Anlage I zum Auftragsverarbeitungsvertrag
Technische und Organisatorische Maßnahmen Noxtua (TOM)

einschließlich zur Gewährleistung der Sicherheit der Daten

1. ORGANISATION

1.1 Der Provider muss dem Kunden auf Anfrage eine aktuelle, vom Management genehmigte und veröffentlichte Informationssicherheitsrichtlinie vorlegen.

1.2 Der Provider muss auf Wunsch vom Kunden eine Person inklusive Kontaktdaten benennen, die für die Informationssicherheit verantwortlich ist.

1.3 Der Provider hat Jasmin Muhmenthaler-Sturm, der Datenschutzbeschützerin GmbH mit Sitz in Regen, als externe Datenschutzbeauftragte bestellt. Sie ist unter der Adresse Unterer Sand 9, 94209 Regen erreichbar und kann per E-Mail an info@datenbeschuetzerin.de oder via Telefonnummer: 09921 88229000 kontaktiert werden. Die Datenschutzbeauftragte arbeitet eng mit dem internen Beauftragten für Informationssicherheit.

2. ASSET MANAGEMENT

2.1 Der Provider hat ein vollständiges Verzeichnis der kritischen Assets, die im Rahmen der Dienstleistung relevant sind, zu führen. Dies umfasst insbesondere sämtliche Hardware, Software, Cloud-Dienste und Daten. Erfasst werden zudem die für die Erbringung der Dienstleistung eingesetzten KI-Basismodelle (selbst-gehostete Open Source-Modelle oder closed-source Frontier-Modelle) einschließlich ihrer jeweiligen Modellkategorie (Ziffer 19), ihres Bezugswegs und ihres Betriebsorts.

2.2 Der Provider muss mindestens jährlich überprüfen, ob das Asset-Verzeichnis aktuell, vollständig und genau ist.

3. PHYSISCHE SICHERHEIT

3.1 Die Sicherheit der Standorte, an denen Dienstleistungen für den Kunden erbracht werden, ist von höchster Bedeutung für den Provider. Um unbefugten physischen Zutritt, Beschädigung oder Veränderung von Kundendaten und den dazugehörigen Systemen und Einrichtungen vorzubeugen, hat der Provider umfassende Maßnahmen zur Zutrittskontrolle implementiert. Diese Maßnahmen sind nach ISO 27001 zertifiziert und gewährleisten, dass nur autorisiertes Personal Zugang zu sensiblen Bereichen hat.

3.2 Die Einrichtung von Sicherheitszonen mit eingeschränktem Zugang ist ein zentraler Aspekt dieser Sicherheitsstrategie. Diese Zonen sind so konzipiert, dass nur bestimmte qualifizierte Mitarbeiter Zugang haben. Schlüssel werden nur an diese autorisierten Mitarbeiter ausgegeben, und es wird sorgfältig protokolliert, wer wann Zugang zu diesen Bereichen hat.

3.3 Darüber hinaus wurde eine klar definierte Anmeldezone eingerichtet, in der Besucher registriert und empfangen werden. Besucher dürfen sich nur in bestimmten, überwachten Bereichen aufhalten und werden durchgehend überwacht, um ihre Anwesenheit zu protokollieren und ihre Aktivitäten zu verfolgen.

3.4 Die physischen Sicherheitsmaßnahmen werden durch Alarmanlagen und eine Rund-um-die-Uhr-Videoüberwachung ergänzt, die eine zusätzliche Abschreckung für potenzielle Eindringlinge darstellen und es ermöglichen, auf Vorfälle zu reagieren. Um einen detaillierten Überblick zu gewährleisten, werden Besucher-Logs geführt, in denen alle ein- und ausgehenden Besucher erfasst werden, einschließlich ihrer Ankunfts- und Abgangszeiten.

3.5 Durch diese mehrschichtigen Sicherheitsvorkehrungen stellt der Provider sicher, dass der physische Zugang zu sensiblen Bereichen streng kontrolliert und überwacht wird, wodurch die Vertraulichkeit und Integrität der Kundendaten aufrechterhalten wird. Diese Maßnahmen sind

Teil des umfassenden Engagements des Providers, die höchsten Sicherheitsstandards einzuhalten und die Daten seiner Kunden zu schützen.

4. HUMAN RESOURCE SICHERHEIT

4.1 Alle Mitarbeiter des Providers müssen auf ihre Sicherheitsverantwortung bei der Handhabung und/oder Verarbeitung von Kundendaten aufmerksam gemacht werden und regelmäßig (mindestens einmal jährlich) Schulungen zum Sicherheitsbewusstsein und zum Datenschutz erhalten.

5. ACCOUNT UND ACCESS MANAGEMENT

5.1 Benutzerkonten, die Zugang zu Systemen und Zugriff auf Kundendaten/Anwendungen ermöglichen, müssen eindeutig einzelnen Personen zugewiesen sein. Benutzerkonten dürfen nicht von mehreren Personen genutzt werden.

