der Nutzer verwaltet, deren Authentifizierung durchführt und das Ergebnis gegenüber dem LDA-Tool bestätigt.

„**Inhalte**“ sind die im Legal Data Hub bereitgestellten Fachinformationen, gegebenenfalls in einer für die KI aufbereiteten Form.

„**Kunde**“ ist der Vertragspartner der LDA, der mit LDA einen Vertrag über die Bereitstellung der KI-gestützten Softwarelösung schließt. Der Kunde ist regelmäßig ein juristischer Fachverlag oder ein sonstiger Content-Anbieter (nachfolgend auch „**Verlag**“), der die LDA-Dienste zur Bereitstellung von KI-Funktionalitäten für seine eigenen Endkunden und deren Nutzer einsetzt. Kunde kann daneben auch eine Kanzlei, ein Unternehmen oder eine sonstige Organisation sein, die das LDA-Tool unmittelbar für eigene Zwecke einsetzt.

„**LDA**“ ist die LDA Legal Data Analytics GmbH, Hochwaldstraße 26, 81377 München, eingetragen im Handelsregister des Amtsgerichts München unter HRB 286277.

„**LDA-Dienste**“ sind sämtliche von LDA im Zusammenhang mit dem LDA-Tool erbrachten Leistungen, insbesondere dessen Bereitstellung, Betrieb, Wartung, Support und Weiterentwicklung.

„**LDA-Tool**“ ist die cloudbasierte Anwendung der LDA zur Informationssuche und -analyse, die Fachinformationen unter Einsatz künstlicher Intelligenz, insbesondere großer Sprachmodelle, erschließt.

„**Legal Data Hub**“ ist die für die Erschließung durch das LDA-Tool strukturierte Datenbank, in der die technisch aufbereiteten Fachinformationen bereitgestellt werden.

„**Meta-Prompt**“ ist die von LDA vorgegebene, dem Nutzer nicht sichtbare Anweisung an das Sprachmodell, die zusammen mit der Eingabe und den ermittelten Textstellen übergeben wird.

„**Nutzer**“ ist die natürliche Person, die die Anwendung tatsächlich bedient – unmittelbar über das LDA-Front-End oder mittelbar über eine Drittapplikation –, indem sie Eingaben tätigt, dadurch Verarbeitungsvorgänge auslöst und die generierten Ausgaben entgegennimmt. Der Nutzer ist entweder selbst Endkunde oder für den Endkunden tätig, insbesondere als Inhaber, Gesellschafter oder im Rahmen eines Dienst-, Arbeits- oder Ausbildungsverhältnisses.

„**Nutzungsdaten**“ sind Daten über Umfang und Art der Nutzung der Anwendung, insbesondere zu Abrechnungszwecken.

„**Partner**“ ist ein Dritter, der die Anwendung über die API in eine eigene Endanwendung (Drittapplikation) einbindet und diese seinen eigenen Kunden zur Verfügung stellt.

„**Personenbezogene Daten**“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO).

„**Protokolldaten**“ sind automatisiert erzeugte Aufzeichnungen über Zugriffe auf die Anwendung und über Systemereignisse, insbesondere zu Zwecken der IT-Sicherheit, der Fehleranalyse und der Abrechnung.

„**Pseudonymisierung**“ ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen (Art. 4 Nr. 5 DSGVO).

„**Reranking**“ ist die nachgelagerte Neugewichtung von Suchergebnissen nach ihrer Relevanz für die konkrete Anfrage.

„**Retrieval-Augmented Generation (RAG)**“ bezeichnet eine Architektur, bei der einschlägige Textstellen zunächst aus einer Wissensdatenbank abgerufen (Retrieval) und anschließend zusammen mit der Eingabe an das Sprachmodell übergeben werden (Generation), anstatt allein auf im Modell angelegtes Wissen zurückzugreifen.

„**Sprachmodell (LLM)**“ ist ein KI-Modell, das natürliche Sprache verarbeiten und generieren kann.

„**Telemetriedaten**“ sind automatisiert erhobene Betriebs- und Leistungsdaten der Anwendung, insbesondere zu Verfügbarkeit, Antwortzeiten, Auslastung und Fehlern.

„**Textstellen (Fundstellen)**“ sind die Passagen aus den Inhalten des Legal Data Hub, die zur Generierung der Antwort verwendet oder über die Suchfunktion angezeigt werden.

„**Unterauftragsverarbeiter**“ ist ein weiterer Auftragsverarbeiter, den der Auftragsverarbeiter zur Ausführung bestimmter Verarbeitungstätigkeiten im Namen des Verantwortlichen heranzieht (Art. 28 Abs. 2 und 4 DSGVO).

„**Vektorisierung**“ bezeichnet den technischen Prozess der Umwandlung von Daten in numerische Vektoren. Dabei werden beliebige Datenformate – wie Text, Bilder oder andere nicht-numerische Informationen – in eine strukturierte Repräsentation überführt, die aus geordneten Zahlenfolgen besteht.

„**Verantwortlicher**“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO).

„**Verarbeitung**“ ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten (Art. 4 Nr. 2 DSGVO).

#### **Hinweis zur Gleichstellung:**

Soweit in dieser Stellungnahme personenbezogene Bezeichnungen im generischen Maskulinum verwendet werden, erfolgt dies ausschließlich aus Gründen der besseren Lesbarkeit und sprachlichen Vereinfachung. Die verwendeten Personenbezeichnungen beziehen sich gleichermaßen auf Personen jeden Geschlechts, sofern sich aus dem jeweiligen Kontext nichts Abweichendes ergibt.

## **A. Allgemeiner Teil**

### **I. Zweck und Hintergrund des Datenschutzkonzepts**

Dieses Datenschutzkonzept soll den Kunden und Nutzern der Legal Data Analytics GmbH („LDA“) einen strukturierten Überblick über die Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung und Nutzung des **LDA-Tools**. Es unterstützt den Kunden bei der Erfüllung ihrer Rechenschafts-, Informations- und Kontrollpflichten. Die Prüfung der datenschutzrechtlichen Zulässigkeit des jeweiligen konkreten Einsatzes obliegt dem Kunden.

Die LDA stellt sicher, dass die Datenerhebung und der Umgang mit den im Zusammenhang mit der Nutzung des LDA-Tools erhobenen Daten in Übereinstimmung mit diesem Datenschutzkonzept erfolgen.

Das Datenschutzkonzept beschreibt den technischen und organisatorischen Stand zum Zeitpunkt des Bearbeitungsstandes. Es ist bei wesentlichen Änderungen des Systems, insbesondere bei Änderungen der eingesetzten Unterauftragsverarbeiter, der Speicherorte, der Speicher- und Löschfristen unverzüglich fortzuschreiben.

### **II. Aufbau und Funktionsweise des Datenschutzkonzepts**

Der allgemeine Teil dieses Datenschutzkonzepts beschreibt das LDA-Tool, seine technische Infrastruktur sowie die datenschutzrechtlichen Rollen der an der Verarbeitung beteiligten Stellen.

Im Rahmen des besonderen Teils des Datenschutzkonzepts wird zunächst der Ablauf der Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung und Nutzung des LDA-Tools beschrieben. Sodann wird im Rahmen des besonderen Teils für jeden einzelnen Verarbeitungsvorgang beschrieben (1) welche personenbezogenen Daten im Zusammenhang mit der Nutzung und Bereitstellung des LDA-Tools verarbeitet werden, (2) von welchen Kategorien betroffener Personen personenbezogene Daten verarbeitet werden, (3) ob, und wenn ja an wen eine Weiterleitung personenbezogener Daten erfolgt, (4) wann und wie eine Löschung der verarbeiteten personenbezogenen Daten vorgenommen wird, (5) ob eine Datenübermittlung in Drittländer stattfindet, (6) wie eine Einhaltung der Datenschutzgrundsätze gewährleistet wird.

### **III. Beschreibung des LDA-Tools**

Die LDA betreibt eine KI-gestützte Softwarelösung für juristische Fachverlage und Content-Anbieter zur effizienten Erschließung von Inhalten. Das System ermöglicht die Eingabe von Anfragen über verschiedene Zugangsmöglichkeiten, insbesondere über eine ChatBook-Oberfläche sowie über eine API-Schnittstelle zur Integration in Drittsysteme, die durch den Kunden eingesetzt werden. Die Eingabe kann durch Softwareapplikationen des Kunden oder durch Endnutzer über das LDA-Front-End erfolgen. Nach erfolgter Eingabe wird diese an das LDA-Back-End weitergeleitet.

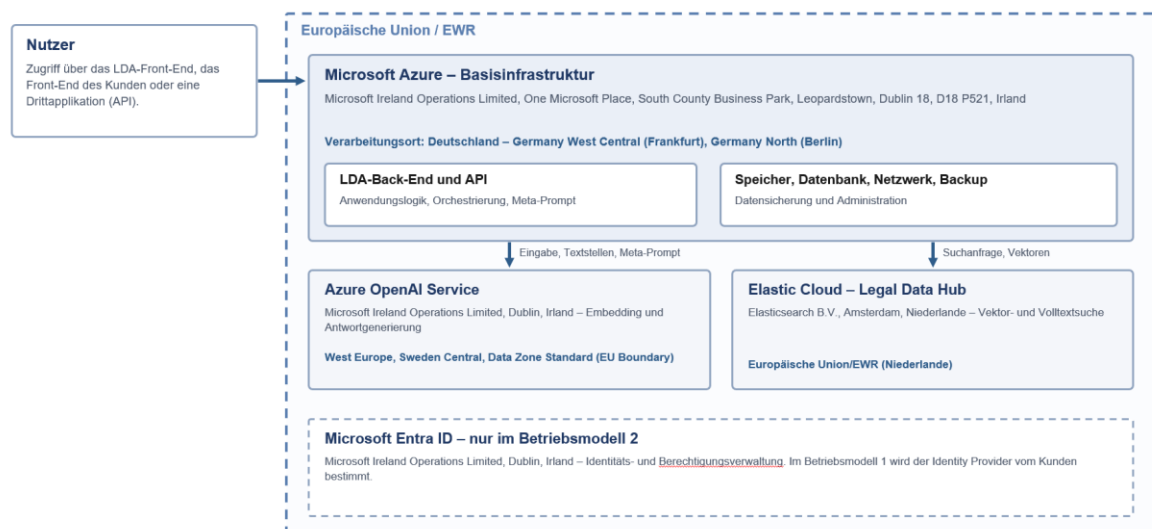
Das System folgt dem Prinzip der Retrieval-Augmented Generation (RAG)-Architektur, bei dem die KI zunächst relevante Informationen aus einer externen Wissensdatenbank abrufen (Retrieval) und anschließend auf Basis dieser abgerufenen Fundstellen eine kontextbezogene und fundierte Antwort generiert (Generation), anstatt allein auf ihr intern trainiertes Wissen zurückzugreifen. LDA setzt keine eigenentwickelte KI-Lösung im Sinne eines eigenen Sprachmodells ein, sondern nutzt bestehende Modelle (u. a. OpenAI) sowie Elastic Search als Komponenten. Die proprietäre Eigenleistung von LDA liegt in der Orchestrierung dieser Komponenten im RAG-Prozess (z. B. Prompt-Engineering, Steuerung der Such- und Antwortlogik).

Nach erfolgter Authentifizierung und Autorisierung des Nutzers wird die Eingabe durch Microsoft Azure OpenAI vektorisiert, also in numerische Repräsentationen umgewandelt. Hierbei werden die von Nutzern eingegebenen Prompts durch Microsoft Azure OpenAI mittels spezieller Embedding-Modelle (z. B. text-embedding-3-small/-large) in Vektoren umgewandelt. Parallel hierzu kann eine Volltextsuche auf Basis der Eingabe in einer Elastic Cloud Datenbank durchgeführt werden. Die Vektorisierung dient als Grundlage für eine Vektorsuche, nach der passende Fundstellen in der Elastic Cloud Datenbank ermittelt werden. Auf Basis der Eingabe und der ermittelten Fundstellen generiert das System eine Antwort (Output).

Das System verfügt über die Fähigkeit zur Quellentransparenz, indem es dem Nutzer die konkrete Textgrundlage offenlegt, auf der eine Antwort basiert, und eine direkte Verlinkung zu den Fundstellen ermöglicht. Die Datenbankstruktur umfasst verschiedene Datenkategorien, darunter Nutzereingaben/Prompts (ggf. mit personenbezogenen Daten), Nutzungsdaten (vor allem zu Abrechnungszwecken), Telemetriedaten sowie System-/Log- und ggf. Cache-Dateien.

Die Authentifizierung kann je nach Konfiguration über einen Identity Provider des Kunden (**Modell 1**) oder über einen LDA Identity Provider bei Microsoft Entra (**Modell 2**) erfolgen.

#### IV. Technische Infrastruktur



Das LDA-Tool und die zugehörigen Datenbestände werden auf der Infrastruktur der Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland betrieben. Die Rechenzentrumsstandorte liegen in Deutschland – Germany West Central (Frankfurt) und Germany North (Berlin). Hiervon zu unterscheiden sind die für die nachfolgend genannten Einzeldienste konfigurierten Verarbeitungsregionen, die von den Standorten der Basisinfrastruktur abweichen können. Die Verarbeitung erfolgt in allen Fällen innerhalb der Europäischen Union beziehungsweise des Europäischen Wirtschaftsraums.

Für die Vektorisierung von Eingaben und Inhalten sowie für die Generierung der Antworten nutzt LDA den Azure OpenAI Service der Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland. Übermittelt werden die Eingabe des Nutzers, die aus dem Legal Data Hub ermittelten Textstellen sowie der von LDA vorgegebene Meta-Prompt. Zurückübertragen werden die Einbettungen beziehungsweise die generierte Antwort. Als geografische Verarbeitungsregion ist West Europe, Sweden Central und Data Zone Standard (EU Boundary) konfiguriert; die Verarbeitung erfolgt damit innerhalb der EU-Datengrenze von Microsoft.

Für den Dienst ist die Speicherung von Eingaben und Ausgaben deaktiviert („Zero Data Retention“ / Opt-Out des Abuse Monitoring), das heißt Microsoft speichert die übermittelten Inhalte nach

Abschluss der Anfrage nicht dauerhaft. Eine Verwendung der übermittelten Inhalte zum Training oder zur Feinabstimmung der Modelle findet nicht statt.

Für die Speicherung der aufbereiteten Fachinhalte und die Durchführung der Vektor- und Volltextsuche nutzt LDA die Elastic Cloud der Elasticsearch B.V., Keizersgracht 281, 1016 ED Amsterdam, Niederlande. Gespeichert werden die Textsegmente, deren Vektorrepräsentationen, Strukturmetadaten und Quellangaben. Übermittelt werden die Suchanfrage beziehungsweise deren Vektorrepräsentation. Zurückübertragen werden die ermittelten Textstellen. Als Verarbeitungsregion ist Europäische Union/EWR (Niederlande) konfiguriert.

Sofern die Authentifizierung nach dem Modell 2 über einen von LDA bereitgestellten Identity Provider erfolgt, nutzt LDA hierfür Microsoft Entra ID der Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland. Verarbeitet werden Identitäts-, Authentifizierungs- und Berechtigungsdaten der Nutzer. Der geografische Verarbeitungsort wird über die im Microsoft Entra Admin Center hinterlegte Standortauswahl bestimmt; hinterlegt ist Deutschland (Germany). Im Modell 1 wird dieser Dienst nicht in Anspruch genommen; der Identity Provider wird in diesem Fall vom Kunden bestimmt.

## **V. Rollen**

### **1. Rolle des Kunden**

Kunde im Sinne dieses Datenschutzkonzepts ist der Vertragspartner der LDA, der mit LDA einen Vertrag über die Bereitstellung und Nutzung des LDA-Tools schließt. Dies ist regelmäßig ein juristischer Fachverlag oder ein sonstiger Content-Anbieter, der das LDA-Tool seinen Endkunden – etwa Kanzleien, Steuerberatungsgesellschaften oder Rechtsabteilungen – zur Verfügung stellt. Kunde kann daneben auch eine Organisation sein, die das LDA-Tool unmittelbar für eigene Zwecke einsetzt; in diesem Fall fallen Kunde und Endkunde zusammen.

