

Anlage 1 zu den Nexis 4 Plattform AGB

Auftragsverarbeitungsvertrag

"Vertrag"

Nachfolgend werden der Verantwortliche und Nexis jeweils als **Vertragspartei** und gemeinsam als **Vertragsparteien** bezeichnet. Verantwortlicher im Sinne dieser Anlage ist der Lizenznehmer.

Präambel

Dieser Vertrag regelt die datenschutzrechtlichen Verpflichtungen betreffend die Verarbeitung personenbezogener Daten im Zuge der von Nexis unter den Nexis 4 Plattform AGB und im Zusammenhang mit dem dazugehörigen Angebot (der "**Hauptvertrag**") erbrachten Leistungen.

Sofern im Rahmen dieses Vertrags nicht abweichend definiert, gelten die in den Nexis 4 Plattform AGB festgelegten Definitionen gleichermaßen fort.

1. Gegenstand der Verarbeitung

- 1.1 Soweit Nexis im Rahmen der Durchführung des Hauptvertrages Zugang zu personenbezogenen Daten erhält, die er im Auftrag des Verantwortlichen verarbeitet ("**Gegenstand der Verarbeitung**"), gelten die Bestimmungen dieses Vertrages. Einzelheiten der Verarbeitung ergeben sich aus Annex 1 (Beschreibung der Verarbeitung), der Bestandteil dieses Vertrages ist.
- 1.2 Der Gegenstand der Verarbeitung gilt als Weisung im Sinne des Punkt 2.1.
- 1.3 Jede Änderung des Gegenstands der Verarbeitung bedarf einer entsprechenden schriftlichen Weisung durch den Verantwortlichen.

2. Verarbeitung nur auf Weisung des Verantwortlichen

- 2.1 Personenbezogene Daten dürfen nur auf schriftliche Weisung des Verantwortlichen, insbesondere in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, verarbeitet werden. Mündliche Weisungen sind vom Verantwortlichen unverzüglich und ohne Aufforderung in Textform (bspw. E-Mail) zu bestätigen.
- 2.2 Sollte Nexis auch ohne Vorliegen einer derartigen Weisung durch nationales Recht oder Unionsrecht zur Verarbeitung

oder Übermittlung verpflichtet sein, so hat Nexis dies dem Verantwortlichen vor Aufnahme der entsprechenden Verarbeitungstätigkeit in Textform (per E-Mail) mitzuteilen, sofern eine derartige Mitteilung nicht aufgrund eines wichtigen öffentlichen Interesses oder sonstigen gesetzlich zwingenden Gründen untersagt ist.

- 2.3 Nexis hat den Verantwortlichen unverzüglich zu informieren, falls er der Auffassung ist, dass eine Weisung des Verantwortlichen gegen anwendbare datenschutzrechtliche Vorschriften verstößt.

3. Wahrung der Vertraulichkeit

Nexis hat alle mit der Verarbeitung personenbezogener Daten beauftragten Personen vor Aufnahme der Tätigkeit zur Wahrung der Vertraulichkeit zu verpflichten, sofern sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

4. Sicherheit der Verarbeitung

- 4.1 Nexis hat gemäß Artikel 32 der Datenschutz-Grundverordnung (Verordnung (EU) 679/2016, "**DSGVO**") erforderliche Maßnahmen für ein angemessenes Schutzniveau zu ergreifen. Die von Nexis gemäß Artikel 32 DSGVO getroffenen technischen und organisatorischen Maßnahmen ergeben sich aus Annex 2 (Technisch-organisatorische Maßnahmen), der Bestandteil dieses Vertrages ist.
- 4.2 Nexis hat unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zu unterstützen.
- 4.3 Nexis unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung seiner Pflichten zur Beantwortung von Anträgen auf Ausübung der in Kapitel III der DSGVO genannten Rechte betroffener Personen.