5.2 Privilegierte Konten sind auf eine kleine Anzahl geeigneter, qualifizierter und autorisierter Personen zu beschränken. Solche Konten dürfen nicht für „alltägliche“ Aktivitäten genutzt werden.

5.3 Berechtigungen sind regelmäßig zu überprüfen, um sicherzustellen, dass nur geeignete Personen Zugang haben und eine angemessene Aufgabentrennung besteht. Administrative Berechtigungen sind vierteljährlich zu überprüfen.

5.4 Der Provider stellt sicher, dass der Fernzugriff auf Systeme, die Kundendaten verarbeiten und/oder speichern, nur autorisiertem Personal gewährt wird und einer Mehrfaktor-Authentifizierung („MFA“) unterliegt.

5.5 Der Provider stellt sicher, dass für administrative Zugriffe eine MFA erzwungen wird, unabhängig davon, von wo sie erfolgen.

5.6 Clients werden nach einer definierten Zeit der Inaktivität automatisch gesperrt, um unbefugten Zugriff zu verhindern. Um die Sicherheit weiter zu erhöhen, erfordert der Entsperrvorgang die Autorisierung durch zwei unabhängige Administratoren, die das Vier-Augen-Prinzip einhalten. Auf diese Weise wird sichergestellt, dass der Zugriff auf sensible Informationen angemessen kontrolliert und überwacht wird.

5.7 Der Provider setzt umfassende Sicherheitsmaßnahmen für mobile Arbeitsgeräte um, um die Vertraulichkeit und Sicherheit der darauf gespeicherten Informationen zu gewährleisten. Dazu verpflichtet der Provider alle Mitarbeiter, Sichtschutzfolien auf ihren mobilen Geräten anzubringen, um unbefugte Einblicke zu verhindern. Zusätzlich wird die Verwendung virtueller privater Netzwerke (VPNs) vorgeschrieben, um eine sichere und verschlüsselte Verbindung bei der Remote-Arbeit herzustellen. Diese Maßnahmen stellen sicher, dass vertrauliche Informationen auch außerhalb des Büros geschützt sind.

5.8 Der Provider setzt ein robustes Eingabekontrollsystem ein, das durch ein umfassendes Dokumentenmanagement-System (DMS) im gesamten Unternehmen ergänzt wird. Dieses DMS ermöglicht eine lückenlose Änderungshistorie und bietet eine Fülle von Vorteilen. Es gewährleistet, dass alle Änderungen an Dokumenten und Dateien nachvollziehbar sind, indem es detaillierte Informationen zu Änderungen, Autorennamen und Zeitstempeln bereitstellt. Das System erleichtert die Versionskontrolle und ermöglicht es Benutzern, auf vorherige Versionen zuzugreifen und Änderungen im Zeitverlauf zu vergleichen. Darüber hinaus bietet das DMS eine sichere Speicherung und den sicheren Austausch von Informationen innerhalb des Unternehmens, wodurch die Zusammenarbeit verbessert und das Risiko von Datenverlusten reduziert wird. Durch die Verwendung dieses DMS mit Änderungshistorie verbessert der Provider die Transparenz und Nachverfolgbarkeit von Änderungen und stärkt so die Sicherheit und Integrität der Daten.

6. PASSWORT MANAGEMENT

6.1 Der Provider muss eine angemessene Passwortrichtlinie einführen. Der Provider stellt hierbei sicher, dass sämtliche Mitarbeiter 2-Faktor-Authentifizierung beim Zugriff auf alle IT-Systeme benutzen müssen. Dies ist vom System Administrator erzwungen.

6.2 Der Provider stellt sicher, dass alle Mitarbeiter ein sicheres Passwort-Management-System verwenden, das strenge Authentifizierungsverfahren erfordert. Das System generiert komplexe Passwörter, die den aktuellen Empfehlungen für Passwortsicherheit entsprechen, und speichert sie sicher. Um die Benutzerfreundlichkeit zu erhöhen, ermöglicht der Provider, wo immer möglich, die Verwendung von Single Sign-On (SSO)-Lösungen, wodurch die Notwendigkeit mehrerer Passwörter reduziert wird und ein sicherer und effizienter Zugang zu den erforderlichen Tools gewährleistet wird. Diese Maßnahme trägt dazu bei, die Sicherheit der Konten zu erhöhen und das Risiko unbefugten Zugriffs zu verringern.

7. NETZWERKSICHERHEIT

7.1 Der Provider stellt sicher, dass alle Systeme, die Kundendaten verarbeiten und/oder speichern und vom Provider oder seinen Subunternehmern betrieben werden, vor Bedrohungen aus dem Netzwerk angemessen geschützt sind.

7.2 Der Provider muss ein aktuelles Inventar aller Netzgrenzen der Organisation führen (z. B. anhand eines Netzwerkdiagramms) und die Netze durch die Anwendung üblicher Schutzarchitekturen schützen (z. B. Netzsegmentierung, Firewalls, physische Zugangskontrollen zu Netzkomponenten usw.).