Der Kunde entscheidet über den Einsatz des LDA-Tools, über die im Legal Data Hub bereitgestellten Inhalte, über den Kreis der zugriffsberechtigten Nutzer sowie über die wesentlichen Konfigurationsparameter, insbesondere über die Speicher- und Löschfristen und über das Authentifizierungsmodell. Er ist damit für die im Rahmen der Bereitstellung und Nutzung des LDA-Tools erfolgende Verarbeitung personenbezogener Daten Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO.

### **2. Rolle der LDA**

Soweit LDA bei der Einrichtung, dem Betrieb, der Wartung oder der Bereitstellung des LDA-Tools auf personenbezogene Daten des Kunden oder seiner Nutzer zugreifen kann, wird LDA als Auftragsverarbeiter im Sinne von Art. 28 DSGVO tätig. LDA ist insoweit insbesondere nicht gemeinsam mit dem Kunden für die Verarbeitung von personenbezogenen Daten im Sinne von Art. 26 Abs. 1 DSGVO verantwortlich. Dies deshalb, da

- LDA keine Entscheidungsbefugnis hinsichtlich des Zwecks der Verarbeitung personenbezogener Daten besitzt;
- der Kunde die Hoheit über die Verwendung der Daten einschließlich deren Löschung oder Vernichtung innehat;
- LDA sich auf der Grundlage des zwischen dem Kunden und der LDA geschlossenen Auftragsverarbeitungsvertrages den Weisungen des Kunden unterwirft.

Dass LDA die technische Ausgestaltung vorschlägt und der Kunde sich diesem Vorschlag anschließt, steht der Verantwortlichkeit des Kunden nicht entgegen.

Soweit LDA im Rahmen der Qualitätssicherung und Produktverbesserung über die Erfüllung der vertraglichen Leistungspflichten hinaus eigene Zwecke verfolgt, gelten die Ausführungen im Besonderen Teil unter „Qualitätssicherung/Produktverbesserung“.

### **3. Beziehung zu den Nutzern**

Die im Rahmen der Nutzung des LDA-Tools zustande kommenden Verträge zwischen dem Kunden und seinen Endkunden kommen ausschließlich zwischen diesen zustande. LDA wird nicht Vertragspartei der Verträge zwischen Kunden und Endkunden.

Nutzer im Sinne dieses Datenschutzkonzepts ist stets die natürliche Person, die das LDA-Tool tatsächlich bedient. Hinsichtlich der personenbezogenen Daten, die der Nutzer als Inhalt seiner Eingabe in das LDA-Tool einbringt – etwa Daten von Mandanten, Vertragspartnern oder Verfahrensgegnern –, entscheidet weder der Kunde noch LDA über den Zweck der Verarbeitung. Welche Inhalte tatsächlich eingegeben werden, bestimmt allein der Endkunde, für den der Nutzer tätig ist oder in dessen Sphäre der Nutzer tätig wird. Der Endkunde entscheidet allein und eigenverantwortlich, ob das LDA-Tool in der Mandats- oder Aufgabenbearbeitung eingesetzt wird, für welche Vorgänge dies zulässig ist und welche Unterlagen dabei verwendet werden dürfen. Er ist insoweit eigener Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO, hat eine eigene Rechtsgrundlage vorzuhalten und seine Informationspflichten nach Art. 13 und 14 DSGVO zu erfüllen.

Hinsichtlich der Eingabeinhalte wird der Kunde als Auftragsverarbeiter des Endkunden tätig; LDA ist insoweit Unterauftragsverarbeiter (Art. 28 Abs. 4 DSGVO) des Kunden. Der Kunde hat mit seinen Endkunden einen entsprechenden Auftragsverarbeitungsvertrag zu schließen und die Einbindung der LDA sowie der von LDA eingesetzten Unterauftragsverarbeiter darin abzubilden.

Setzt der Kunde das LDA-Tool unmittelbar für eigene Zwecke ein, ist LDA unmittelbar Auftragsverarbeiterin des Kunden.

Die Nutzer können personenbezogene Daten in das LDA-Tool eingeben, deren Verarbeitung weder erforderlich noch vom Kunden oder Endkunden vorgesehen ist (sogenannte aufgedrängte Daten). Weder der Kunde noch LDA können solche Eingaben technisch verhindern, da eine inhaltliche Filterung der Eingabe die Funktionsfähigkeit einzelner Anwendungsfälle beeinträchtigen würde. Die datenschutzrechtliche Verantwortung für die Eingabeinhalte trifft daher den Endkunden als Verantwortlichen. Der Kunde hat seine Endkunden vertraglich zu verpflichten, ihre Nutzer entsprechend anzuweisen.

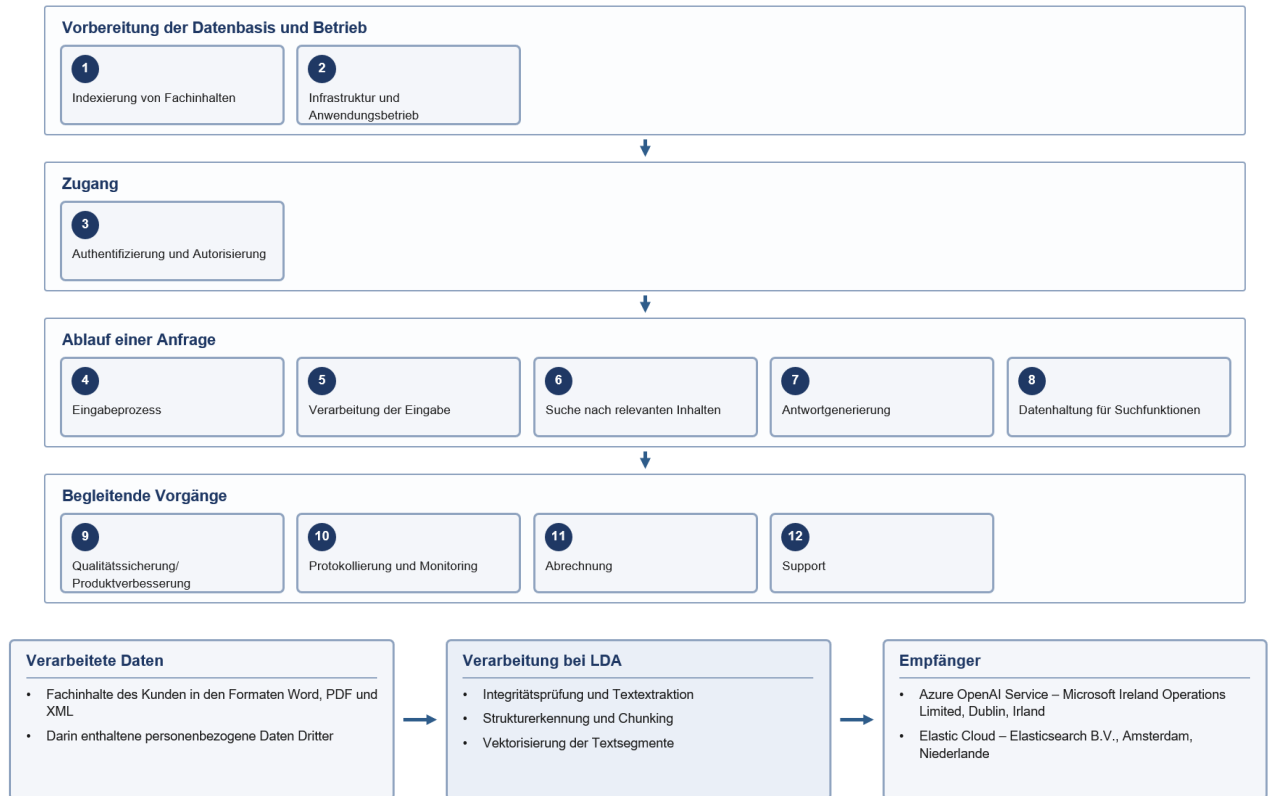
### **4. Rolle von Partnern mit eigener Drittapplikation**

Bindet ein Partner das LDA-Tool über die API in eine eigene Endanwendung ein, entscheidet er eigenständig über Ausgestaltung und Datenverarbeitung innerhalb seiner Anwendung. LDA hat auf die Verarbeitung innerhalb der Drittapplikation keinen Einfluss. Der Partner ist insoweit eigener Verantwortlicher. Für die Verarbeitung innerhalb des LDA-Tools bleibt es bei der vorstehend beschriebenen Rollenverteilung.

## B. Besonderer Teil

### I. Verarbeitungsvorgänge bei der Nutzung des LDA-Tools

Die nachfolgende Übersicht ordnet die einzelnen Verarbeitungsvorgänge in den Ablauf der Nutzung ein. Die Nummerierung entspricht der Gliederung dieses Abschnitts.



#### 1. Indexierung von Verlags- bzw. Kundenfachinhalten (Vorbereitung der Datenbasis)

##### 1.1. Beschreibung des Verarbeitungsvorgangs

Zur Vorbereitung der Datenbasis werden Verlagspublikationen bzw. Fachinhalten in verschiedenen Formaten (Word, PDF, XML) entgegengenommen und technisch analysiert. Im Rahmen der technischen Analyse werden die Dateien auf Integrität und Verwendbarkeit überprüft. Anschließend erfolgt die Textextraktion sowie eine Strukturerkennung der Dokumentinhalte. Die Strukturerkennung identifiziert Überschriften, Absätze, Fußnoten, Randnummern sowie juristische Elemente wie Gesetzeszitate und Fundstellen. Die Strukturinformationen werden gespeichert und ermöglichen die Kontextualisierung bei der späteren Suche. Die Dokumenttexte werden sodann durch Chunking in kleinere, inhaltlich zusammenhängende Segmente aufgeteilt, wobei die Segmentgrenzen unter Wahrung der inhaltlichen Integrität an Absätze, Überschriften oder Randnummern angepasst werden.

Abschließend werden die aufbereiteten Texte über den Azure OpenAI Service mit Embedding-Modellen (text-embedding-3-small bzw. -large) vektorisiert. Die Vektoren werden zusammen mit den ursprünglichen Textsegmenten, Strukturmetadaten und Quellangaben in den Legal Data Hub integriert, einer auf Elastic Cloud basierenden Datenbank, die sowohl Vektorsuche als auch Volltextsuche ermöglicht.

## 1.2. Art der personenbezogenen Daten

Die indexierten Fachinhalte enthalten regelmäßig keine personenbezogenen Daten der Nutzer. Sie können jedoch personenbezogene Daten Dritter enthalten, soweit die Fachinformationen solche wiedergeben, etwa

- Angaben zu Verfahrensbeteiligten in veröffentlichten Gerichtsentscheidungen, soweit diese nicht (hinreichend) anonymisiert wurden,
- Namen von Autoren, Herausgebern und Bearbeitern der Fachinhalte sowie
- Namen von sonstigen in den Fachbeiträgen genannte Personen

## 1.3. Kategorien betroffener Personen

Im Zusammenhang mit der Indexierung von Verlags- bzw. Kundenfachinhalten können personenbezogene Daten von folgenden Kategorien betroffener Personen verarbeitet werden:

- Verfahrensbeteiligte aus veröffentlichten Entscheidungen
- Autoren, Herausgeber und Bearbeiter von Fachinhalten
- Sonstige in den Fachinhalten genannte natürliche Personen

## 1.4. Empfänger der Daten

Die Fachinhalte werden zur Vektorisierung an die **Microsoft Ireland Operations Limited**, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland (Azure OpenAI Service) und zur Speicherung an die **Elasticsearch B.V.**, Keizersgracht 281, 1016 ED Amsterdam, Niederlande (Elastic Cloud) übermittelt. Beide Empfänger sind Unterauftragsverarbeiter der LDA. Eine Weitergabe an weitere Dritte findet nicht statt.

## 1.5. Regelfristen für die Löschung der Daten

Die indexierten Inhalte werden für die Dauer des Vertragsverhältnisses mit dem Kunden vorgehalten. Nimmt der Kunde Inhalte aus dem Legal Data Hub heraus, werden die zugehörigen Textsegmente, Metadaten und Vektoren gelöscht. Nach Beendigung des Vertragsverhältnisses erfolgt die Löschung oder Rückgabe nach Wahl des Kunden gemäß Art. 28 Abs. 3 lit. g DSGVO innerhalb von 60 Kalendertagen nach Vertragsende; LDA bescheinigt dem Kunden die Löschung. Die Frist trägt dem Umstand Rechnung, dass der Kunde vor der Löschung Gelegenheit haben muss, die Rückgabe der Daten zu verlangen.

## 1.6. Übermittlung der Daten in Drittländer

Eine Übermittlung in ein Drittland findet nicht statt.

Der Azure OpenAI Service ist auf die Verarbeitungsregionen West Europe, Sweden Central und Data Zone Standard (EU Boundary) konfiguriert; die Elastic Cloud wird in der Region Europäische Union/EWR (Niederlande) betrieben. Die Verarbeitung erfolgt damit ausschließlich innerhalb der Europäischen Union beziehungsweise des Europäischen Wirtschaftsraums.

## **1.7. Einhaltung der Datenschutzgrundsätze**

### **1.7.1. Rechtmäßigkeit der Verarbeitung**

#### **a) Perspektive des Kunden**

Für die in den Fachinhalten enthaltenen personenbezogenen Daten Dritter kann die Verarbeitung in der Regel auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden. Das berechtigte Interesse des Kunden liegt in der Erschließung und Verwertung der von ihm verlegten oder lizenzierten Fachinhalte sowie in deren Bereitstellung für die juristische Recherche. Die Abwägung fällt regelmäßig zugunsten des Kunden aus, da es sich um bereits veröffentlichte Inhalte handelt, die Verarbeitung den mit der Veröffentlichung verfolgten Zweck fortführt und die Inhalte gegenüber der Veröffentlichung nicht angereichert werden.

Enthalten die Fachinhalte besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO – etwa Gesundheitsdaten in veröffentlichten Entscheidungen –, ist zusätzlich ein Erlaubnistatbestand nach Art. 9 Abs. 2 DSGVO erforderlich. In Betracht kommen insbesondere Art. 9 Abs. 2 lit. e DSGVO, soweit die betroffene Person die Daten offensichtlich öffentlich gemacht hat, sowie Art. 9 Abs. 2 lit. f DSGVO. Der Kunde ist als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO dafür verantwortlich, dass eine geeignete Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Indexierung von Verlags- bzw. Kundenfachinhalten vorliegt.

#### **b) Perspektive von LDA**

LDA ist bei der Indexierung als Auftragsverarbeiter im Sinne von Art. 28 DSGVO tätig, da sie die Daten ausschließlich zur Erfüllung der vertraglichen Pflichten des Kunden verarbeitet und keine eigenen Zwecke verfolgt. Als Auftragsverarbeiter benötigt LDA für diese Verarbeitungstätigkeit keine eigene Rechtsgrundlage. Die Rechtmäßigkeit der Datenverarbeitung leitet sich aus der Rechtsgrundlage des Kunden als Verantwortlichem ab.

### **1.7.2. Transparenz**

Soweit die Inhalte personenbezogene Daten Dritter enthalten, obliegt die Erfüllung der Informationspflichten nach Art. 14 DSGVO dem Kunden; für veröffentlichte Entscheidungen kommt regelmäßig die Ausnahme des Art. 14 Abs. 5 DSGVO in Betracht.

### **1.7.3. Zweckbindung**

Die LDA verarbeitet die Fachinhalte ausschließlich zum Zweck der Erschließung durch das LDA-Tool. Eine Nutzung zu anderen Zwecken, insbesondere zum Training oder zur Feinabstimmung von KI-Modellen, findet nicht statt.

### **1.7.4. Datenminimierung**

Verarbeitet werden ausschließlich die vom Kunden übergebenen Fachinhalte. Eine darüber hinausgehende Erhebung findet nicht statt. Der Kunde entscheidet, welche Inhalte er bereitstellt, und kann die Bereitstellung jederzeit einschränken.