5. Informationspflichten und Kontrollrechte

- 5.1 Der Verantwortliche hat das Recht, sich jederzeit persönlich oder durch einen von ihm benannten Vertreter von der Einhaltung der Bedingungen dieses Vertrages zu überzeugen. Nexis hat dem Verantwortlichen bzw. den von ihm benannten Vertreter Zugang zu den im Zusammenhang mit der Verarbeitung stehenden wesentlichen Räumlichkeiten zu verschaffen. Diese Überprüfungen erfolgen ausschließlich während der gewöhnlichen Geschäftszeiten von Nexis und, sofern nicht im Einzelfall

zwingend anders erforderlich, mit einer vorherigen Ankündigungsfrist von mindestens 14 Werktagen. Der Verantwortliche wird sicherstellen, dass derartige Überprüfungen in einer Weise durchgeführt werden, die den Geschäftsbetrieb von Nexis so wenig wie möglich beeinträchtigt. Eine solche Überprüfung soll grundsätzlich nicht häufiger als einmal jährlich erfolgen. Die im Rahmen dieser jährlichen Überprüfung anfallenden Kosten trägt jede Partei selbst. Darüberhinausgehende Prüfungen sollen nur erfolgen, wenn konkrete Anhaltspunkte für einen Verstoß gegen die datenschutzrechtlichen Verpflichtungen durch Nexis vorliegen. Zeigt sich im Rahmen einer zusätzlichen Überprüfung, dass Nexis nicht gegen die datenschutzrechtlichen Verpflichtungen verstoßen hat, trägt der Verantwortliche die für Nexis entstehenden, angemessenen Kosten.

- 5.2 Nexis hat dem Verantwortlichen alle Daten und Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in diesem Vertrag genannten Verpflichtungen erforderlich sind.

6. Unterauftragsverarbeiter

- 6.1 Nexis besitzt die allgemeine schriftliche Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in Annex 3 aufgeführt sind. Nexis unterrichtet den Verantwortlichen mindestens 30 Tage im Voraus ausdrücklich in Textform über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Nexis stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.
- 6.2 Nexis stellt sicher, dass Unterauftragsverarbeiter durch einen Vertrag zur Einhaltung der gleichen datenschutzrechtlichen Pflichten verpflichtet werden, die in diesem Vertrag festgelegt sind, insbesondere zur Gewährleistung geeigneter technischer und organisatorischer Maßnahmen gemäß Artikel 28 Abs. 4 DSGVO.
- 6.3 Eine Liste der zum Zeitpunkt des Vertragsschlusses vom Verantwortlichen genehmigten Unterauftragsverarbeiter ist in Annex 3 (Autorisierte Unterauftragsverarbeiter) enthalten, der Bestandteil dieses Vertrages ist.

7. Beginn, Laufzeit, Kündigung

- 7.1 Dieser Vertrag tritt mit dem Hauptvertrag und spätestens mit Erbringung der Leistungen durch Nexis gemäß des Hauptvertrags in Kraft.
- 7.2 Dieser Vertrag wird auf Dauer des Hauptvertrages abgeschlossen und endet, wenn der Hauptvertrag durch Zeitablauf endet oder sonst vorzeitig beendet wird.
- 7.3 Die ordentliche Kündigung dieses Vertrages ohne Kündigung des Hauptvertrags ist ausgeschlossen.

8. Rechtsfolgen der Beendigung

- 8.1 Nexis hat nach Beendigung dieses Vertrages oder Beendigung der Verarbeitungsleistungen alle personenbezogenen Daten, Verarbeitungsergebnisse und Unterlagen, die personenbezogene Daten enthalten, nach Wahl des Verantwortlichen zurückzugeben und/oder zu löschen, außer er ist durch nationale Vorschriften oder Unionsrecht zur Weiterspeicherung verpflichtet.
- 8.2 Trifft der Verantwortliche bei oder vor Beendigung dieses Vertrages oder der Verarbeitungsleistungen keine entsprechende Wahl, so sind alle personenbezogenen Daten, zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

9. Sonstiges

- 9.1 Die Vertragsparteien verpflichten sich, sämtliche Rechte und Pflichten aus diesem Vertrag einschließlich dieser Überbindungsverpflichtung wechselseitig auf ihre jeweiligen Gesamtrechtsnachfolger zu überbinden.
- 9.2 Alle Änderungen und Ergänzungen sowie die Aufhebung dieses Vertrages und seiner Anhänge einschließlich des Abgehens von der hier festgelegten Form bedürfen zu ihrer Wirksamkeit der Textform (bspw. E-Mail), soweit keine strengere, insbesondere notarielle Form erforderlich sein sollte.
- 9.3 Durch die Ungültigkeit, Gesetzwidrigkeit oder Undurchsetzbarkeit einer oder mehrere der in diesem Vertrag enthaltenen Bestimmungen wird die Gültigkeit, Rechtmäßigkeit und Durchsetzbarkeit der übrigen Bestimmungen dieses Vertrages in keiner Weise berührt. Eine unwirksame, nichtige oder undurchsetzbare Bestimmung dieses Vertrages gilt – soweit gesetzlich zulässig – durch eine solche rechtswirksame, gültige und durchsetzbare Bestimmung ersetzt, die ihr nach dem von

den Vertragsparteien rechtlich und wirtschaftlich verfolgten Zweck am nächsten kommt.