8. VERSCHLÜSSELUNG

8.1 Zum Schutz von Kundendaten muss der Provider Verschlüsselungen nach Industriestandards (z.B. AES-256, RSA-2048) bei der Übertragung (in-transit) und Speicherung (at-rest) implementieren. Dies umfasst mindestens:

8.1.1 Datenspeicherung (at-rest) auf mobilen Geräten wie Laptops, Mobiltelefone, Tablets, Wechselmedien,

8.1.2 Datenzugriff (in-transit) auf Dateifreigaben, Datenbanken und Cloud-Speicher und

8.1.3 Übertragungsmethoden (in-transit) wie z. B. E-Mail, Dateifreigaben, VPNs, drahtlose Übertragungen.

8.2 Für die persistente Speicherung von Kundendaten im LECS-System (Live Encrypted Cloud Storage) setzt der Provider zusätzlich folgende Verschlüsselungsmaßnahmen ein: Alle sensiblen Inhalte – einschließlich Chat-Nachrichten, hochgeladener Dateien und Dateinamen – werden vor der Übertragung an das Speichersystem verschlüsselt. Die Verschlüsselung erfolgt mittels XChaCha20Poly1305 (Authenticated Encryption with Associated Data) mit symmetrischen 256-Bit-Schlüsseln, die individuell pro Projekt (z. B. je Konversation) generiert werden. Schlüssel werden mittels CSPRNG erzeugt. Die Nonce wird für jede Verschlüsselungsoperation frisch und zufällig generiert (192 Bit). Jeder verschlüsselte Datensatz ist durch Additional Authenticated Data (AD) kontextgebunden (Mandanten-ID, Nutzer-ID, Projekt-ID, Datei-ID). Die Schlüsselverwaltung erfolgt über einen dedizierten, gehärteten Unlock Key Vault; die Entschlüsselung des Keyrings erfolgt ausschließlich im Browser des Nutzers. Projektschlüssel werden dem Backend nur für die Dauer der jeweiligen Anfrage bereitgestellt und danach sofort verworfen (ephemeraler Schlüsselzugriff). Klarstellend umfasst der Verschlüsselungsumfang auch die KI-generierten Antworten beider Modellkategorien (Ziffer 19). Der Zugriff auf den Unlock Key Vault erfordert eine Dual-IDP-Authentifizierung. Dies umfasst eine Authentifizierung sowohl gegenüber dem Noxtua-IDP als auch gegenüber dem Mandanten-IDP (z. B. Beck-IDP). Eng begrenzte betriebliche Metadaten (z. B. Zugriffsmuster, Dateigröße, zufällig generierte IDs und strukturelle Pfadpräfixe) verbleiben aus Betriebsgründen im Klartext; sie enthalten keine Mandanteninhalte oder personenbezogenen Daten und unterliegen denselben Mandantengrenzen und Zugriffskontrollen wie die verschlüsselten Inhalte.

9. SYSTEMBESCHAFFUNG, ENTWICKLUNG UND PFLEGE

9.1 Der Provider muss über einen sicheren Entwicklungsprozess verfügen, um Sicherheitsvorfälle zu verhindern und um Schwachstellen im Code während des Entwicklungsprozesses zu identifizieren und zu beheben. Alle Anwendungen, die Kundendaten verarbeiten und/oder speichern, müssen vor der Freigabe anhand geeigneter Standards, wie z. B. OWASP Secure Coding, getestet und validiert werden.

9.2 Um die Sicherheit und Zuverlässigkeit der Softwareentwicklung zu gewährleisten, setzt der Provider auf eine robuste Continuous Integration (CI) und Continuous Deployment (CD) Pipeline. Dieser sichere CI/CD-Prozess umfasst mehrere Stufen, darunter Test, Staging und Deployment. Während der Testphase werden automatisierte Tests durchgeführt, um sicherzustellen, dass der Code den Qualitäts- und Sicherheitsstandards entspricht. Diese Tests umfassen Unit-Tests, Integrationstests und Sicherheitsüberprüfungen, um potenzielle Schwachstellen frühzeitig zu identifizieren. Nach erfolgreichem Abschluss der Testphase wird der Code in einer Staging-Umgebung bereitgestellt, die der Produktionsumgebung ähnelt. In dieser Phase werden abschließende Tests durchgeführt, um sicherzustellen, dass die Software wie erwartet funktioniert und mit der Infrastruktur kompatibel ist. Nach der erfolgreichen Validierung in der Staging-Umgebung erfolgt das Deployment, wobei der Code in die Produktionsumgebung freigegeben wird. Dieser Prozess wird durch strenge Zugriffskontrollen und Versionskontrolle ergänzt, um die Integrität des Codes während jeder Phase zu gewährleisten. Durch diese sichere CI/CD-Pipeline wird sichergestellt, dass nur vollständig getesteter und validierter Code in die Produktionsumgebung gelangt, wodurch die Zuverlässigkeit und Sicherheit der Software gewährleistet wird.