### **1.7.5. Richtigkeit**

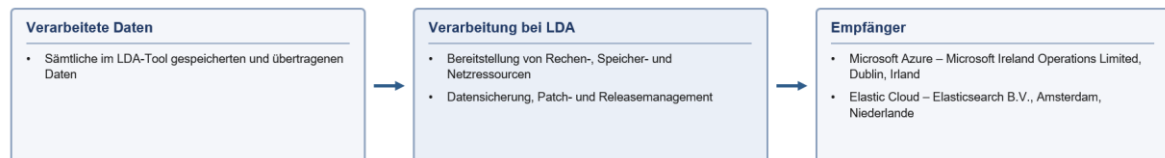
Die inhaltliche Richtigkeit der Fachinhalte liegt in der Verantwortung des Kunden. Das LDA-Tool gibt die Inhalte unverändert wieder und verlinkt auf die Originalfundstelle, sodass Abweichungen erkennbar sind.

### 1.7.6. Integrität und Vertraulichkeit

Die Inhalte werden verschlüsselt übertragen und gespeichert. Die Datenbestände sind mandantenbezogen getrennt. Der Zugriff innerhalb der LDA ist auf die für die Indexierung zuständigen Mitarbeiter beschränkt. Einzelheiten ergeben sich aus dem Abschnitt „Technische und organisatorische Maßnahmen“.

### 1.7.7. Rechenschaftspflicht

Die Rechenschaftspflicht kann durch den Kunden anhand der Angaben in diesem Datenschutzkonzept erfüllt werden.



## 2. Infrastruktur und Anwendungsbetrieb

### 2.1. Beschreibung des Verarbeitungsvorgangs

LDA betreibt das LDA-Tool auf der im Allgemeinen Teil unter „Technische Infrastruktur“ (A. IV.) beschriebenen Cloud-Infrastruktur. Der Verarbeitungsvorgang umfasst die Bereitstellung von Rechen-, Speicher- und Netzwerkressourcen, den Betrieb der Anwendungs- und Datenbankdienste, das Netzwerk- und Zugriffsmanagement, die Datensicherung (Backup) sowie das Patch-, Release- und Konfigurationsmanagement.

Personenbezogene Daten werden im Rahmen dieses Verarbeitungsvorgangs nicht zu eigenen inhaltlichen Zwecken ausgewertet. Die Verarbeitung ist akzessorisch. Sie besteht in der Speicherung ruhender Daten, in deren Übertragung zwischen den Systemkomponenten sowie in einem anlassbezogenen administrativen Zugriff im Rahmen von Wartung, Störungsbeseitigung und Datensicherung.

### 2.2. Art der personenbezogenen Daten

Von der Verarbeitung betroffen sind sämtliche im LDA-Tool gespeicherten oder übertragenen personenbezogenen Daten, insbesondere:

- Identitäts-, Authentifizierungs- und Berechtigungsdaten der Nutzer
- Eingaben und generierte Antworten sowie die hieraus erzeugten Einbettungen
- indexierte Fachinhalte einschließlich der darin enthaltenen Daten Dritter
- Protokoll-, Telemetrie- und Nutzungsdaten
- Administrationsdaten (Kennung des administrativen Zugriffs, Zeitpunkt, ausgeführte Aktion)

### 2.3. Kategorien betroffener Personen

Im Zusammenhang mit dem Anwendungsbetrieb können personenbezogene Daten von folgenden Kategorien betroffener Personen verarbeitet werden:

- Nutzer
- Beschäftigte und Ansprechpartner des Kunden und der Endkunden
- Administratoren der LDA und der eingesetzten Unterauftragsverarbeiter
- sonstige Dritte, deren Daten in Eingaben oder Fachinhalten enthalten sind

### 2.4. Empfänger der Daten

Empfänger ist die **Microsoft Ireland Operations Limited**, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland als Betreiberin der Cloud-Infrastruktur (Microsoft Azure) sowie – für die Suchdatenhaltung – die **Elasticsearch B.V.**, Keizersgracht 281, 1016 ED Amsterdam, Niederlande (Elastic Cloud). Beide sind Unterauftragsverarbeiter der LDA.

### 2.5. Regelfristen für die Löschung der Daten

Für die einzelnen Datenkategorien gelten die Fristen des jeweiligen Verarbeitungsvorgangs. Datensicherungen werden rollierend für 35 Kalendertage vorgehalten und anschließend überschrieben; dies entspricht einer täglichen Sicherung mit 30-tägiger Vorhaltung zuzüglich der Wochensicherungen. Löschungen im Produktivsystem schlagen mit dem Ablauf des Sicherungszyklus, also spätestens nach 35 Kalendertagen, auf die Datensicherungen durch; bis dahin sind die Daten in den Sicherungen gegen einen Zugriff im Regelbetrieb geschützt. Protokolle administrativer Zugriffe werden nach 90 Kalendertagen gelöscht.

### 2.6. Datenübermittlung in Drittländer

Eine Übermittlung in ein Drittland findet nicht statt. Die Basisinfrastruktur wird ausschließlich an den Standorten Deutschland – Germany West Central (Frankfurt) und Germany North (Berlin) betrieben.

Soweit im Rahmen von Wartung oder Störungsbeseitigung ausnahmsweise ein Zugriff von Personal der Empfänger aus einem Drittland in Betracht kommt, stellen LDA und der Unterauftragsverarbeiter die Einhaltung des Kapitels V DSGVO durch die von der Kommission nach Art. 46 Abs. 2 DSGVO erlassenen Standardvertragsklauseln sicher.

### 2.7. Einhaltung der Datenschutzgrundsätze

#### 2.7.1. Rechtmäßigkeit der Verarbeitung

##### a) Perspektive des Kunden

Der Betrieb der Anwendung ist zur Erfüllung des zwischen dem Kunden und seinen Endkunden geschlossenen Nutzungsvertrages erforderlich; Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO.

##### b) Perspektive LDA

LDA wird insoweit als Auftragsverarbeiterin im Sinne von Art. 28 DSGVO tätig und benötigt für diese Verarbeitungstätigkeit keine eigene Rechtsgrundlage. Die Rechtmäßigkeit der Verarbeitung leitet sich aus der Rechtsgrundlage des Kunden als Verantwortlichem ab.

### 2.7.2. Transparenz

Die Nutzer werden über die Datenschutzerklärung des Kunden über den Betrieb der Anwendung und die eingesetzten Dienstleister informiert. LDA stellt dem Kunden hierfür die erforderlichen Angaben zur Verfügung.

### 2.7.3. Zweckbindung

Die im Rahmen des Betriebs zugänglichen Daten werden ausschließlich zur Bereitstellung und Aufrechterhaltung der LDA-Dienste verarbeitet. Eine inhaltliche Auswertung oder eine Nutzung zum Training von KI-Modellen findet nicht statt.

### 2.7.4. Datenminimierung

Administrative Zugriffe auf produktive Datenbestände erfolgen nur anlassbezogen, nach dem Grundsatz der geringsten Rechte und werden protokolliert.

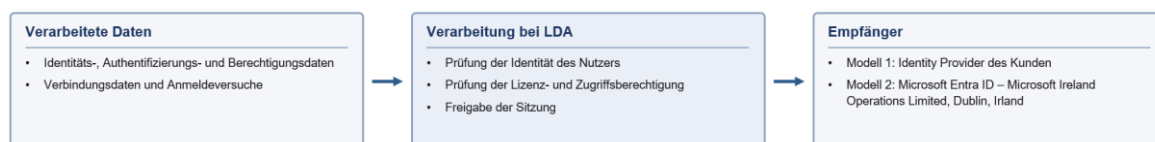
### 2.7.5. Richtigkeit

Der Betrieb verändert die verarbeiteten Inhalte nicht. Die Richtigkeit der Daten richtet sich nach dem jeweiligen Verarbeitungsvorgang.

### 2.7.6. Rechenschaftspflicht

Die Rechenschaftspflicht kann durch den Kunden anhand der Angaben in diesem Datenschutzkonzept erfüllt werden

## 3. Authentifizierung und Autorisierung



### 3.1. Beschreibung der Verarbeitungstätigkeit

Die Überprüfung der Authentifizierung und Autorisierung der Nutzer erfolgt als zentraler Schritt vor dem Zugriff auf das LDA-Tool. Hierbei ist zwischen zwei Betriebsmodellen zu unterscheiden, die sich durch die Ausgestaltung der Authentifizierungs- und Autorisierungsinfrastruktur voneinander abgrenzen.

#### 3.1.1. Modell 1 – Identity Provider des Kunden

Bei Modell 1 erfolgt die Authentifizierung über einen Identity Provider des Kunden. In diesem Konfigurationsszenario stellt der Kunde die Authentifizierungsinfrastruktur bereit und kontrolliert die Identitätsverwaltung der Nutzer. Die Überprüfung der Nutzungsberechtigung erfolgt durch Informationsübertragung vom LDA-Back-End an den vom Verlag betriebenen oder beauftragten Identity Provider. Der Verlag legt die Zweckbestimmung fest und bestimmt, zu welchem Zweck personenbezogene Daten im Rahmen des Authentifizierungsprozesses verarbeitet werden.

#### 3.1.2. Modell 2 – Identity Provider der LDA

Bei Modell 2 erfolgt die Authentifizierung über einen von LDA bereitgestellten Identity Provider. In diesem Konfigurationsszenario stellt LDA die Authentifizierungsinfrastruktur bereit oder beauftragt

einen entsprechenden Dienstleister, insbesondere Microsoft Azure Directory bzw. Entra ID. LDA verwaltet in diesem Fall die Identitäten und Zugriffsrechte der Nutzer. Die Überprüfung erfolgt durch Informationsübertragung vom LDA-Back-End an den von LDA bestimmten Identity Provider.

Nach erfolgreicher Authentifizierung und Autorisierung wird die Eingabe des Nutzers an das LDA-Back-End weitergeleitet und der weitere Verarbeitungsvorgang eingeleitet.

### 3.2. Art der personenbezogenen Daten

Im Zusammenhang mit der Authentifizierung und Autorisierung werden die nachfolgenden personenbezogenen Daten verarbeitet:

- Name, Vorname
- Benutzerkennung
- E-Mail-Adresse
- Organisationszugehörigkeit
- Berechtigungsprofil, Modul- und Lizenzzuordnung
- Authentifizierungsstatus
- Zeitpunkt und Ergebnis der Authentifizierungsversuche
- Verbindungsdaten, insb. IP-Adresse

### 3.3. Kategorien betroffener Personen

Im Zusammenhang mit der Authentifizierung und Autorisierung können personenbezogene Daten von folgenden Kategorien betroffener Personen verarbeitet werden:

- Nutzer
- Beschäftigte des Kunden
- Administratoren

### 3.4. Empfänger der Daten

#### 3.4.1. Modell 1 – Identity Provider des Kunden

In Modell 1 werden die Daten an den vom Kunden betriebenen oder beauftragten Identity Provider übermittelt; der Kunde bestimmt diesen Empfänger selbst.

#### 3.4.2. Modell 2 – Identity Provider der LDA

In Modell 2 werden die Daten an die **Microsoft Ireland Operations Limited**, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland (Microsoft Entra ID) als Unterauftragsverarbeiter der LDA übermittelt.

### 3.5. Regelfristen für die Löschung der Daten

#### 3.5.1. Modell 1 – Identity Provider des Kunden

In Modell 1 obliegt die Festlegung der Löschfristen dem Kunden.

### 3.5.2. Modell 2 – Identity Provider der LDA

Die Identitäts- und Berechtigungsdaten werden für die Dauer der Zugriffsberechtigung vorgehalten. Wird die Berechtigung entzogen oder das Nutzerkonto gelöscht, erfolgt die Löschung innerhalb von 60 Kalendertagen. Die Frist berücksichtigt, dass eine versehentliche Deaktivierung innerhalb eines angemessenen Zeitraums rückgängig gemacht werden muss. Authentifizierungsprotokolle werden nach 90 Kalendertagen gelöscht.

### 3.6. Datenübermittlung in Drittländer

Bei **Modell 1** obliegt die Bewertung dem Kunden.

Bei **Modell 2** wird der geografische Verarbeitungsort über die im Microsoft Entra Admin Center hinterlegte Standortauswahl bestimmt. LDA hat als Standort Deutschland (Germany) konfiguriert; die Verarbeitung erfolgt innerhalb der EU-Datengrenze, sodass eine Übermittlung in ein Drittland nicht stattfindet.

### 3.7. Einhaltung der Datenschutzgrundsätze

#### 3.7.1. Rechtmäßigkeit der Verarbeitung

##### a) Perspektive des Kunden

Die Verarbeitung der Identitäts- und Berechtigungsdaten ist zur Erfüllung des zwischen dem Kunden und dem Endkunden geschlossenen Nutzungsvertrages erforderlich; Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO. Ohne Authentifizierung und Autorisierung kann der vertraglich geschuldete, lizenzabhängige Zugang zu den Inhalten nicht gewährt werden.

Soweit im Rahmen der Authentifizierung darüber hinaus Daten zur Erkennung und Abwehr von Missbrauch verarbeitet werden – insbesondere fehlgeschlagene Anmeldeversuche und Verbindungsdaten –, kann die Verarbeitung auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden. Das berechnete Interesse liegt in der Sicherheit der Systeme und im Schutz der lizenzierten Inhalte vor unbefugter Nutzung.

Ist der Nutzer Beschäftigter des Endkunden, hat der Endkunde für die von ihm zu verantwortende Verarbeitung eine eigene Rechtsgrundlage vorzuhalten; in Betracht kommen Art. 6 Abs. 1 lit. b DSGVO sowie Art. 88 DSGVO in Verbindung mit den nationalen Vorschriften zum Beschäftigtendatenschutz.

##### b) Perspektive LDA

Sowohl bei der Nutzung eines vom Kunden selbst ausgewählten Identity Providers (Modell 1) als auch bei der Nutzung eines von LDA bereitgestellten Identity Providers (Modell 2) bestimmt der Verlag bzw. Kunden den Zweck der Verarbeitung.

Der Zweck liegt in der Authentifizierung der Endnutzer zur Überprüfung deren Nutzungsberechtigung an den LDA-Diensten. Dieser Zweck wird vom Kunden vorgegeben und bildet den maßgeblichen Anknüpfungspunkt für die datenschutzrechtliche Rollenverteilung. Hinsichtlich der Mittel der Verarbeitung kann entweder der Verlag oder LDA die Auswahl des Identity Providers treffen und damit die technische und organisatorische Ausgestaltung festlegen. Entscheidend ist jedoch, dass die Entscheidung über die Mittel nachrangig zur Zweckbestimmung ist und die Wahl des technischen Mittels (Identity Provider) nicht zu einer Veränderung der Verantwortlichkeit führt, solange der Zweck der Verarbeitung durch den Verlag bestimmt bleibt.

Unabhängig von der Frage, wer den Identity Provider auswählt, bleibt der Kunde Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO, da er die maßgeblichen Schlüsselemente der Zweckbestimmung festlegt und über die wesentlichen Aspekte der Verarbeitung entscheidet. Die LDA unterstützt durch die technische Bereitstellung der Schnittstellen zur Informationsübertragung und ggfs. durch die Bereitstellung des Identity Providers lediglich die Realisierung der vom Verlag definierten Zweckbestimmung. In beiden Konstellationen ist die Rolle der LDA als Auftragsverarbeiter i.S.v. Art. 28 DSGVO zu bewerten, da sie weisungsgebunden tätig wird, keinen eigenen Zweck verfolgt und die Datenverarbeitung ausschließlich zur Erfüllung der vertraglichen Verpflichtungen gegenüber dem Verlag durchführt.

### 3.7.2. Transparenz

Die Nutzer werden über die Datenschutzerklärung des Kunden über die Verarbeitung im Rahmen der Authentifizierung informiert.

### 3.7.3. Zweckbindung

Die Authentifizierungsdaten werden ausschließlich zur Überprüfung der Nutzungsberechtigung und zur Steuerung des Zugriffs verarbeitet. Eine Nutzung zu anderen Zwecken findet nicht statt.

### 3.7.4. Datenminimierung

Verarbeitet werden nur diejenigen Identitätsmerkmale, die zur Prüfung der Berechtigung erforderlich sind. Die Berechtigungsprofile sind so ausgestaltet, dass Nutzer nur auf die für sie freigeschalteten Inhalte und Funktionen zugreifen können.