9.4 Rechtswahl und Gerichtsstand ergibt sich aus den Nexis 4 Plattform AGB.

Für den Verantwortlichen:

_____, am _____

Name:

Funktion:

Für Nexis:

_____, am _____

Name:

Funktion:

Annex 1

Gegenstand der Verarbeitung

Gegenstand der Verarbeitung	Technischer Betrieb der Software NEXIS
Zweck der Verarbeitung	Bereitstellung der Software NEXIS 4 gemäß des Hauptvertrags
Art der Verarbeitung	• Erhebung (von Systemen des Verantwortlichen) • Speicherung • Organisation • Auslesung • Löschung • Übermittlung (an Systeme des Verantwortlichen) • Monitoring und Logging (Erfassen von Auffälligkeiten und Fehlern) • KI-gestützte Analyse, Textproduktion und Automatisierung
Dauer der Verarbeitung	Gemäß Laufzeit des Hauptvertrags
Kategorien personenbezogener Daten	Die Kategorien der verarbeiteten personenbezogenen Daten werden durch den Verantwortlichen im Rahmen der Nutzung unserer Dienstleistung bestimmt. Hierbei handelt es sich im Sinne der erbrachten Leistung gemäß des Hauptvertrags regelmäßig um: • Vor- und Nachname

	• Geschäftliche Stammdaten (z.B. E-Mail-Adresse, Abteilung, Standort) • Technische Informationen (z.B. IP-Adresse) • Identity and Access Management bezogene Informationen (z.B. Berechtigungszuweisungen) • Prompt- und sonstige Texteingaben sowie Ausgaben
Kategorien von betroffenen Personen	Mitarbeiter des Verantwortlichen, Geschäftspartner des Verantwortlichen
Übermittlung an Drittländer (oder internationale Organisationen)	Grundsätzlich Verarbeitung innerhalb der Europäischen Union/des Europäischen Wirtschaftsraums, Drittlandübermittlungen oder Drittlandzugriffe können im Rahmen von Microsoft-Support-, Sicherheits-, Wartungs- oder Konzernleistungen nicht vollständig ausgeschlossen werden und erfolgen nur auf Grundlage geeigneter Garantien nach Art. 44 ff. DSGVO, insbesondere Angemessenheitsbeschluss, EU-Standardvertragsklauseln und ergänzender Maßnahmen.

Annex 2

Technische und organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen hat Nexis die folgenden technischen und organisatorischen Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus im Sinne von Artikel 32 DSGVO umgesetzt:

1. Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)
<i>Zutrittskontrolle</i>
• Chipkarten / Transpondersysteme • Sicherheitsschlösser • Absicherung der Gebäudeschächte • Türen mit Knauf auf Außenseite • Schlüsselregelung / Liste • Empfang / Rezeption / Pförtner • Besucherbuch / Protokoll der Besucher • Mitarbeiter- / Besucherausweise • Besucher in Begleitung durch Mitarbeiter • Sorgfalt bei Auswahl Reinigungsdienste
<i>Zugangskontrolle</i>
• Login mit Benutzername & Passwort • Login mit 2-Faktor-Authentifizierung • Anti-Virus-Software Server • Anti-Virus-Software Clients • Firewall • Verschlüsselung von Datenträgern • Automatische Desktopsperre • Benutzerberechtigungskonzept • Administrierte Benutzerverwaltung • Zwingende Passwortanforderungen • Clean Desk Richtlinie • Mobile Device Policy • Remote Working Policy
<i>Zugriffskontrolle</i>
• Automatisierte Logauswertung