9.3 Um die Sicherheit der Softwarebeschaffung und -entwicklung zu gewährleisten, setzt der Provider auf einen rigorosen Prozess. Dieser Prozess beginnt mit der Bestimmung klarer Verantwortlichkeiten und der Benennung verantwortlicher Ansprechpartner, sowohl intern als auch bei externen Auftragnehmern. Durch diese klare Zuordnung wird sichergestellt, dass während des gesamten Beschaffungs- und Entwicklungsprozesses konsequent sichere Praktiken angewendet werden. Regelmäßige Kontrollen und Überprüfungen der weisungsgebundenen Auftragsdurchführung stellen sicher, dass externe Anbieter die vereinbarten Datenschutz- und Sicherheitsstandards einhalten. Um die Unabhängigkeit und Objektivität zu gewährleisten, werden regelmäßige unabhängige Audits durchgeführt, um die Einhaltung der vereinbarten Weisungen zu überprüfen. Dieser Prozess umfasst auch die Überprüfung der Sicherheitsmaßnahmen, der Datenschutzpraktiken und der allgemeinen Compliance mit den geltenden Vorschriften. Durch diese proaktiven Maßnahmen wird sichergestellt, dass die beschafften Systeme und Softwarekomponenten den Sicherheits- und Datenschutzanforderungen entsprechen und dass alle Beteiligten während des gesamten Lebenszyklus der System- und Softwarebeschaffung verantwortungsvoll handeln.

9.4 Der Provider erbringt die wesentlichen Bestandteile der Dienstleistung, insbesondere die Anwendung selbst, die kuratierte Datenbasis, die Datenhaltung, die Verschlüsselung und die Schlüsselverwaltung, mit eigenen Ressourcen auf einer von ihm kontrollierten Infrastruktur. Soweit einzelne Leistungsbestandteile, insbesondere die Bereitstellung von Basismodellen für die Inferenz (Ziffer 19), durch externe Dienstleister erbracht werden, gilt Folgendes:

(a) Der Provider führt ein aktuelles Verzeichnis aller eingesetzten Unterauftragsverarbeiter einschließlich deren Unterauftragsverarbeiter und stellt es dem Kunden auf Anfrage zur Verfügung. Änderungen werden dem Kunden in der vertraglich vereinbarten Form vorab angezeigt.

(b) Der Provider verpflichtet die eingesetzten Dienstleister vertraglich auf ein Schutzniveau, das dem dieser Anlage entspricht, und gibt die Verpflichtung zur Verschwiegenheit nach § 203 StGB entlang der gesamten Kette weiter.

(c) Der Provider wählt die Dienstleister sorgfältig aus, prüft deren technische und organisatorische Maßnahmen vor der Beauftragung und überwacht deren Einhaltung fortlaufend, mindestens jährlich.

(d) Der Einsatz externer Dienstleister erfolgt so, dass die Verarbeitung ausschließlich innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums oder der Schweiz stattfindet, für die ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt.

9.5 Der Provider stellt sicher, dass vor dem Einsatz eines neuen Basismodells sowie bei Änderung des Bezugswegs eines bereits eingesetzten Basismodells ein dokumentiertes Freigabeverfahren durchlaufen wird. Im Rahmen dieses Freigabeverfahren prüft und dokumentiert der Provider mindestens den Betriebsort, die Vertrags- und Weisungskette einschließlich der Verschwiegenheitsverpflichtung, die Speicher- und Protokollierungseinstellungen des jeweiligen Anbieters (insbesondere der Ausschluss einer Nutzung zu Trainingszwecken und der Ausschluss einer Speicherung auf der Inferenzebene) sowie die Auswirkungen auf die Maßnahmen dieser Anlage. Das Ergebnis wird versioniert festgehalten und dem Kunden auf Anfrage vorgelegt.

10. CHANGE MANAGEMENT

10.1 Um alle Änderungen an Systemen zu kontrollieren, die Kundendaten verarbeiten und/oder speichern, stellt der Provider sicher, dass formale Zuständigkeiten und Verfahren für das Change Management etabliert sind.

11. VERFÜGBARKEITSKONTROLLE

11.1 Der Provider implementiert robuste Sicherheitsmaßnahmen, um Systeme und Netzwerke, die Kundendaten verarbeiten und/oder speichern, vor bösartigem Code und Malware zu schützen. Dazu werden alle Server und Clients mit fortschrittlichen Viren- und Malware-Schutzsystemen ausgestattet, die in der Lage sind, Bedrohungen in Echtzeit zu erkennen und abzuwehren. Diese Schutzsysteme werden regelmäßig aktualisiert, um sicherzustellen, dass sie gegen die neuesten Bedrohungen gewappnet sind, und sie unterliegen regelmäßigen Sicherheitsüberprüfungen, um ihre Wirksamkeit zu gewährleisten. Durch diese proaktiven Maßnahmen wird sichergestellt, dass Kundendaten vor schädlichen Angriffen geschützt sind.