### 3.7.5. Richtigkeit

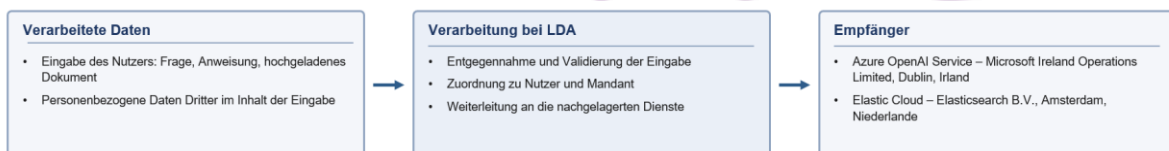
Die Richtigkeit der Identitätsdaten wird über den jeweiligen Identity Provider gewährleistet. Änderungen der Nutzerdaten werden dort nachgeführt und wirken unmittelbar auf die Zugriffsrechte.

### 3.7.6. Integrität und Vertraulichkeit

Die Übertragung der Authentifizierungsinformationen erfolgt verschlüsselt über standardisierte Protokolle. Passwörter werden nicht im Klartext gespeichert. Fehlgeschlagene Authentifizierungsversuche werden protokolliert und ausgewertet. Für administrative Zugänge besteht eine Zwei-Faktor-Authentifizierung.

### 3.7.7. Rechenschaftspflicht

Die Rechenschaftspflicht kann durch den Kunden anhand der Angaben in diesem Datenschutzkonzept erfüllt werden.



## 4. Eingabeprozess

### 4.1. Beschreibung des Verarbeitungsvorgangs

Eingaben können je nach Betriebsmodell über ein vom Kunden bereitgestelltes Frontend, über das LDA-Frontend oder über eine Drittapplikation eines Partners übermittelt werden. Das LDA-Tool unterstützt verschiedene Arten der Eingabe, darunter textuelle Eingaben in Form von Fragen oder Anweisungen sowie die Eingabe von Dokumenten, die vom System analysiert und verarbeitet werden. Mit der Eingabe leitet der Nutzer den weiteren Verarbeitungsvorgang ein.

### 4.2. Art der personenbezogenen Daten

Der Inhalt der Eingabe wird vom Nutzer bestimmt. In Betracht kommen sämtliche Kategorien personenbezogener Daten, insbesondere:

- Namen, Anschriften, Geburtsdaten, Kontaktdaten
- Vertrags- und Mandatsinformationen
- Bankverbindungen und Finanzdaten
- Beschäftigungsdaten
- Steuer-Identifikationsnummern und sonstige Identifikationsmerkmale
- Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO, insbesondere Gesundheitsdaten
- Daten, die dem Berufsgeheimnis unterliegen

Hinzu treten die technischen Begleitdaten der Eingabe (Zeitpunkt, Nutzerkennung, Verbindungsdaten).

### 4.3. Kategorien betroffener Personen

Im Zusammenhang mit dem Eingabeprozess können personenbezogene Daten von folgenden Kategorien betroffener Personen verarbeitet werden:

- Nutzer
- Sonstige Dritte, deren Daten durch den Nutzer eingegeben oder hochgeladen werden

### 4.4. Empfänger der Daten

Die Eingabe wird an das LDA-Back-End übermittelt und von dort an die Unterauftragsverarbeiter weitergeleitet, die für die Vektorisierung (**Microsoft Ireland Operations Limited**, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland, Azure OpenAI Service) und für die Suche (**Elasticsearch B.V.**, Keizersgracht 281, 1016 ED Amsterdam, Niederlande, Elastic Cloud) zuständig sind. Eine Weitergabe an sonstige Dritte findet nicht statt.

### 4.5. Regelfristen für die Löschung der Daten

Die Speicherdauer der Eingaben richtet sich nach der Konfiguration und den Vorgaben des Kunden. In der Standardkonfiguration werden Eingaben, Antworten und der zugehörige Verlauf 90 Kalender-tage nach der letzten Nutzung gelöscht; der Kunde kann eine kürzere Frist festlegen. Bei Löschung einer Eingabe werden auch die zugehörigen Einbettungen, Cache-Inhalte und Protokolleinträge erfasst.

Der Nutzer kann einzelne Eingaben und den zugehörigen Verlauf jederzeit über die Löschfunktion in der Anwendung selbst löschen.

#### **4.6. Datenübermittlung in Drittländer**

Eine Übermittlung in ein Drittland findet nicht statt. Die an den Azure OpenAI Service weitergeleiteten Eingaben werden in den Regionen West Europe, Sweden Central und Data Zone Standard (EU Boundary) verarbeitet, die an die Elastic Cloud weitergeleiteten Suchanfragen in der Region Europäische Union/EWR (Niederlande).

#### **4.7. Einhaltung der Datenschutzgrundsätze**

##### **4.7.1. Rechtmäßigkeit der Verarbeitung**

###### **a) Perspektive des Kunden**

Die Verarbeitung der Eingabe ist zur Erfüllung des Nutzungsvertrages erforderlich; Rechtsgrundlage ist insoweit Art. 6 Abs. 1 lit. b DSGVO.

Für die inhaltlichen Bestandteile der Eingabe, insbesondere für personenbezogene Daten Dritter, die der Nutzer einbringt, ist nicht der Kunde, sondern der Endkunde Verantwortlicher. Dieser hat eine eigene Rechtsgrundlage vorzuhalten.

###### **b) Perspektive LDA**

LDA wird insoweit als Auftragsverarbeiterin im Sinne von Art. 28 DSGVO tätig und benötigt für diese Verarbeitungstätigkeit keine eigene Rechtsgrundlage. Die Rechtmäßigkeit der Verarbeitung leitet sich aus der Rechtsgrundlage des Kunden als Verantwortlichem ab.

Hinsichtlich der vom Nutzer eingebrachten Inhalte wird LDA als Unterauftragsverarbeiter des Endkunden tätig (Art. 28 Abs. 4 DSGVO). LDA verfolgt hinsichtlich der Eingaben keine eigenen Zwecke; insbesondere findet keine Auswertung der Eingabeinhalte zu Zwecken der Produktentwicklung oder des Modelltrainings statt.

##### **4.7.2. Transparenz**

Die Nutzer werden über die Datenschutzerklärung des Kunden über die Verarbeitung ihrer Eingaben informiert. Gegenüber den weiteren betroffenen Personen – insbesondere Mandanten – obliegt die Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO der Organisation des Nutzers.

Der Kunde weist seine Nutzer in den Nutzungsbedingungen und an der Eingabemaske auf die Vorgaben zur Eingabe personenbezogener Daten hin.

##### **4.7.3. Zweckbindung**

Die Eingaben werden ausschließlich zur Erbringung der vom Nutzer angeforderten Funktion verarbeitet. Eine Nutzung zu anderen Zwecken, insbesondere zum Training oder zur Feinabstimmung von KI-Modellen, findet nicht statt.

##### **4.7.4. Datenminimierung**

Die Entscheidung, ob und welche personenbezogenen Daten eingegeben werden, obliegt dem jeweiligen Nutzer. Eine inhaltliche Filterung der Eingabe durch eine Guardrails-Funktion wird nicht eingesetzt, da für bestimmte Anfragen – etwa den Klausel-Check – die unveränderte Originaleingabe für die ordnungsgemäße Verarbeitung maßgeblich ist; eine vorgelagerte Veränderung würde die Funktionsfähigkeit beeinträchtigen.

Der Kunde hat Nutzer daher dazu anzuhalten, nur diejenigen Informationen einzugeben, die für die jeweilige Anfrage erforderlich sind.

#### 4.7.5. Richtigkeit

Die Richtigkeit der Eingaben liegt in der Verantwortung des Nutzers. Eine Berichtigung ist durch Löschung und erneute Eingabe möglich.

#### 4.7.6. Integrität und Vertraulichkeit

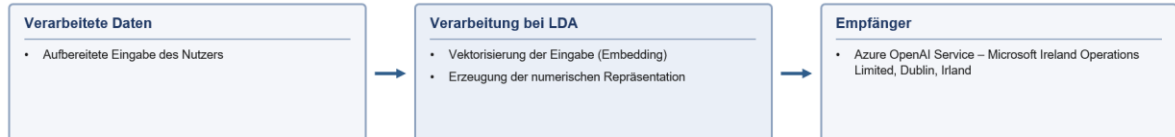
Die Eingaben werden verschlüsselt übertragen und gespeichert. Die Datenbestände sind mandantenbezogen getrennt. Der Zugriff auf Eingaben durch Mitarbeiter der LDA ist auf das für die Leistungserbringung unerlässliche Maß beschränkt und wird protokolliert. Volltextinhalte von Eingaben werden nicht in Protokolldateien gespeichert.

Angesichts der berufsrechtlichen Verschwiegenheitspflichten der Nutzer sind die Mitarbeiter der LDA und der eingesetzten Unterauftragsverarbeiter unter Hinweis auf § 203 StGB zur Verschwiegenheit verpflichtet.

#### 4.7.7. Rechenschaftspflicht

Die Rechenschaftspflicht kann durch den Kunden anhand der Angaben in diesem Datenschutzkonzept erfüllt werden. Für die von der Organisation des Nutzers zu verantwortenden Eingabeinhalte hat diese eigene Nachweise vorzuhalten.

### 5. Verarbeitung der Eingabe



#### 5.1. Beschreibung des Verarbeitungsvorgangs

Nach dem Eingabeprozess erfolgt zunächst ein Pre-Processing der Eingabedaten. Im Rahmen des Pre-Processing erfolgt die technische Aufbereitung und Formatierung der Eingabedaten, insbesondere die Vereinheitlichung von Zeichencodierungen, die Normalisierung von Sonderzeichen und Umlauten, die Konvertierung in eine konsistente Kodierung (UTF-8) sowie die Überführung in ein strukturiertes Format wie JSON. Der eigentliche Inhalt der Anfrage wird dabei nicht verändert oder inhaltlich manipuliert.

Bei längeren Texten erfolgt eine Aufteilung in kleinere Segmente (Chunking) unter Wahrung der inhaltlichen Integrität. Die Segmentierung erfolgt unter Berücksichtigung der inhaltlichen Zusammenhänge, um sicherzustellen, dass die Segmente semantisch kohärent bleiben und wichtige Informationen nicht an Segmentgrenzen verloren gehen.

Anschließend wird die Eingabe über den Azure OpenAI Service mittels Embedding-Modellen (text-embedding-3-small bzw. -large) vektorisiert, also in numerische Repräsentationen umgewandelt. Dies bildet die Grundlage für die nachfolgende Vektorsuche. Der Embedding-Schritt wird unabhängig vom konkreten Anwendungsfall zentral vor der Suche durchgeführt.

## 5.2. Art der verarbeiteten Daten

Verarbeitet werden die unter Ziffer 4.2 (Eingabeprozess) dargestellten Datenkategorien. Hinzu treten die aus der Eingabe erzeugten Einbettungen.

## 5.3. Kategorien betroffener Personen

Von der Verarbeitung betroffen sind die unter Ziffer 4.3 (Eingabeprozess) dargestellten Kategorien betroffener Personen.

## 5.4. Empfänger der Daten

Die Eingabe wird zur Vektorisierung an die **Microsoft Ireland Operations Limited**, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland (Azure OpenAI Service) als Unterauftragsverarbeiter der LDA übermittelt.

## 5.5. Regelfristen für die Löschung der Daten

Die Eingaben werden beim Azure OpenAI Service nach der eingestellten Konfiguration nicht gespeichert; es ist die Einstellung „no data retention“ bzw. das entsprechende Opt-Out konfiguriert. Die im LDA-Tool erzeugten Einbettungen unterliegen den unter Ziffer 4.5 (Eingabeprozess) dargestellten Fristen.

## 5.6. Datenübermittlung in Drittländer

Eine Übermittlung in ein Drittland findet nicht statt. Der Azure OpenAI Service ist auf die Verarbeitungsregionen West Europe, Sweden Central und Data Zone Standard (EU Boundary) konfiguriert; die Verarbeitung erfolgt damit innerhalb der EU-Datengrenze.

## 5.7. Einhaltung der Datenschutzgrundsätze

### 5.7.1. Rechtmäßigkeit der Verarbeitung

#### a) Perspektive des Kunden

Die Vektorisierung der Eingabe ist ein zwingend erforderlicher Zwischenschritt der vertraglich geschuldeten Leistung. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO; für die inhaltlichen Bestandteile der Eingabe gelten die Ausführungen zum Eingabeprozess entsprechend.

#### b) Perspektive LDA

LDA wird insoweit als Auftragsverarbeiterin im Sinne von Art. 28 DSGVO tätig und benötigt für diese Verarbeitungstätigkeit keine eigene Rechtsgrundlage. Die Rechtmäßigkeit der Verarbeitung leitet sich aus der Rechtsgrundlage des Kunden als Verantwortlichem ab.

Ein eigener Zweck der LDA oder des Azure OpenAI Service ist mit der Vektorisierung nicht verbunden. Die Einbettungen werden ausschließlich zur Durchführung der nachfolgenden Suche erzeugt.

### 5.7.2. Transparenz

Die Nutzer sind durch den Kunden in einer einfachen und verständlichen Sprache über sämtliche Datenverarbeitungen im Zusammenhang mit der Verarbeitung der Eingabe sowie auf ihre diesbezüglichen Rechte hinzuweisen.

### 5.7.3. Zweckbindung

Die Vektorisierung erfolgt ausschließlich zur Durchführung der nachfolgenden Suche. Eine Nutzung der Eingaben oder Einbettungen zum Training oder zur Feinabstimmung von Modellen findet nicht statt; dies ist vertraglich sichergestellt und technisch konfiguriert.

### 5.7.4. Datenminimierung

Übermittelt wird ausschließlich die vom Nutzer getätigte Eingabe in der zur Vektorisierung erforderlichen Form. Eine Anreicherung um weitere Daten findet nicht statt. Der Nutzerkontext wird nicht mit übermittelt.

### 5.7.5. Richtigkeit

Der Inhalt der Eingabe wird beim Pre-Processing nicht verändert. Die Vektorisierung ist ein rein technischer Vorgang ohne inhaltliche Veränderung.

### 5.7.6. Integrität und Vertraulichkeit

Die Übermittlung an den Azure OpenAI Service erfolgt verschlüsselt. Die Verarbeitung findet innerhalb der konfigurierten Region statt. Microsoft ist durch Auftragsverarbeitungsvertrag zur Vertraulichkeit verpflichtet.

### 5.7.7. Rechenschaftspflicht

Die Rechenschaftspflicht kann durch den Kunden anhand der Angaben in diesem Datenschutzkonzept erfüllt werden.

## 6. Suche nach relevanten Inhalten



### 6.1. Beschreibung des Verarbeitungsvorgangs

Auf Basis der vektorisierten Eingabe wird eine Vektorsuche nach passenden Textstellen in der Elastic-Cloud-Datenbank durchgeführt. Die Vektorsuche beruht auf dem Vergleich des Vektors der Eingabe mit den Vektoren der im Legal Data Hub gespeicherten Inhalte durch Berechnung der Ähnlichkeit. Diese semantische Suche ermöglicht es, auch dann relevante Inhalte zu finden, wenn diese nicht exakt dieselben Begriffe verwenden wie die Eingabe, aber thematisch verwandt sind.

Parallel hierzu kann eine Volltextsuche auf Basis der Eingabe durchgeführt werden, die Inhalte identifiziert, die die in der Eingabe enthaltenen Begriffe exakt oder in ähnlicher Form verwenden.

Nach Durchführung von Vektor- und Volltextsuche erfolgt eine nachgelagerte Neugewichtung der Suchergebnisse (Reranking), die die Relevanz der gefundenen Textstellen für die konkrete Anfrage verfeinert und die Ergebnisse für die Antwortgenerierung auswählt.

## 6.2. Art der personenbezogenen Daten

Verarbeitet werden die unter Ziffer 4.2 (Eingabeprozess) dargestellten Datenkategorien sowie die aus der Eingabe erzeugten Einbettungen. Hinzu treten die in den Textstellen des Legal Data Hub enthaltenen personenbezogenen Daten Dritter (Ziffer 1.2 – Indexierung).

## 6.3. Kategorien betroffener Personen

Im Zusammenhang mit der Suche nach relevanten Inhalten können personenbezogene Daten von folgenden Kategorien betroffener Personen verarbeitet werden:

- Nutzer
- Sonstige Dritte, deren Daten durch den Nutzer eingegeben oder hochgeladen werden
- Sonstige in den Fachinhalten genannte natürliche Personen

## 6.4. Empfänger der Daten

Die Suchanfrage wird an die **Elasticsearch B.V.**, Keizersgracht 281, 1016 ED Amsterdam, Niederlande (Elastic Cloud) als Unterauftragsverarbeiter der LDA L übermittelt.

## 6.5. Regelfristen für die Löschung der Daten

Die Suchanfragen werden nach Durchführung der Suche nicht dauerhaft gespeichert. Soweit Suchanfragen zur Fehleranalyse protokolliert werden, gelten die unter Ziffer 10.5 (Protokollierung und Monitoring zur Sicherheit) dargestellten Fristen.

## 6.6. Datenübermittlung in Drittländer

Eine Übermittlung in ein Drittland findet nicht statt. Die Elastic Cloud wird in der Region Europäische Union/EWR (Niederlande) betrieben.

## 6.7. Einhaltung der Datenschutzgrundsätze

### 6.7.1. Rechtmäßigkeit der Verarbeitung

#### a) Perspektive des Kunden

Die Durchführung der Suche ist zur Erfüllung des Nutzungsvertrages erforderlich; Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO. Für die in den ermittelten Textstellen enthaltenen personenbezogenen Daten Dritter gilt die zur Indexierung dargestellte Rechtsgrundlage des Art. 6 Abs. 1 lit. f DSGVO fort.

#### b) Perspektive LDA

LDA wird insoweit als Auftragsverarbeiterin im Sinne von Art. 28 DSGVO tätig und benötigt für diese Verarbeitungstätigkeit keine eigene Rechtsgrundlage. Die Rechtmäßigkeit der Verarbeitung leitet sich aus der Rechtsgrundlage des Kunden als Verantwortlichem ab.

### 6.7.2. Transparenz

Die Nutzer sind durch den Kunden in einer einfachen und verständlichen Sprache über sämtliche Datenverarbeitungen im Zusammenhang mit der Suche nach relevanten Inhalten sowie auf ihre diesbezüglichen Rechte hinzuweisen.

### 6.7.3. Zweckbindung

Die Suchanfragen werden ausschließlich zur Ermittlung der einschlägigen Textstellen verarbeitet. Eine Auswertung des Suchverhaltens einzelner Nutzer zu anderen Zwecken findet nicht statt.

### 6.7.4. Datenminimierung

Übermittelt wird ausschließlich die zur Durchführung der Suche erforderliche Anfrage. Die Suchergebnisse werden auf die für die Antwortgenerierung relevanten Textstellen beschränkt.

### 6.7.5. Richtigkeit

Die Suche gibt die im Legal Data Hub gespeicherten Inhalte unverändert wieder. Die Relevanzgewichtung verändert die Inhalte nicht.

### 6.7.6. Integrität und Vertraulichkeit

Die Übermittlung an Elastic erfolgt verschlüsselt. Die Datenbestände sind mandantenbezogen getrennt; die Suche erfolgt ausschließlich innerhalb der für den jeweiligen Nutzer freigeschalteten Inhalte. Elastic ist durch Auftragsverarbeitungsvertrag zur Vertraulichkeit verpflichtet.

### 6.7.7. Rechenschaftspflicht

Die Rechenschaftspflicht kann durch den Kunden anhand der Angaben in diesem Datenschutzkonzept erfüllt werden.

## 7. Antwortgenerierung



### 7.1. Beschreibung des Verarbeitungsvorgangs

Die Antwortgenerierung erfolgt auf Basis der Eingabe, der ermittelten Textstellen aus dem Legal Data Hub und eines von der LDA vorgegebenen Meta-Prompts. Die eigentliche Generierung erfolgt durch Sprachmodelle des Azure OpenAI Service, die auf Basis des bereitgestellten Kontextes eine Antwort in natürlicher Sprache erstellen.

Das LDA-Tool legt dem Nutzer die konkrete Textgrundlage offen, auf der die Antwort beruht, und ermöglicht eine direkte Verlinkung zu den Fundstellen. Dies ermöglicht dem Nutzer, die generierte Antwort zu verifizieren und die ursprünglichen Quellen im Legal Data Hub nachzulesen.

Soweit die Eingabe oder die Textstellen personenbezogene Daten enthalten, werden diese im Rahmen der Antwortgenerierung an den Azure OpenAI Service übermittelt und dort verarbeitet. Die generierte Antwort kann personenbezogene Daten enthalten, wenn diese in der Eingabe oder den Textstellen enthalten waren.

### 7.2. Art der personenbezogenen Daten

Verarbeitet werden die unter Ziffer 4.2 (Eingabeprozess) und Ziffer 1.2 (Indexierung) dargestellten Datenkategorien. Hinzu treten die in der generierten Antwort wiedergegebenen personenbezogenen Daten.

### 7.3. Kategorien betroffener Personen

Im Zusammenhang mit der Suche nach relevanten Inhalten können personenbezogene Daten von folgenden Kategorien betroffener Personen verarbeitet werden:

- Nutzer
- Sonstige Dritte, deren Daten durch den Nutzer eingegeben oder hochgeladen werden
- Sonstige in den Fachinhalten genannte natürliche Personen

### 7.4. Empfänger der Daten

Die Eingabe, die ermittelten Textstellen und der Meta-Prompt werden an die **Microsoft Ireland Operations Limited**, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland (Azure OpenAI Service) als Unterauftragsverarbeiter der LDA übermittelt. Die generierte Antwort wird an den Nutzer zurückgegeben.

### 7.5. Regelfristen für die Löschung der Daten

Beim Azure OpenAI Service werden Eingaben und Antworten nach der eingestellten Konfiguration nicht gespeichert. Die im LDA-Tool gespeicherten Antworten unterliegen den unter Ziffer 4.5 (Eingabeprozess) dargestellten Fristen.

### 7.6. Datenübermittlung in Drittländer

Eine Übermittlung in ein Drittland findet nicht statt. Der Azure OpenAI Service ist auf die Verarbeitungsregionen West Europe, Sweden Central und Data Zone Standard (EU Boundary) konfiguriert; die Verarbeitung erfolgt damit innerhalb der EU-Datengrenze.

### 7.7. Einhaltung der Datenschutzgrundsätze

#### 7.7.1. Rechtmäßigkeit der Verarbeitung

##### a) Perspektive des Kunden

Die Generierung der Antwort ist die vertraglich geschuldete Hauptleistung; Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO. Für die in der Eingabe und in den Textstellen enthaltenen personenbezogenen Daten Dritter gelten die Ausführungen zum Eingabeprozess und zur Indexierung entsprechend.

Eine automatisierte Entscheidung im Einzelfall im Sinne von Art. 22 Abs. 1 DSGVO ist mit der Antwortgenerierung nicht verbunden. Die Ausgabe des LDA-Tools ist ein Rechercheergebnis, das der Nutzer eigenverantwortlich bewertet; eine rechtliche Wirkung oder eine vergleichbare erhebliche Beeinträchtigung tritt erst durch die anschließende menschliche Entscheidung ein. Der Kunde hat seine Endkunden darauf hinzuweisen, dass die Ausgaben nicht ungeprüft zur Grundlage von Entscheidungen über betroffene Personen gemacht werden dürfen.

##### b) Perspektive LDA

LDA wird insoweit als Auftragsverarbeiterin im Sinne von Art. 28 DSGVO tätig und benötigt für diese Verarbeitungstätigkeit keine eigene Rechtsgrundlage. Die Rechtmäßigkeit der Verarbeitung leitet sich aus der Rechtsgrundlage des Kunden als Verantwortlichem ab.

### 7.7.2. Transparenz

Die Nutzer sind durch den Kunden in einer einfachen und verständlichen Sprache über sämtliche Datenverarbeitungen im Zusammenhang mit der Antwortgenerierung sowie auf ihre diesbezüglichen Rechte hinzuweisen.

### 7.7.3. Zweckbindung

Die übermittelten Daten werden ausschließlich zur Generierung der angeforderten Antwort verarbeitet. Eine Nutzung zum Training oder zur Feinabstimmung von Modellen findet nicht statt.

### 7.7.4. Datenminimierung

An das Sprachmodell werden ausschließlich die Eingabe, die für die Beantwortung ausgewählten Textstellen und der Meta-Prompt übergeben. Der Umfang der übergebenen Textstellen ist auf das für die Beantwortung erforderliche Maß beschränkt.

### 7.7.5. Richtigkeit

Die Antworten werden von einer KI auf Wahrscheinlichkeitsbasis erzeugt und können unrichtig sein; sie können auch unrichtige Aussagen über natürliche Personen enthalten. Eine inhaltliche Richtigkeitsprüfung findet innerhalb des LDA-Tools nicht statt. Dem wird durch folgende Maßnahmen Rechnung getragen:

- Quellentransparenz und Verlinkung der Fundstellen, die dem Nutzer die Überprüfung anhand der Originalquelle ermöglichen;
- Hinweis in den Nutzungsbedingungen, dass die Antworten fehlerhaft sein können und vom Nutzer eigenverantwortlich zu prüfen sind;
- Beschränkung der Wissensbasis auf die im Legal Data Hub bereitgestellten, kuratierten Fachinformationen.

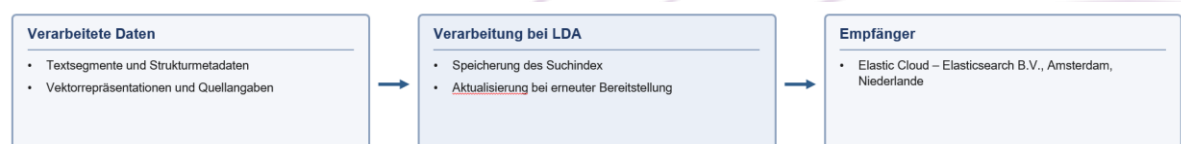
### 7.7.6. Integrität und Vertraulichkeit

Die Übermittlung an den Azure OpenAI Service erfolgt verschlüsselt. Die Verarbeitung findet innerhalb der konfigurierten Region statt. Microsoft ist durch Auftragsverarbeitungsvertrag zur Vertraulichkeit verpflichtet.

### 7.7.7. Rechenschaftspflicht

Die Rechenschaftspflicht kann durch den Kunden anhand der Angaben in diesem Datenschutzkonzept erfüllt werden.

## 8. Datenhaltung für Suchfunktionen



### 8.1. Beschreibung der Verarbeitung

Die Speicherung und Verarbeitung von Daten für die Suchfunktion erfolgten in Form von Vektoren, Rohtext und Metadaten. Die Vektoren werden in der Elastic-Cloud-Datenbank gespeichert und dienen der semantischen Suche, während der Rohtext der Verlagsinhalte und die Metadaten die

Volltextsuche sowie die Rekonstruktion der ursprünglichen Inhalte ermöglichen. Die Speicherung erfolgt in den von LDA betriebenen Systemen sowie bei den genehmigten Unterauftragsverarbeitern.

## **8.2. Art der personenbezogenen Daten**

Die indexierten Fachinhalte enthalten regelmäßig keine personenbezogenen Daten der Nutzer. Sie können jedoch personenbezogene Daten Dritter enthalten, soweit die Fachinformationen solche wiedergeben, etwa

- Angaben zu Verfahrensbeteiligten in veröffentlichten Gerichtsentscheidungen, soweit diese nicht (hinreichend) anonymisiert wurden,
- Namen von Autoren, Herausgebern und Bearbeitern der Fachinhalte sowie
- Namen von sonstigen in den Fachbeiträgen genannte Personen

## **8.3. Kategorien betroffener Personen**

Im Zusammenhang mit der Datenhaltung für die Suchfunktion können personenbezogene Daten von folgenden Kategorien betroffener Personen verarbeitet werden:

- Verfahrensbeteiligte aus veröffentlichten Entscheidungen
- Autoren, Herausgeber und Bearbeiter von Fachinhalten
- Sonstige in den Fachinhalten genannte natürliche Personen

## **8.4. Empfänger der Daten**

Die Speicherung erfolgt bei der **Elasticsearch B.V.**, Keizersgracht 281, 1016 ED Amsterdam, Niederlande (Elastic Cloud) als Unterauftragsverarbeiter der LDA. Eine Weitergabe an sonstige Dritte findet nicht statt.

## **8.5. Regelfristen für die Löschung der Daten**

Die indexierten Inhalte werden für die Dauer des Vertragsverhältnisses mit dem Kunden vorgehalten. Nimmt der Kunde Inhalte aus dem Legal Data Hub heraus, werden die zugehörigen Textsegmente, Metadaten und Vektoren gelöscht. Nach Beendigung des Vertragsverhältnisses erfolgt die Löschung oder Rückgabe nach Wahl des Kunden gemäß Art. 28 Abs. 3 lit. g DSGVO innerhalb von 60 Kalendertagen nach Vertragsende; LDA bescheinigt dem Kunden die Löschung.

## **8.6. Datenübermittlung in Drittländer**

Eine Übermittlung in ein Drittland findet nicht statt. Die Elastic Cloud wird in der Region Europäische Union/EWR (Niederlande) betrieben.

## **8.7. Einhaltung der Datenschutzgrundsätze**

### **8.7.1. Rechtmäßigkeit der Verarbeitung**

#### **a) Perspektive des Kunden**

Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO, soweit die Speicherung zur Erfüllung des Nutzungsvertrages erforderlich ist, sowie Art. 6 Abs. 1 lit. f DSGVO für die in den Inhalten enthaltenen personenbezogenen Daten Dritter. Auf die Ausführungen unter Ziffer 1.7.1 (Indexierung, Rechtmäßigkeit der Verarbeitung) wird verwiesen.

## b) Perspektive LDA

LDA wird insoweit als Auftragsverarbeiterin im Sinne von Art. 28 DSGVO tätig und benötigt für diese Verarbeitungstätigkeit keine eigene Rechtsgrundlage. Die Rechtmäßigkeit der Verarbeitung leitet sich aus der Rechtsgrundlage des Kunden als Verantwortlichem ab.

### 8.7.2. Transparenz

Die Erfüllung der Informationspflichten gegenüber den in den Fachinhalten genannten Personen obliegt dem Kunden. Für veröffentlichte Entscheidungen und Fachbeiträge kommt regelmäßig die Ausnahme des Art. 14 Abs. 5 DSGVO in Betracht.

### 8.7.3. Zweckbindung

Die gespeicherten Daten werden ausschließlich zur Bereitstellung der Such- und Antwortfunktionen verwendet.

### 8.7.4. Datenminimierung

Gespeichert werden ausschließlich die für die Suchfunktionalität erforderlichen Daten.

### 8.7.5. Richtigkeit

Die gespeicherten Textsegmente geben die Fachinhalte unverändert wieder. Die inhaltliche Richtigkeit der Inhalte liegt in der Verantwortung des Kunden. Aktualisierungen und Berichtigungen der Fachinhalte werden bei erneuter Bereitstellung durch den Kunden in den Legal Data Hub übernommen; die zugehörigen Vektoren werden dabei neu erzeugt.

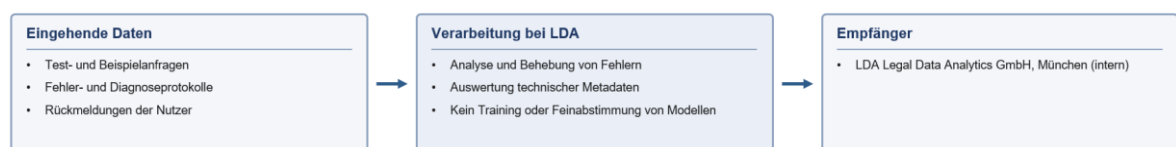
### 8.7.6. Integrität und Vertraulichkeit

Die Speicherung erfolgt verschlüsselt. Die Datenbestände sind mandantenbezogen getrennt. Der administrative Zugriff ist beschränkt und wird protokolliert.

### 8.7.7. Rechenschaftspflicht

Die Rechenschaftspflicht kann durch den Kunden anhand der Angaben in diesem Datenschutzkonzept erfüllt werden.