11.2 Alle Sicherheitssysteme, einschließlich Viren- und Malware-Schutzprogramme, unterliegen einem rigorosen Update-Prozess. Updates werden automatisch und regelmäßig eingespielt, um sicherzustellen, dass die Systeme mit den neuesten Sicherheitsverbesserungen und -patches ausgestattet sind. Durch diese proaktive Update-Strategie werden Schwachstellen minimiert und die Systeme vor bekannten Sicherheitsbedrohungen geschützt.

11.3 Um auf mögliche Notfallszenarien vorbereitet zu sein, hat der Provider einen umfassenden Notfallplan entwickelt und erfolgreich getestet. Dieser Plan umfasst verschiedene Szenarien, wie beispielsweise Cyber-Angriffe, Naturkatastrophen oder technische Ausfälle, und beschreibt detailliert die Schritte, die im Falle eines Notfalls einzuleiten sind. Regelmäßige Notfallübungen gewährleisten, dass das Personal mit den Verfahren vertraut ist und dass der Plan effektiv ist.

11.4 Darüber hinaus hat der Provider ein robustes Sicherheitskonzept für Software- und IT-Anwendungen implementiert. Dazu gehört die Verwendung sicherer Programmierpraktiken, die regelmäßige Durchführung von Sicherheitsaudits und die Einhaltung bewährter Praktiken bei der Softwareentwicklung. Durch diese Maßnahmen wird sichergestellt, dass die Anwendungen sicher sind und die Vertraulichkeit und Integrität der verarbeiteten Daten gewahrt bleibt.

11.5 Um Datenverluste zu verhindern, hat der Provider zuverlässige Back-up-Verfahren etabliert. Daten werden regelmäßig an sicheren, externen Standorten gesichert, um ihre Verfügbarkeit im Falle von Systemausfällen zu gewährleisten. Darüber hinaus werden Daten im gesicherten Netzwerk gespeichert, wobei der Zugriff streng kontrolliert wird. Um die Redundanz zu erhöhen, werden Festplatten gespiegelt, wodurch die Widerstandsfähigkeit des Systems gegen Ausfälle verbessert wird.

11.6 Im Falle von Brand- oder Löschwasserschäden hat der Provider vorbeugende Maßnahmen ergriffen. Dazu gehören feuerfeste Einrichtungen, automatische Brandschutzsysteme und

Löschwasserschutzmechanismen. Diese Maßnahmen minimieren das Risiko von Schäden an den Systemen und gewährleisten den fortlaufenden Schutz der gespeicherten Daten.

12. TECHNISCHE SICHERHEITSÜBERPRÜFUNGEN

12.1 Der Provider verpflichtet sich (auf eigene Kosten), regelmäßig eine unabhängige qualifizierte Prüforganisation mit der Durchführung von Penetrationstests an den Systemen des Providers zu beauftragen, die zur Erbringung von Dienstleistungen für den Kunden verwendet werden.

13. TRENNUNGSGEBOT

13.1 Um die Vertraulichkeit und Integrität der Daten verschiedener Mandanten oder Kunden in einem Cloud-basierten Multi-Tenant-System zu gewährleisten, implementiert der Provider eine robuste Mandantentrennung auf logischer Ebene. Jeder Mandant wird innerhalb der Cloud-Umgebung logisch getrennt, wobei der Zugang zu sensiblen Informationen streng kontrolliert wird. Durch die Verwendung von Zugriffsberechtigungen, Verschlüsselungstechniken und sicheren Datenbanken wird sichergestellt, dass die Daten verschiedener Mandanten voneinander isoliert sind. Dieser Ansatz ermöglicht eine sichere und effiziente Nutzung gemeinsamer Ressourcen, während gleichzeitig die Vertraulichkeit gewahrt bleibt.

13.2 Zusätzlich zu diesen logischen Trennmaßnahmen werden Test- und Produktivsysteme strikt voneinander getrennt. Die Testumgebung ist vollständig isoliert und hat keine Auswirkungen auf die tatsächlichen Produktivdaten. Dieser Ansatz ermöglicht sicheres Testen und Entwickeln, ohne das Risiko, dass vertrauliche Informationen offengelegt werden.