## 9. Qualitätssicherung/Produktverbesserung



### 9.1. Beschreibung des Verarbeitungsvorgangs

Zur Sicherstellung der Qualität der LDA-Dienste werden regelmäßige Tests zu Performance, Datenqualität und Antwortgenerierung durchgeführt. Diese Tests dienen der kontinuierlichen Verbesserung des Systems und der Sicherstellung der Qualität der generierten Antworten und Suchergebnisse. Zudem werden zum Zwecke der Fehleranalyse und Qualitätssicherung Systemaktivitäten und Nutzungsereignisse protokolliert, wobei unter anderem Zeitpunkt und Art der Anfragen, aufgerufene Endpunkte, Antwortzeiten sowie Fehler- und Diagnose-Logs erfasst werden. Die Ergebnisse der Qualitätssicherung werden dokumentiert und identifizierte Herausforderungen werden systematisch

adressiert. Eine Verwendung personenbezogener Daten zum Training oder zur Verbesserung von KI-Modellen findet nicht statt.

## 9.2. Art der personenbezogenen Daten

Im Rahmen der Qualitätssicherung werden insbesondere die nachfolgenden Kategorien personenbezogener Daten verarbeitet:

- Test- und Beispielanfragen einschließlich der hierzu generierten Antworten
- ausgewählte reale Eingaben und Antworten, soweit dies zur Analyse eines konkreten Fehlers erforderlich ist
- Fehler-, Diagnose- und Ereignisprotokolle
- Technische Metadaten (Zeitpunkt und Art der Anfrage, aufgerufener Endpunkt, Antwortzeit, Fehlercode)
- Nutzer- und Mandantenkennung, regelmäßig in pseudonymisierter Form
- Rückmeldungen der Nutzer zur Qualität der Antworten (Bewertungen, Freitextangaben)

Reale Eingaben und Antworten werden nur ausgewertet, soweit dies zur Fehleranalyse unerlässlich ist. Für die Zwecke der Produktverbesserung im engeren Sinne verwendet LDA ausschließlich anonymisierte oder aggregierte Auswertungen.

## 9.3. Kategorien betroffener Personen

Im Zusammenhang mit der Qualitätssicherung können personenbezogene Daten von folgenden Kategorien betroffener Personen verarbeitet werden:

- Nutzer
- Beschäftigte und Ansprechpartner des Kunden und der Endkunden
- sonstige Dritte, deren Daten in Eingaben oder Fachinhalten enthalten sind

## 9.4. Empfänger der Daten

Empfänger sind die für Qualitätssicherung und Entwicklung zuständigen Beschäftigten der **Legal Data Analytics GmbH**, Hochwaldstraße 26, 81377 München. Eine Weitergabe an sonstige Dritte findet nicht statt. Eine Verwendung personenbezogener Daten zum Training oder zur Feinabstimmung von KI-Modellen findet nicht statt.

## 9.5. Regelfristen für die Löschung der Daten

Fehler- und Diagnoseprotokolle werden nach 90 Kalendertagen gelöscht. Dokumentationen zu durchgeführten Tests werden für zwölf Monate aufbewahrt, um wiederkehrende Fehlerbilder über einen Release-Zyklus hinweg auswerten zu können. Rückmeldungen der Nutzer werden nach zwölf Monaten gelöscht oder anonymisiert. Für Auswertungen, die in anonymisierter oder aggregierter Form vorliegen, gelten die Löschfristen nicht, da kein Personenbezug mehr besteht.

## 9.6. Datenübermittlung in Drittländer

Eine Übermittlung in ein Drittland findet nicht statt. Die Auswertung erfolgt in den Systemen der LDA.

## **9.7. Einhaltung der Datenschutzgrundsätze**

### **9.7.1. Rechtmäßigkeit der Verarbeitung**

#### **a) Perspektive des Kunden**

Soweit der Kunde die Qualitätssicherung veranlasst, ist Rechtsgrundlage Art. 6 Abs. 1 lit. b DSGVO, da ein funktionsfähiger und fehlerfreier Dienst Gegenstand des Nutzungsvertrages ist. Ergänzend kommt Art. 6 Abs. 1 lit. f DSGVO in Betracht.

#### **b) Perspektive LDA**

Soweit die Qualitätssicherung der Erfüllung der gegenüber dem Kunden geschuldeten Leistungspflichten dient – insbesondere der Sicherstellung der Funktionsfähigkeit, der Fehlerbehebung und der Einhaltung vereinbarter Qualitätsanforderungen –, wird LDA als Auftragsverarbeiterin tätig und benötigt keine eigene Rechtsgrundlage.

### **9.7.2. Transparenz**

Der Kunde hat seine Nutzer in der Datenschutzerklärung darüber zu informieren, dass Nutzungsergebnisse zu Zwecken der Fehleranalyse und Qualitätssicherung protokolliert werden.

### **9.7.3. Zweckbindung**

Die Daten werden ausschließlich zur Sicherstellung und Verbesserung der Qualität der LDA-Dienste verarbeitet. Eine Nutzung zu Werbezwecken, zur Profilbildung oder zum Training von KI-Modellen findet nicht statt.

### **9.7.4. Datenminimierung**

Die Auswertung erfolgt vorrangig anhand technischer Metadaten und synthetischer Testdaten. Ein Zugriff auf reale Eingabeinhalte erfolgt nur, wenn eine Fehleranalyse anders nicht möglich ist. Volltextinhalte von Eingaben werden nicht in Protokolldateien gespeichert.

### **9.7.5. Richtigkeit**

Die Qualitätssicherung dient gerade der Sicherstellung der Richtigkeit und Nachvollziehbarkeit der Ergebnisse. Erkannte Abweichungen werden dokumentiert und systematisch behoben

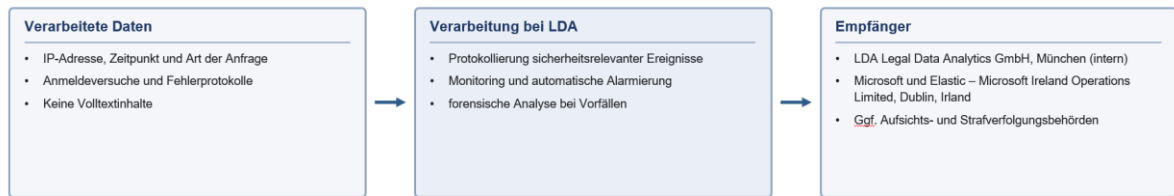
### **9.7.6. Integrität und Vertraulichkeit**

Der Zugriff auf Qualitätssicherungsdaten ist auf einen begrenzten Kreis berechtigter Beschäftigter beschränkt und wird protokolliert. Die Beschäftigten sind zur Vertraulichkeit und – im Hinblick auf die berufsrechtlichen Verschwiegenheitspflichten der Nutzer – unter Hinweis auf § 203 StGB verpflichtet.

### **9.7.7. Rechenschaftspflicht**

Die Rechenschaftspflicht kann durch den Kunden anhand der Angaben in diesem Datenschutzkonzept erfüllt werden.

## 10. Protokollierung und Monitoring zur Sicherheit



### 10.1. Beschreibung des Verarbeitungsvorgangs

Die Protokollierung von Systemaktivitäten und Nutzungsereignissen erfolgt zu den Zwecken der IT-Sicherheit, zum Zweck der Erkennung von Angriffen sowie der Sicherstellung der Verfügbarkeit und Integrität der LDA-Dienste. Im Rahmen dieses Verarbeitungsvorgangs werden sämtliche Zugriffe auf das System erfasst und überwacht, wobei insbesondere folgende Daten protokolliert werden: IP-Adressen der anfragenden Systeme, Zeitpunkt und Art der Anfragen, verwendete User-Agent-Informationen, aufgerufene API-Endpunkte, Antwortzeiten der Systeme, erfolgreiche und fehlgeschlagene Authentifizierungsversuche sowie sämtliche Fehler- und Diagnose-Logs.

Die Protokolldaten werden in sicherer Form gespeichert und durch automatisierte Monitoring-Tools auf anomale Muster, ungewöhnliche Zugriffsversuche, verdächtige Aktivitäten oder Sicherheitsvorfälle analysiert. Diese Echtzeitüberwachung ermöglicht eine frühzeitige Erkennung von Sicherheitsbedrohungen, unbefugten Zugriffsversuchen oder Systemstörungen sowie eine zeitnahe Reaktion auf identifizierte Vorfälle. Zudem dienen die Protokolldaten der forensischen Analyse bei Sicherheitsvorfällen, der Nachverfolgung von Missbrauchsversuchen sowie der Einhaltung von Sicherheitsstandards und vertraglichen Anforderungen.

### 10.2. Art der personenbezogenen Daten

Im Rahmen der Protokollierung und des Monitorings werden insbesondere die nachfolgenden Kategorien personenbezogener Daten verarbeitet:

- IP-Adressen der anfragenden Systeme
- Zeitpunkt und Art der Anfrage
- User-Agent-Informationen
- aufgerufene API-Endpunkte und Antwortzeiten
- Nutzer- und Mandantenkennung
- erfolgreiche und fehlgeschlagene Authentifizierungsversuche
- Fehler- und Diagnoseprotokolle sowie ausgelöste Sicherheitswarnungen

Volltextinhalte von Eingaben und Antworten werden nicht protokolliert.

### 10.3. Kategorien betroffener Personen

Im Zusammenhang mit der Protokollierung können personenbezogene Daten von folgenden Kategorien betroffener Personen verarbeitet werden:

- Nutzer
- Administratoren der LDA und der eingesetzten Unterauftragsverarbeiter
- Beschäftigte und Ansprechpartner des Kunden und der Endkunden

- Dritte, von deren Systemen aus auf die Anwendung zugegriffen wird, einschließlich unbefugter Zugriffsversuche

#### 10.4. Empfänger der Daten

Empfänger sind die für den sicheren Betrieb zuständigen Beschäftigten der **Legal Data Analytics GmbH**, Hochwaldstraße 26, 81377 München sowie die **Microsoft Ireland Operations Limited**, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland und die **Elasticsearch B.V.**, Keizersgracht 281, 1016 ED Amsterdam, Niederlande als Unterauftragsverarbeiter, soweit die Protokolldaten in deren Systemen anfallen oder dort ausgewertet werden.

Im Fall eines Sicherheitsvorfalls können Protokolldaten an die zuständige Aufsichtsbehörde und an Strafverfolgungsbehörden sowie an zur Vertraulichkeit verpflichtete externe Forensikdienstleister übermittelt werden.

#### 10.5. Regelfristen für die Löschung der Daten

Sicherheitsrelevante Protokolldaten werden nach 90 Kalendertagen gelöscht; eine längere Speicherung ist nur zulässig, soweit sie zur Aufklärung eines konkreten Sicherheitsvorfalls erforderlich ist. Die Frist orientiert sich an der für Sicherheitsprotokolle regelmäßig als angemessen angesehenen Spanne von 30 bis 90 Tagen. Unterlagen zu einem dokumentierten Sicherheitsvorfall werden für die Dauer der Aufklärung und der Geltendmachung von Ansprüchen aufbewahrt, längstens bis zum Ablauf des dritten Kalenderjahres nach dem Jahr, in dem der Vorfall bekannt geworden ist (§§ 195, 199 Abs. 1 BGB). Für abrechnungsrelevante Protokolldaten gelten die Fristen nach Ziffer 11.5 (Abrechnung).

#### 10.6. Datenübermittlung in Drittländer

Eine Übermittlung in ein Drittland findet nicht statt. Die Protokolldaten werden in den Systemen der LDA sowie, soweit sie dort anfallen, in den unter Ziffer 2.6 (Infrastruktur und Anwendungsbetrieb) genannten Verarbeitungsregionen der Unterauftragsverarbeiter verarbeitet.

#### 10.7. Einhaltung der Datenschutzgrundsätze

##### 10.7.1. Rechtmäßigkeit der Verarbeitung

###### c) Perspektive des Kunden

Rechtsgrundlage für den Kunden ist Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit Art. 32 DSGVO sowie Art. 6 Abs. 1 lit. f DSGVO.

###### d) Perspektive LDA

Soweit die Protokollierung der Erfüllung der gegenüber dem Kunden geschuldeten Leistungspflichten dient, wird LDA als Auftragsverarbeiterin tätig und benötigt keine eigene Rechtsgrundlage.

##### 10.7.2. Transparenz

Der Kunde informiert seine Nutzer in der Datenschutzerklärung über die Protokollierung, deren Zwecke und die Speicherdauer.

##### 10.7.3. Zweckbindung

Die Protokolldaten werden ausschließlich zu den Zwecken der IT-Sicherheit, der Angriffserkennung, der Sicherstellung der Verfügbarkeit und der Fehleranalyse verarbeitet. Von diesem Grundsatz

ausgenommen ist die Verwendung der Nutzungsereignisse für die Abrechnung, die gesondert unter Ziffer 11 (Abrechnung) dargestellt ist.

#### 10.7.4. Datenminimierung

Protokolliert werden nur die für die genannten Zwecke erforderlichen Ereignisse und Metadaten. Volltextinhalte von Eingaben und Antworten werden nicht protokolliert. Der Zugriff auf Protokolldaten ist auf die für den sicheren Betrieb zuständigen Beschäftigten beschränkt.

#### 10.7.5. Richtigkeit

Die Protokolldaten werden automatisiert und unverändert erzeugt. Eine nachträgliche Veränderung ist durch die Konfiguration der Protokollierung ausgeschlossen.

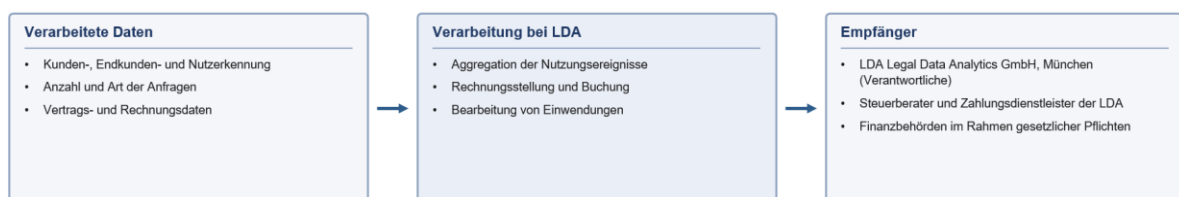
#### 10.7.6. Integrität und Vertraulichkeit

Die Protokolldaten werden verschlüsselt gespeichert, gegen nachträgliche Veränderung geschützt und mandantenbezogen getrennt gehalten. Der Zugriff erfolgt nach dem Grundsatz der geringsten Rechte, ist durch Zwei-Faktor-Authentifizierung abgesichert und wird seinerseits protokolliert.

#### 10.7.7. Rechenschaftspflicht

Die Rechenschaftspflicht kann durch den Kunden anhand der Angaben in diesem Datenschutzkonzept erfüllt werden.

### 11. Abrechnung



#### 11.1. Beschreibung des Verarbeitungsvorgangs

Für die Abrechnung der Nutzung der LDA-Dienste erhebt und verarbeitet LDA verschiedene Daten, um eine konkrete Abrechnung gegenüber den Kunden vorzunehmen. Die Abrechnung erfolgt auf Basis der erfassten Nutzungsdaten, insbesondere der Anzahl und Art der API-Anfragen je Nutzer und Kunde.

Diese abrechnungsrelevanten Daten werden durch die Protokollierung von Systemaktivitäten und Nutzungsereignissen erhoben und ermöglichen eine nutzungsabhängige Vergütung der LDA-Dienste gegenüber dem Verlag und Kunden als Auftraggeber.

#### 11.2. Art der personenbezogenen Daten

Im Rahmen der Abrechnung werden insbesondere die nachfolgenden Kategorien personenbezogener Daten verarbeitet:

- Kunden- und Endkundenkennung sowie Vertrags- und Lizenzdaten
- Nutzerkennung, soweit die Abrechnung nutzerbezogen erfolgt
- Anzahl und Art der Anfragen je Nutzer, Endkunde und Abrechnungszeitraum
- Verbrauchs- und Kontingentdaten

- Name und dienstliche Kontaktdaten der Ansprechpartner des Kunden
- Rechnungs-, Zahlungs- und Buchungsdaten

### **11.3. Kategorien betroffener Personen**

Im Zusammenhang mit der Abrechnung können personenbezogene Daten von folgenden Kategorien betroffener Personen verarbeitet werden:

- Nutzer
- Ansprechpartner und Beschäftigte des Kunden und der Endkunden

### **11.4. Empfänger der Daten**

Empfänger sind die für Vertrieb und Buchhaltung zuständigen Beschäftigten der LDA L sowie der Kunde als Rechnungsempfänger. Hinzu treten der Steuerberater und der eingesetzte Zahlungsdienstleister der LDA.

### **11.5. Regelfristen für die Löschung der Daten**

Rechnungen und die zugehörigen Buchungsbelege werden entsprechend den handels- und steuerrechtlichen Aufbewahrungsfristen für acht Jahre aufbewahrt (§ 147 Abs. 3 AO, § 257 Abs. 4 HGB). Die zugrunde liegenden nutzerbezogenen Rohnutzungsdaten werden nach Abschluss der Abrechnung und Ablauf der Einwendungsfrist, spätestens zwölf Monate nach Ende des jeweiligen Abrechnungszeitraums, gelöscht oder auf Kundenebene aggregiert. Die Frist stellt sicher, dass Einwendungen gegen eine Jahresabrechnung noch anhand der zugrunde liegenden Einzelnachweise geprüft werden können.

### **11.6. Datenübermittlung in Drittländer**

Eine Übermittlung in ein Drittland findet nicht statt; die Abrechnungsdaten werden ausschließlich innerhalb der Europäischen Union verarbeitet.

### **11.7. Einhaltung der Datenschutzgrundsätze**

#### **11.7.1. Rechtmäßigkeit der Verarbeitung**

##### **a) Perspektive des Kunden**

Der Kunde verarbeitet die Abrechnungsdaten zur Erfüllung des mit LDA geschlossenen Vertrages sowie zur Weiterberechnung gegenüber seinen Endkunden; Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO.

##### **b) Perspektive LDA**

Für die Abrechnung ihrer eigenen Leistungen ist LDA eigene Verantwortliche. Sie verfolgt insoweit einen eigenen Zweck und handelt nicht weisungsgebunden.

Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO, soweit die Verarbeitung zur Erfüllung des zwischen LDA und dem Kunden geschlossenen Vertrages erforderlich ist, sowie Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit den handels- und steuerrechtlichen Aufbewahrungs- und Aufzeichnungspflichten.

### 11.7.2. Transparenz

LDA informiert die Ansprechpartner des Kunden nach Art. 13 DSGVO über die Verarbeitung ihrer Kontaktdaten. Über die nutzungsabhängige Abrechnung und die hierfür erhobenen Daten informiert der Kunde seine Nutzer in der Datenschutzerklärung.

### 11.7.3. Zweckbindung

Die Abrechnungsdaten werden ausschließlich zur Abrechnung der LDA-Dienste, zur Erfüllung der handels- und steuerrechtlichen Pflichten sowie zur Bearbeitung von Einwendungen gegen die Abrechnung verarbeitet.

### 11.7.4. Datenminimierung

Erhoben werden ausschließlich die für die Abrechnung erforderlichen Daten.

### 11.7.5. Richtigkeit

Die Abrechnung erfolgt auf Grundlage automatisiert erfasster Nutzungsereignisse. Der Kunde kann Einwendungen gegen die Abrechnung erheben; LDA prüft diese anhand der zugrundeliegenden Protokolldaten und berichtigt die Abrechnung bei berechtigten Einwendungen.

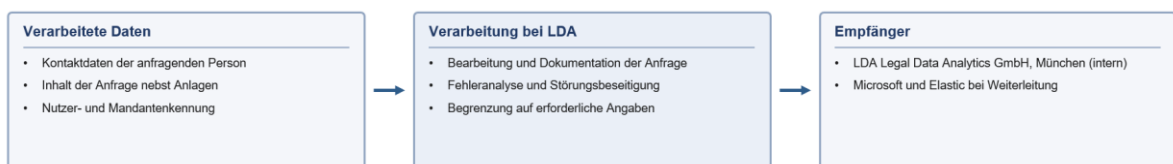
### 11.7.6. Integrität und Vertraulichkeit

Die Abrechnungsdaten werden verschlüsselt gespeichert. Der Zugriff ist auf die für Vertrieb und Buchhaltung zuständigen Beschäftigten beschränkt. Eine Verknüpfung der Abrechnungsdaten mit Eingabeinhalten findet nicht statt.

### 11.7.7. Rechenschaftspflicht

Die Rechenschaftspflicht kann durch den Kunden anhand der Angaben in diesem Datenschutzkonzept erfüllt werden.

## 12. Support



### 12.1. Beschreibung der Verarbeitung

Die Supportbearbeitung umfasst die Entgegennahme, Bearbeitung und Dokumentation von Support-Anfragen sowie die Identifizierung und Behebung von Fehlern oder Störungen im Zusammenhang mit der Nutzung der LDA-Dienste. Im Rahmen dieses Verarbeitungsvorgangs werden Support- und Kommunikationsdaten erhoben und verarbeitet, die Informationen über die anfragenden Personen (wie Namen, E-Mail-Adressen, Telefonnummern), den Inhalt der Support-Anfrage sowie die durchgeführten Maßnahmen zur Problemlösung enthalten können. Die Supportbearbeitung dient der Gewährleistung der Funktionsfähigkeit der LDA-Dienste, der zeitnahen Behebung technischer Probleme sowie der Unterstützung der Nutzer bei Fragen zur Nutzung des Systems.

## 12.2. Art der personenbezogenen Daten

Im Rahmen der Supportbearbeitung werden insbesondere die nachfolgenden Kategorien personenbezogener Daten verarbeitet:

- Name und dienstliche Kontaktdaten der anfragenden Person (E-Mail-Adresse, Telefonnummer)
- Nutzer- und Mandantenkennung sowie Angaben zur eingesetzten Konfiguration
- Inhalt der Support-Anfrage einschließlich beigefügter Screenshots, Protokollauszüge und Beispielergebnisse
- Bearbeitungsvermerke, Statusinformationen und der Kommunikationsverlauf

Die von der anfragenden Person beigefügten Unterlagen können personenbezogene Daten Dritter sowie dem Berufsgeheimnis unterliegende Informationen enthalten.

## 12.3. Kategorien betroffener Personen

Im Zusammenhang mit der Supportbearbeitung können personenbezogene Daten von folgenden Kategorien betroffener Personen verarbeitet werden:

- Nutzer
- Ansprechpartner und Beschäftigte des Kunden und der Endkunden
- sonstige Dritte, deren Daten in den übermittelten Unterlagen enthalten sind

## 12.4. Empfänger der Daten

Empfänger sind die für den Support zuständigen Beschäftigten der LDA. Soweit die Störung im Verantwortungsbereich eines Unterauftragsverarbeiters liegt, können die zur Analyse erforderlichen Angaben an die **Microsoft Ireland Operations Limited**, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland oder die **Elasticsearch B.V.**, Keizersgracht 281, 1016 ED Amsterdam, Niederlande weitergegeben werden.

## 12.5. Regelfristen für die Löschung der Daten

Support-Tickets werden nach Abschluss der Bearbeitung für zwölf Monate aufbewahrt und anschließend gelöscht; die Frist ermöglicht die Auswertung wiederkehrender Störungsbilder und die Bearbeitung von Folgeanfragen. Beigefügte Unterlagen mit Eingabeinhalten werden unmittelbar nach Abschluss der Fehleranalyse gelöscht, spätestens 30 Kalendertage nach Abschluss des Tickets. Soweit die Korrespondenz Bestandteil der Vertragsabwicklung ist, gelten die handels- und steuerrechtlichen Aufbewahrungsfristen von sechs beziehungsweise acht Jahren (§ 257 Abs. 4 HGB, § 147 Abs. 3 AO).

## 12.6. Datenübermittlung in Drittländer

Eine Übermittlung in einen Drittstaat findet nicht statt.

## **12.7. Einhaltung der Datenschutzgrundsätze**

### **12.7.1. Rechtmäßigkeit der Verarbeitung**

#### **a) Perspektive des Kunde**

Der Kunde verarbeitet die Supportdaten zur Erfüllung des Nutzungsvertrages gegenüber seinen Endkunden; Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO, ergänzend Art. 6 Abs. 1 lit. f DSGVO.

#### **b) Perspektive LDA**

Hinsichtlich der Kontaktdaten der anfragenden Person und der Dokumentation des Bearbeitungsvorgangs ist LDA eigene Verantwortliche. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO, soweit der Support Bestandteil der vertraglich geschuldeten Leistung ist, im Übrigen Art. 6 Abs. 1 lit. f DSGVO; das berechnigte Interesse liegt in der ordnungsgemäßen Bearbeitung und Dokumentation von Störungsmeldungen.

Hinsichtlich der in den übermittelten Unterlagen enthaltenen Eingabeinhalte wird LDA als Auftragsverarbeiterin beziehungsweise Unterauftragsverarbeiter tätig und benötigt keine eigene Rechtsgrundlage.

### **12.7.2. Transparenz**

LDA informiert die anfragenden Personen nach Art. 13 DSGVO über die Verarbeitung ihrer Kontaktdaten. Der Kunde informiert seine Nutzer über den Supportprozess und über die Vorgabe, Support-Anfragen keine über das Erforderliche hinausgehenden personenbezogenen Daten beizufügen.

### **12.7.3. Zweckbindung**

Die Supportdaten werden ausschließlich zur Bearbeitung und Dokumentation der Anfrage, zur Behebung der gemeldeten Störung und zur Vermeidung gleichartiger Störungen verarbeitet.

### **12.7.4. Datenminimierung**

Die Nutzer sind anzuhalten, Support-Anfragen nur diejenigen Informationen beizufügen, die zur Analyse der Störung erforderlich sind, und auf die Übermittlung von Mandats- und Gesundheitsdaten sowie sonstiger besonderer Kategorien personenbezogener Daten zu verzichten. LDA fordert die Übermittlung von Eingabeinhalten nur an, wenn die Analyse anders nicht möglich ist.

### **12.7.5. Richtigkeit**

Die Angaben der anfragenden Person werden unverändert dokumentiert. Unrichtige Angaben werden auf Hinweis berichtigt.

### **12.7.6. Integrität und Vertraulichkeit**

Der Zugriff auf Support-Tickets ist auf die zuständigen Beschäftigten beschränkt und wird protokolliert. Angesichts der berufsrechtlichen Verschwiegenheitspflichten der Nutzer sind die Beschäftigten der LDA und der eingesetzten Dienstleister unter Hinweis auf § 203 StGB zur Verschwiegenheit verpflichtet.

### **12.7.7. Rechenschaftspflicht**

Die Rechenschaftspflicht kann durch den Kunden anhand der Angaben in diesem Datenschutzkonzept erfüllt werden.

## **II. Rechte der betroffenen Personen**

Anlaufstelle für die Ausübung der Betroffenenrechte ist derjenige Verantwortliche, in dessen Verantwortungsbereich die Verarbeitung fällt. Für die Bereitstellung und Nutzung des LDA-Tools ist dies der Kunde, für die Inhalte der Eingaben der Endkunde, für Abrechnung und Support LDA selbst. LDA unterstützt den Kunden nach Art. 28 Abs. 3 lit. e DSGVO. Wendet sich eine betroffene Person unmittelbar an LDA, leitet LDA die Anfrage unverzüglich an den Kunden weiter und beantwortet sie nicht selbst, soweit LDA insoweit als Auftragsverarbeiterin handelt.

### **1. Recht auf Auskunft (Art. 15 DSGVO)**

Die von der Verarbeitung betroffenen Personen können Auskunft darüber verlangen, ob im Zusammenhang mit der Nutzung des LDA-Tools personenbezogene Daten über sie verarbeitet werden, und wenn dies der Fall ist,

- welche Datenkategorien für welche Zwecke verarbeitet wurden;
- welchen Empfängern bzw. Empfängerkategorien die Daten offengelegt wurden;
- wie lange die Daten gespeichert werden;
- woher die Daten stammen;
- ob eine automatisierte Einzelentscheidung bzw. ein Profiling stattgefunden hat.

Den betroffenen Personen ist zudem auf Verlangen eine Kopie der verarbeiteten personenbezogenen Daten zur Verfügung zu stellen.

LDA kann die innerhalb der LDA-Systeme gespeicherten und einer betroffenen Person, einem Nutzerkonto oder einer Kundeninstanz zuordenbaren personenbezogenen Daten auf dokumentierte Anfrage des Kunden auslesen und dem Kunden in geeigneter Form bereitstellen. Berücksichtigt werden können insbesondere Identitäts- und Berechtigungsdaten, gespeicherte Eingaben und generierte Antworten, der zugehörige Verlauf sowie zuordenbare Protokoll- und Nutzungsdaten. Die Prüfung der Identität der betroffenen Person und die Beantwortung des Auskunftersuchens obliegen dem Kunden als Verantwortlichem.

### **2. Recht auf Berichtigung (Art. 16 DSGVO)**

Die betroffenen Personen können verlangen, dass unrichtige personenbezogene Daten unverzüglich berichtigt und – soweit der Zweck der Verarbeitung dies erfordert – unvollständige Daten ergänzt werden.

Der Anspruch richtet sich nicht gegen das eingesetzte KI-Modell, sondern gegen die gespeicherten Datenbestände. Berichtigungsfähig sind daher die Identitäts- und Berechtigungsdaten, die im Legal Data Hub gespeicherten Fachinhalte einschließlich der zugehörigen Textsegmente und Metadaten sowie gespeicherte Eingaben und Antworten. Stellt der Kunde einen Fachinhalt berichtigt erneut bereit, werden die zugehörigen Textsegmente und Vektoren neu erzeugt; die berichtigte Fassung ist damit auch für künftige Suchanfragen maßgeblich.

Generierte Antworten werden nicht dauerhaft als Aussage über eine bestimmte Person vorgehalten, sondern anlassbezogen erzeugt. Enthält eine gespeicherte Antwort eine unrichtige Aussage über eine betroffene Person, wird sie auf Weisung des Kunden gelöscht; eine Berichtigung des Modells ist

weder möglich noch erforderlich, da die Modelle nicht mit den Inhalten des Legal Data Hub trainiert werden.

### 3. **Recht auf Löschung (Art. 17 DSGVO)**

Die von der Verarbeitung betroffenen Personen können – soweit kein Ausschlussgrund nach Art. 17 Abs. 3 DSGVO und § 35 BDSG eingreift – die Löschung der sie betreffenden personenbezogenen Daten verlangen, wenn,

- die Daten für den Zweck, für den sie erhoben oder sonst verarbeitet wurden, nicht mehr benötigt werden;
- die Daten unrechtmäßig erhoben wurden;
- die Löschung zur Erfüllung einer Verpflichtung erforderlich ist.

Soweit personenbezogene Daten innerhalb der LDA-Systeme gespeichert und einer betroffenen Person, einem Nutzerkonto oder einer Kundeninstanz zugeordnet werden können, kann LDA diese auf dokumentierte Weisung des Kunden löschen. Die Löschung erfasst die zugehörigen abgeleiteten Daten, insbesondere Einbettungen, Verlaufseinträge und Cache-Inhalte. Wird ein Inhalt aus dem Legal Data Hub entfernt, werden die zugehörigen Textsegmente, Metadaten und Vektoren mitgelöscht; der Inhalt wird anschließend nicht mehr als Grundlage für die Antwortgenerierung herangezogen.

Löschungen im Produktivsystem schlagen mit dem Ablauf des Sicherungszyklus auf die Datensicherungen durch; bis dahin sind die betreffenden Daten in den Sicherungen gegen einen Zugriff im Regelbetrieb geschützt. Bestehen gesetzliche Aufbewahrungspflichten, insbesondere nach § 147 AO und § 257 HGB für abrechnungsbezogene Belege, oder ist eine unmittelbare Löschung technisch nicht möglich, wird die weitere Verarbeitung der betreffenden Daten eingeschränkt.

Bei Fachinhalten ist zu berücksichtigen, dass einer Löschung berechnigte Gegeninteressen entgegenstehen können, etwa das Recht auf freie Meinungsäußerung und Information nach Art. 17 Abs. 3 lit. a DSGVO. Die Abwägung obliegt dem Kunden als Verantwortlichem für die bereitgestellten Inhalte.