13.3 Der Provider speichert Kundendaten im LECS-System (Live Encrypted Cloud Storage) verschlüsselt auf der Cloud-Infrastruktur der Open Telekom Cloud (OBS/OTC) innerhalb der EU. Die Speicherung erfolgt projektbasiert: Jedes Projekt (z. B. jede Konversation) verfügt über einen eigenen kryptographischen Schlüssel (256-Bit, XChaCha20Poly1305). Eine kryptographische Mandantentrennung ist damit auf Projektebene gewährleistet. Die Aufbewahrungsdauer wird durch den jeweiligen Kunden konfiguriert (Minimum: 8 Stunden nach Sitzungsende). Nach Ablauf der konfigurierten Frist werden die Daten automatisiert und unwiderruflich gelöscht. Während der aktiven Verarbeitung werden Projektschlüssel dem Backend nur für die Dauer der jeweiligen Anfrage übergeben und anschließend sofort verworfen. Die Server-Infrastruktur und der Code unterliegen regelmäßigen Sicherheitsüberprüfungen und Audits. Die Speicherung erfolgt ausschließlich in Rechenzentren innerhalb der EU sowie der Schweiz (SwissOTC); für die Schweiz besteht ein datenschutzrechtlicher Angemessenheitsbeschluss der EU-Kommission. Eine Übermittlung in sonstige Drittländer findet nicht statt. Diese Ziffer betrifft die Speicherung der Kundendaten. Für die Verarbeitung im Rahmen der Modellinferenz gilt ergänzend Ziffer 19; auch dort erfolgt die Verarbeitung ausschließlich innerhalb der EU und der Schweiz.

13.4 Die Zuordnung von Mitarbeitern zu bestimmten Server- oder Code-Verantwortlichkeiten folgt strengen Richtlinien. Mitarbeiter haben nur Zugriff auf die Systeme und Codeabschnitte, die für ihre spezifischen Aufgaben erforderlich sind, und alle Zugriffsanfragen werden gründlich geprüft und autorisiert. Durch diese Maßnahmen wird sichergestellt, dass die Serverumgebung und der Code sicher und vertraulich behandelt werden.

13.5 Die kryptographische Trennung im LECS-System gewährleistet zusätzlich zur logischen Mandantentrennung (Ziffer 13.1), dass selbst bei einer Kompromittierung des Speichersystems nur Daten eines einzelnen Projekts betroffen sein können. Dies wird erreicht durch: (i) individuelle 256-Bit-Verschlüsselungsschlüssel pro Projekt; (ii) kontextgebundene Verschlüsselung mittels Additional Authenticated Data (Mandanten-ID, Nutzer-ID, Projekt-ID, Datei-ID); (iii) Schlüsselverwaltung über einen dedizierten, gehärteten Unlock Key Vault, der vom übrigen Noxtua-Backend getrennt betrieben wird.

14. SCHWACHSTELLENMANAGEMENT

14.1 Der Provider hat technische Schwachstellen zu identifizieren und Techniken einzusetzen, um diese in geeigneter Weise zu reduzieren oder zu beseitigen (z.B. Sicherheitspatches, Konfigurationsänderungen, abschwächende Kontrollen).

14.2 Der Provider stellt sicher, dass alle Systeme, die Kundendaten speichern, übertragen oder verarbeiten, regelmäßig Schwachstellen-Scans unterzogen werden:

14.2.1 Mindestens vierteljährlich und

14.2.2 unmittelbar nach jeder wesentlichen Systemänderung oder Softwarecode-Aktualisierung.

14.3 Der Provider verwendet zur Prioritätseinstufungen der Schwachstellenbehebung die Einstufung gemäß Common Vulnerability Scoring System („CVSS“) und behebt die Schwachstellen innerhalb folgender Fristen:

14.3.1 Einstufung als kritisches Risiko innerhalb von 7 Tagen,

14.3.2 Einstufung als hohes Risiko innerhalb von 14 Tagen,

14.3.3 Einstufung als mittleres Risiko innerhalb von 30 – 45 Tagen,

14.3.4 Einstufung als geringes Risiko innerhalb von 90 Tagen.

15. PROTOKOLLIERUNG

15.1 Der Provider hat vollständige und genaue Protokollierungen darüber zu führen, wo auf Kundendaten in den Systemen des Providers zugegriffen wurde. Mindestens muss nachvollziehbar sein, welche Person auf die Daten zugegriffen und/oder sie verändert hat, wann diese Zugriffe/Veränderungen (Datum und Uhrzeit) erfolgten sowie wann An- und Abmeldevorgänge stattfanden.

15.2 Der Provider stellt sicher, dass die o.g. Protokollierungen mindestens sechs Monate lang aufbewahrt werden.

15.3 Der Provider protokolliert je Anfrage, welche Modellkategorie nach Ziffer 19 für deren Verarbeitung verwendet wurde. Diese Protokolle enthalten keine Inhalte der Ein- oder Ausgaben. Der Kunde erhält auf Anfrage Auskunft aus diesen Protokollen.

16. SICHERHEITSVORFÄLLE

16.1 Der Provider muss ein dokumentiertes Verfahren zur Sicherheitsvorfallbehandlung etablieren.

16.2 Der Provider stellt sicher, dass das Verfahren zur Sicherheitsvorfallbehandlung mindestens einmal jährlich getestet und ggf. aktualisiert wird.

17. DATENAUFBEWAHRUNG / -LÖSCHUNG / -VERNICHTUNG

17.1 Der Provider muss folgende Verfahren im Rahmen der Datenaufbewahrung/-löschung etablieren:

(a) Verfahren, die es ermöglichen, Daten nach einem festgelegten Zeitplan zu löschen/zu aktualisieren,

(b) Verfahren, die eine unwiderrufliche Löschung oder Rückgabe der Daten an den Kunden bei Beendigung/Beendigung des Vertrags ermöglichen und

(c) Verfahren, die sicherstellen, dass personenbezogene Daten, die bei der Erbringung der Dienstleistungen des Providers an den Kunden über Fernzugriff oder andere Mittel heruntergeladen werden, nach Gebrauch gelöscht werden.

17.2 Der Provider stellt sicher, dass Kundendaten auf Anweisung vom Kunden durch geeignete Methoden (dreimaliges Überschreiben, Entmagnetisierung oder physische Vernichtung) sicher vernichtet werden. Diese Anforderung gilt sowohl während als auch am Ende der Vertragslaufzeit.

17.3 Der Provider stellt sicher, dass alle Daten entweder zurückgegeben oder wie mit dem Kunden vereinbart vernichtet wurden, und stellt einen Prüfpfad zur Verfügung, der dies belegt, z.B. in Form von Vernichtungszertifikaten.

17.4 Der Provider gewährleistet die Sicherheit des Datentransports durch die Implementierung mehrerer Sicherheitsmaßnahmen. Dazu gehört die Verwendung von verschlüsselten Containern und die Zusammenarbeit mit vertrauenswürdigen Kurierdiensten, die speziell für den sicheren Transport sensibler Informationen ausgebildet sind. Alle physischen Datenträger, einschließlich Laptops, externer Festplatten und USB-Sticks, sind mit starken Verschlüsselungsprotokollen geschützt, um die Vertraulichkeit der Daten während des Transports zu gewährleisten. Um die Authentizität und Integrität der Daten zu gewährleisten, werden elektronische Signaturen verwendet, wodurch die Empfänger die Integrität der erhaltenen Informationen überprüfen können. Darüber hinaus setzt der Provider ein robustes Mobile Device Management-System (MDM) ein, das es ermöglicht, mobile Geräte zu lokalisieren, zu überwachen und erforderlichenfalls remote zu löschen, wodurch das Risiko von Datenverlusten oder unbefugtem Zugriff minimiert wird. Durch diese umfassenden Maßnahmen stellt der Provider sicher, dass Daten während des Transports geschützt sind und die höchsten Sicherheitsstandards eingehalten werden.

17.5 Für die im LECS-System gespeicherten Kundendaten hat der Provider ein automatisiertes Aufbewahrungs- und Löschkonzept implementiert:

(a) Die Aufbewahrungsfrist ist je Mandant (Organisation) durch den Kunden konfigurierbar über eine Administrationsoberfläche. Die Mindestfrist beträgt 8 Stunden nach Sitzungsende. Standardmäßig ist eine unbegrenzte Aufbewahrung aktiv; eine achtstündige Aufbewahrung wird ausschließlich auf ausdrücklichen Kundenwunsch eingerichtet. Unabhängig von der gewählten Aufbewahrungsdauer können einzelne Chats jederzeit manuell durch die Nutzer gelöscht werden.

(b) Die Löschung erfolgt automatisiert und richtliniengesteuert. Der Provider erstellt revisionssichere Audit-Protokolle über durchgeführte Löschvorgänge.

(c) Bei Beendigung des Vertragsverhältnisses eines Kunden mit dem Auftraggeber werden sämtliche für diesen Kunden im LECS-System gespeicherten Daten sowie die zugehörigen Verschlüsselungsschlüssel unverzüglich und unwiderruflich gelöscht (kryptographische Löschung). Im Anschluss an die kryptographische Löschung werden die verschlüsselten Inhalte und die zugehörigen Metadaten aus den produktiven Systemen entfernt; Restbestände in Backups werden im Rahmen der vereinbarten Backup-Aufbewahrungsfrist überschrieben bzw. vernichtet. Auf Anfrage stellt der Provider eine Löschbestätigung bereit.

(d) Die Wirksamkeit des Löschmechanismus wird regelmäßig überprüft und dokumentiert.

18. SPRACHEINGABE (VOICE INPUT)

18.1 Der Provider stellt die Spracheingabe (Voice Input) über das selbst gehostete Spracherkennungsmodell noxtua-ai-voice (Automatic Speech Recognition, ASR) bereit. Das Modell wird ausschließlich innerhalb der eigenen, in der in Europa betriebenen Infrastruktur des Providers betrieben; eine Einbindung externer Sprachdienste oder eine Übermittlung an Dritte findet nicht statt.

18.2 Das per Mikrofon erfasste Audio wird ausschließlich flüchtig im Arbeitsspeicher zur Transkription verarbeitet und unmittelbar nach der Transkription verworfen. Es wird weder auf einem Datenträger noch in einer Datenbank gespeichert; es findet kein Antwort-Caching statt.

Transkripte werden ausschließlich an den Client zurückgegeben und nicht serverseitig gespeichert.