### 4. **Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)**

Von der Verarbeitung betroffene Personen können in den nachfolgend näher beschriebenen Fällen verlangen, dass die Verarbeitung der sie betreffenden personenbezogenen Daten eingeschränkt wird. Nach einer Einschränkung der Verarbeitung dürfen die Daten grundsätzlich nur noch gespeichert werden. Eine anderweitige Verarbeitung der Daten, deren Verarbeitung eingeschränkt wurde, ist nur in den Grenzen des Art. 18 Abs. 2 DSGVO zulässig, etwa im Rahmen von Rechtsstreitigkeiten oder mit Einwilligung des Nutzers.

Ein Anspruch auf Einschränkung der Verarbeitung besteht in folgenden Fällen:

- Die von der Verarbeitung betroffene Person bestreitet die Richtigkeit der über ihn gespeicherten Daten. Während die Richtigkeit geprüft wird, sind die Daten zu sperren.
- Die Verarbeitung ist unrichtig, die von der Verarbeitung betroffene Person verlangt aber statt einer Löschung zunächst nur die Sperrung.
- Die Daten werden für die ursprünglichen Zwecke nicht mehr benötigt, die von der Verarbeitung betroffene Person benötigt sie aber zur Rechtsausübung.

- Die von der Verarbeitung betroffene Person hat aufgrund seiner besonderen persönlichen Situation ein Widerspruchsrecht gegen die Verarbeitung seiner Daten ausgeübt. Während der Widerspruch geprüft wird, müssen die Daten gesperrt werden.

Der Kunde kann einzelne Nutzerkonten deaktivieren, Berechtigungen entziehen und einzelne Inhalte für die Suche sperren. Soweit eine Einschränkung bereits gespeicherter Daten erforderlich ist, unterstützt LDA den Kunden auf dokumentierte Weisung durch geeignete technische oder organisatorische Maßnahmen, insbesondere durch Kennzeichnung, Zugriffssperre oder Herausnahme aus dem Suchindex.

## 5. **Recht auf Datenübertragbarkeit (Art. 20 DSGVO)**

Die betroffenen Personen haben das Recht, die sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Sie haben zudem das Recht, die Daten einem Dritten zu übermitteln, ohne behindert zu werden; soweit technisch machbar, können sie die unmittelbare Übermittlung an einen Dritten verlangen.

Das Recht besteht nur, soweit die Verarbeitung automatisiert erfolgt, auf einer Einwilligung oder auf einem Vertrag beruht und die Daten von der betroffenen Person selbst bereitgestellt wurden. Es erfasst daher die Identitäts- und Berechtigungsdaten sowie die vom Nutzer eingegebenen Inhalte und den zugehörigen Verlauf. Nicht erfasst sind die im Legal Data Hub gespeicherten Fachinhalte, da deren Verarbeitung auf Art. 6 Abs. 1 lit. f DSGVO beruht und die Daten nicht von der betroffenen Person bereitgestellt wurden. Ebenfalls nicht erfasst sind die generierten Antworten, soweit sie nicht von der betroffenen Person bereitgestellt, sondern vom System abgeleitete Daten darstellen.

Soweit die gesetzlichen Voraussetzungen erfüllt sind und die Daten innerhalb der LDA-Systeme gespeichert werden, stellt LDA die einer betroffenen Person oder einem Nutzerkonto zuordenbaren Daten auf dokumentierte Anfrage des Kunden in einem strukturierten, gängigen und maschinenlesbaren Format bereit. Die konkrete Form richtet sich nach Art, Umfang und technischer Struktur der gespeicherten Daten.

## 6. **Recht auf Widerspruch (Art. 21 DSGVO)**

Soweit die Verarbeitung auf Art. 6 Abs. 1 lit. f DSGVO beruht, können betroffene Personen ihr aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit widersprechen. Der Verantwortliche verarbeitet die Daten dann nicht mehr, es sei denn, er weist zwingende schutzwürdige Gründe nach, die die Interessen der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Bei der Nutzung des LDA-Tools betrifft dies insbesondere

- die Indexierung und Bereitstellung von Fachinhalten, soweit darin personenbezogene Daten Dritter enthalten sind;
- die Protokollierung zu Zwecken der IT-Sicherheit, soweit sie über die Erfüllung der Pflichten aus Art. 32 DSGVO hinausgeht;
- die Verarbeitung zu Zwecken der Produktverbesserung, soweit LDA insoweit eigene Zwecke verfolgt.

Ein Widerspruch gegen die Verarbeitung zu Trainingszwecken kommt nicht in Betracht, da personenbezogene Daten der Nutzer und der Endkunden weder zum Training noch zur Feinabstimmung von KI-Modellen verwendet werden.

Widersprüche gegen die Indexierung von Fachinhalten sind an den Kunden als Verantwortlichen zu richten. Der Kunde prüft, ob dem Widerspruch zwingende schutzwürdige Gründe entgegenstehen; hierfür kommt insbesondere das Informationsinteresse der Allgemeinheit an der Zugänglichkeit veröffentlichter Rechtsprechung in Betracht.

### **III. Technische und organisatorische Maßnahmen**

Gemäß Art. 32 DSGVO sind angemessene technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko angemessenes Schutzniveau für die im Zusammenhang mit der Nutzung des LDA-Tools verarbeiteten personenbezogenen Daten zu gewährleisten. Zur Gewährleistung eines angemessenen Schutzniveaus hat LDA die nachfolgenden technischen und organisatorischen Maßnahmen ergriffen:

#### **1. Zutrittskontrolle (physische Sicherheit)**

- Betrieb der produktiven Systeme in geeigneten und zertifizierten Rechenzentren (z. B. ISO 27001).
- 24/7-Überwachung der Rechenzentren (Videoüberwachung, Sicherheitsdienst); die physische Sicherheit der Rechenzentren wird durch den eingesetzten, zertifizierten Hosting-Anbieter (insbesondere Microsoft Azure) gewährleistet.
- Dokumentierte Zutrittsregelungen und Besucherprotokollierung.
- Trennung von Büro- und Serverinfrastruktur.

#### **2. Zugangskontrolle (Systemzugang)**

- Personalisierte Benutzerkonten ohne gemeinsame Accounts.
- Starke Authentifizierungsverfahren (z. B. Multi-Faktor-Authentifizierung für Administrationszugänge).
- Passwort-Richtlinien (Komplexität, Mindestlänge, Rotation, sichere Speicherung mittels Hashverfahren).
- Automatische Sperrung bei Fehlversuchen.
- Verschlüsselte Verbindungen (TLS) für sämtliche externen und internen Zugriffe.

#### **3. Zugriffskontrolle (Berechtigungskonzept)**

- Rollen- und berechtigungsbasiertes Zugriffskonzept (RBAC).
- „Need-to-know“-Prinzip für Mitarbeiterzugriffe.
- Regelmäßige Überprüfung und Rezertifizierung von Berechtigungen.

#### **4. Authentifizierung und Autorisierung von API-Zugriffen**

- Nutzung sicherer Authentifizierungsmechanismen (z. B. OAuth2, Token-basierte Verfahren).
- Verwendung individueller Client-IDs und Secrets.

- Möglichkeit zur Rotation und Sperrung kompromittierter Zugangsdaten.
- Rate-Limiting, Throttling und Missbrauchserkennung.

## 5. Verschlüsselung

- Transportverschlüsselung (TLS 1.2 oder höher).
- Verschlüsselung sensibler Daten im Ruhezustand (Encryption-at-Rest).
- Verschlüsselte Datensicherungen.
- Sichere Schlüsselverwaltung mit Zugriffsbeschränkung.
- Getrennte Speicherung von Schlüsseln und verschlüsselten Daten.

## 6. Pseudonymisierung und Datenminimierung

- Verarbeitung personenbezogener Daten nur, soweit technisch erforderlich bzw. unvermeidbar.
- Logging ohne unnötige Speicherung vollständiger Inhaltsdaten.
- Speicher- und Löschfristen.

## 7. Weitergabekontrolle

- Zugriff externer Dienstleister nur auf vertraglicher Grundlage (Art. 28 DSGVO).
- Technische Absicherung von Schnittstellen.

## 8. Eingabekontrolle / Protokollierung

- Protokollierung sicherheitsrelevanter Ereignisse (Login, Konfigurationsänderungen, Admin-Zugriffe).
- Schutz der Logdaten vor Manipulation und unbefugtem Zugriff.
- Zeitlich synchronisierte Systeme (z. B. NTP).

## 9. Verfügbarkeitskontrolle

- Redundante Systemarchitektur.
- Monitoring von Systemzustand, Performance und Verfügbarkeit.
- Automatisierte Backups mit regelmäßiger Wiederherstellungstestung.
- Notfall- und Wiederanlaufpläne (Disaster-Recovery-Konzept).
- Schutz vor DDoS-Angriffen und anderen Verfügbarkeitsbedrohungen.

## 10. Integritätskontrolle

- Regelmäßige Sicherheitsupdates und Patch-Management.

- Einsatz von Code-Reviews und Sicherheitsprüfungen im Entwicklungsprozess.
- Trennung von Entwicklungs-, Test- und Produktionsumgebungen.
- Absicherung gegen unbefugte Veränderung von Konfigurationsdaten.

#### **11. Datentrennung**

- Getrennte Verarbeitung von Test- und Produktivdaten.
- Keine Vermischung von Auftragsdaten mit eigenen Daten des Auftragnehmers.

#### **12. Lösch- und Aufbewahrungskonzept**

- Dokumentiertes Löschkonzept entsprechend vertraglicher Vorgaben.
- Automatisierte Löschroutinen für Logs und Nutzungsdaten.
- Vollständige Löschung oder Rückgabe nach Vertragsende.

#### **13. Vertraulichkeit und Verpflichtung der Mitarbeiter**

- Verpflichtung aller Mitarbeiter auf Vertraulichkeit gemäß Art. 28 Abs. 3 DSGVO.
- Spezifische Verpflichtung nach § 203 StGB bei möglicher Verarbeitung von Berufsgeheimnissen.
- Regelmäßige Datenschutz- und IT-Sicherheitsschulungen.
- Dokumentierte Onboarding- und Offboarding-Prozesse.

#### **14. Sicherheit bei mobiler Arbeit / Telearbeit**

- Festplattenverschlüsselung auf mobilen Geräten.
- Bildschirm-Sperrmechanismen.
- Richtlinien zur sicheren Nutzung öffentlicher Netzwerke.

#### **15. Incident-Response-Management**

- Dokumentiertes Verfahren zur Behandlung von Sicherheitsvorfällen.
- Interner Meldeprozess für Datenschutzverletzungen.
- Bewertung und Klassifizierung von Vorfällen.
- Unterstützung des Auftraggebers bei Meldungen nach Art. 33, 34 DSGVO.
- Dokumentation sämtlicher Datenschutzvorfälle.

#### **16. Datenschutzmanagement und Compliance**

- Bestellung eines Datenschutzbeauftragten.
- Durchführung von Risikoanalysen.

- Regelmäßige interne Überprüfung der Wirksamkeit der TOMs.
- Möglichkeit des Nachweises durch Zertifikate, Auditberichte oder Testate.

#### **IV. Verletzungen des Schutzes personenbezogener Daten**

LDA unterhält einen dokumentierten Prozess zur Erkennung, Bewertung und Bearbeitung von Verletzungen des Schutzes personenbezogener Daten. Wird LDA eine solche Verletzung bekannt, meldet sie diese dem Kunden unverzüglich nach Art. 33 Abs. 2 DSGVO, spätestens innerhalb von 24 Stunden nach Kenntniserlangung.

Die Meldung enthält, soweit verfügbar, eine Beschreibung der Art der Verletzung, die betroffenen Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen und vorgeschlagenen Abhilfemaßnahmen. LDA unterstützt den Kunden bei der Erfüllung seiner Pflichten nach Art. 33 und 34 DSGVO.

Die Entscheidung über die Meldung an die Aufsichtsbehörde und über die Benachrichtigung der betroffenen Personen trifft der Kunde als Verantwortlicher. Soweit LDA eigene Verantwortliche ist, nimmt sie die Bewertung und Meldung selbst vor.

#### **V. Datenschutz-Folgenabschätzung**

Die Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO trifft den Verantwortlichen. LDA unterstützt den Kunden hierbei nach Art. 28 Abs. 3 lit. f DSGVO durch die Bereitstellung der erforderlichen Informationen, insbesondere durch dieses Datenschutzkonzept.

Der Einsatz des LDA-Tools erfüllt nicht ohne Weiteres die Kriterien der Muss-Liste der deutschen Aufsichtsbehörden. Für eine Pflicht zur Durchführung kann jedoch sprechen, dass innovative Technologie eingesetzt wird und dass in erheblichem Umfang Daten verarbeitet werden können, die dem Berufsgeheimnis unterliegen oder besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO darstellen. Der Kunde und der Endkunde haben die Erforderlichkeit daher eigenständig zu prüfen und das Ergebnis zu dokumentieren.

#### **VI. Berufsgeheimnis und § 203 StGB**

Berufsträger der steuer-, wirtschafts- und rechtsberatenden Berufe sind zur Verschwiegenheit über alle Informationen, die ihnen in Ausübung ihres Berufs bekannt geworden und nicht offenkundig sind, verpflichtet (§ 43a BRAO, § 57 StBerG, u.a.). Die Verschwiegenheit von Beratern ist wesentliche Grundlage einer vertrauensvollen Zusammenarbeit von Mandanten und Berufsträgern. Die Verpflichtung zur Verschwiegenheit betrifft zudem alle von Berufsträgern beschäftigten oder sonst für diese tätigen Personen und eingesetzten externen Dienstleister (§ 43e BRAO, §§ 62, 62a StBerG, u.a.).

Berufsträger dürfen danach Dienstleistern Tatsachen, auf die sich die Verschwiegenheitsverpflichtungen beziehen, nur offenbaren, wenn die Offenbarung zur Inanspruchnahme der Dienstleistungen erforderlich ist (§ 43e Abs. 1 BRAO), der Dienstleister sorgfältig ausgewählt, in Textform zur Verschwiegenheit entsprechend den berufsrechtlichen Anforderungen verpflichtet, über die strafrechtlichen Folgen einer Pflichtverletzung belehrt (§ 203 StGB) und verpflichtet wurde, sich nur insoweit Kenntnis von Tatsachen und damit fremden Geheimnissen zu verschaffen, soweit dies für die Erfüllung des Vertrags erforderlich ist und nur weitere Dienstleister oder Personen zur Erfüllung des Vertrags heranzuziehen, soweit ihm dies gestattet und auferlegt wurde, auch diese Personen und Dienstleister zur Verschwiegenheit zu verpflichten.

Berufsträger haben daher vor der Offenlegung von der Verschwiegenheitsverpflichtung unterliegenden Tatsachen und Informationen zu prüfen, ob der konkrete Dienstleister die berufsrechtlichen Voraussetzungen und die strafbefreienden Tatbestandsvoraussetzungen für den Einsatz zum Zwecke der Berufsausübung durch den Berufsträger erfüllt.

Die Nutzung von KI-Systemen durch Berufsträger kann unter Umständen die Offenlegung von Informationen („*fremde Geheimnisse*“) bedingen, die strengen rechtlichen, insbesondere berufsrechtlichen Anforderungen unterliegen. LDA ist ein geeigneter Dienstleister im Sinne von § 43e BRAO, § 62a BRAO u.a., sodass fremde Geheimnisse gegenüber LDA nicht „*unbefugt offenbart*“ werden. LDA erfüllt nachhaltig und konsequent die Anforderung zur Verarbeitung personenbezogener Daten und „*fremder Geheimnisse*“, die Berufsträger in Ausübung ihres Berufs erlangt haben.

LDA ist ein Dienstleister, der die berufs-, datenschutz- und strafrechtlichen Anforderungen bereits bei der Entwicklung und Bereitstellung der KI-Systeme berücksichtigt und strukturell in der Unternehmens- und Systemarchitektur verankert hat. Berufsträger, die in eigener Verantwortung ausschließlich erforderliche Informationen offenbaren, können darauf vertrauen, dass die Nutzung des Legal Data Hub den Compliance-Anforderungen entspricht.