18.3 Es erfolgt kein Inhalts-Logging der Audiodaten oder Transkripte in Anwendungsprotokollen sowie keine Übermittlung an Dritt-Analyse-, Monitoring- oder Error-Tracking-Dienste. Die Übertragung erfolgt transportverschlüsselt.

18.4 Es wird kein Stimmabdruck (Voiceprint) erzeugt und keine Sprecheridentifikation oder biometrische Kategorisierung vorgenommen (No-Voiceprint-Design). Der Mikrofonzugriff erfolgt erst nach Browser-Berechtigung; bei aktivem Mikrofon wird ein deutlicher Aufnahmeindikator angezeigt. Administratoren können die Spracheingabe je Organisation aktivieren und deaktivieren.

19. MODELLINFERENZ UND MODELLKATEGORIEN

19.1 Für die Verarbeitung von Nutzeranfragen stehen zwei Modellkategorien zur Verfügung. Die Kategorie legt fest, welches Basismodell die Anfrage verarbeitet und auf welchem Weg dieses Modell bezogen wird. Alle übrigen Bestandteile des Systems – insbesondere die kuratierte Datenbasis, die Verschlüsselung nach Ziffer 8, die Speicherung nach Ziffer 13 sowie die Submodelle für Texterkennung, Suche und Spracheingabe – sind in beiden Kategorien identisch. Die Submodelle werden ausschließlich vom Provider selbst gehostet.

19.2 **Athena Agent:** Der Provider betreibt eine lokale, für den juristischen Einsatz nachtrainierte Kopie eines Open-Source-Modells auf eigener, europäisch kontrollierter Infrastruktur (Open Telekom Cloud der Telekom Deutschland GmbH sowie IONOS SE, Rechenzentren in Deutschland und in der Schweiz). Die Modellgewichte werden vor ihrem Einsatz hash-verifiziert. Es bestehen kein Rückkanal und keine Telemetrie zum ursprünglichen Entwickler des Basismodells; dieser erhält weder Zugriff auf das Modell im Betrieb noch auf Ein- oder Ausgaben. In der Verarbeitungskette dieser Kategorie steht kein Anbieter, der dem Recht eines Drittstaates unterliegt.

19.3 **Minerva Agent:** Diese Kategorie eröffnet den Zugang zu Frontier-Modellen (closed source). Vertragspartnerin und Unterauftragsverarbeiterin des Providers ist die Telekom Deutschland GmbH, die das jeweilige Modell über ihre AI Foundation Services innerhalb der Open Telekom Cloud bereitstellt. Unterauftragsverarbeiterin der Telekom Deutschland GmbH ist Google, die die Modellumgebung in einem Rechenzentrum in der Europäischen Union betreibt. Der Zugriff erfolgt nicht über das offene Internet, sondern über eine verschlüsselte, vom Internet isolierte Verbindung.

19.4 In der Modellumgebung der Kategorie nach Ziffer 19.3 (Minerva Agent) werden die Anfragen ausschließlich flüchtig im Arbeitsspeicher des Unterunterauftragnehmers des Providers und nur für die Dauer der jeweiligen Anfrage verarbeitet. Auf dieser Inferenzebene werden keine Daten gespeichert (Zero Data Retention). Die Sicherstellung der Zero Data Retention ist durch drei dokumentierte Maßnahmen gegeben: (i) deaktiviertes Daten-Caching im Arbeitsspeicher, (ii) abgewählte Protokollierung der Eingaben zur Missbrauchsüberwachung und (iii) Verzicht auf Funktionen, die eine Speicherung zwingend voraussetzen. Ein Zugriff des Personals des Modellanbieters auf Ein- oder Ausgaben findet nicht statt.

19.5 In keiner der beiden Kategorien (Athena oder Minerva) werden Eingaben, Ausgaben oder hochgeladene Inhalte zum Training der zugrunde liegenden Modelle verwendet. Der Konversationsverlauf wird unverändert nach Ziffer 8.2 verschlüsselt und nach Ziffer 13.3 auf der vom Provider kontrollierten europäischen Infrastruktur unter eigenen Schlüsseln gespeichert; eine Speicherung auf Systemen eines Modellanbieters findet nicht statt.

19.6 Der Administrator des Kunden legt fest, welche Modellkategorien in einem Arbeitsbereich verfügbar sind, und kann einzelne Kategorien vollständig deaktivieren. Athena Agent ist die Voreinstellung. Innerhalb der freigegebenen Kategorien entscheidet der Nutzer je Arbeitsbereich oder je Aufgabe. Die tatsächlich verwendete Kategorie ist an jeder Antwort ausgewiesen; ein automatischer Wechsel zwischen den Kategorien findet nicht statt.

19.7 Die Verpflichtung zur Verschwiegenheit nach § 203 StGB ist über die gesamte Verarbeitungskette beider Kategorien weitergegeben. Die Einführung der Modellkategorien ändert weder die Zwecke der Verarbeitung noch die Kategorien der verarbeiteten Daten noch die Rollenverteilung zwischen Kunde und Provider.