- Protokollierung aller Datenzugriffe
- Protokollierung der Anwendungszugriffe
- Differenzierte Berechtigungen Daten, Anwendungen, Betriebssystem
- Differenzierte Berechtigungen lesen, ändern, löschen
- Datenverschlüsselung „at rest“
- Transportverschlüsselung „in transit“
- Reduktion von Administratorzugängen
- Sorgfalt Auswahl Administratoren
- Verwaltung der Benutzerrechte durch Administratoren

Trennungskontrolle

- Automatisierte Logauswertung
- Protokollierung aller Datenzugriffe
- Protokollierung Anwendungszugriffe
- Differenzierte Berechtigungen Daten, Anwendungen, Betriebssystem
- Differenzierte Berechtigungen lesen, ändern, löschen
- Mandantentrennung logisch
- Trennung von Test- und Produktivsystemen
- Reduktion von Administratorzugängen
- Sorgfalt Auswahl Administratoren
- Verwaltung der Benutzerrechte durch Administratoren

Pseudonymisierung

- Pseudonymisierung von Kundendaten in Dateien, wenn anwendbar und technisch möglich
- Pseudonymisierung von Kundendaten in NEXIS 4 (Analysesoftware), wenn anwendbar und technisch möglich

Weitergabekontrolle

- Starke Abschottung des internen Netzes mit Hilfe eines gesicherten Tunnels (VPN-Zugang)
- Begrenzter Mitarbeiterkreis
- Mitarbeiter geschult in Informationssicherheit
- Verpflichtung der Mitarbeiter auf sorgfältigen Umgang mit Informationen und Geheimhaltung
- E-Mail-Verschlüsselung (S/MIME / PGP)
- Einsatz von VPN
- Datenverschlüsselung „at rest“
- Transportverschlüsselung „in transit“
- Dokumentation von Datenempfängern, Speicherdauer und Sicherheitsmaßnahmen
- Regelmäßige Kontrolle der Datenübermittlungen

2. Gewährleistung der Integrität und Eingabekontrolle (Art. 32 Abs. 1 lit. b DSGVO)

- Protokollierung von Nutzeraktionen bei Eingabe von Daten

- Protokollierung von Nutzeraktionen bei Änderungen von Daten
- Protokollierung von Nutzeraktionen beim Löschen von Daten
- Protokollierung aller Aktionen in NEXIS 4 bei der Verarbeitung personenbezogener Daten
- Bedarfsfallbezogene Auswertung der Protokolle
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Kennzeichnung erfasster Daten
- Dedizierter Logserver
- Übersicht über Programme mit Zugriff auf personenbezogene Daten
- Individuelle Benutzerprofile
- Vergabe von Rechten basierend auf einem Berechtigungskonzept
- Organisatorische Festlegung von Eingabezuständigkeiten
- Verpflichtung auf das Datengeheimnis bzw. zur Vertraulichkeit/Verschwiegenheit
- Berechtigungskonzept für Logzugriff

3. Gewährleistung der Belastbarkeit von Systemen (Art. 32 Abs. 1 lit. b DSGVO)

- Lastausgleich (load balancing) der Netzwerkkomponenten
- Lastausgleich (load balancing) der Dienste
- Ausweichverarbeitungsanlagen vorhanden
- Redundante USV
- Redundante Klimatisierung
- Redundante Stromversorgung
- Redundante Brandbekämpfung
- Computer Emergency Response Team (CERT)
- Regelmäßige Penetration-Tests
- Regelmäßiges Patchen aller Systeme
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Regelmäßiges Training der Mitarbeiter

4. Gewährleistung der Verfügbarkeit und Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten (Art. 32 Abs. 1 lit. b, c DSGVO)

- Unterbringung der Server in spezifischem Serverraum in den Geschäftsräumen der Nexis GmbH oder dem Anbieter des Rechenzentrums
- Brandmeldeanlage (BMA)
- Feuer- und Rauchmeldeanlagen
- Wasserlose Brandbekämpfung im Serverraum
- Temperatur- und Feuchtigkeitsüberwachung Serverraum
- Klimatisierung des Serverraums
- Blitz- und Überspannungsschutz
- Unterbrechungsfreie Stromversorgung (USV)
- Notstromgenerator
- Schutzsteckdosen Serverraum
- RAID-System / Festplattenspiegelung

- Videoüberwachung Serverraum
- Alarmmeldung bei unberechtigtem Zutritt zum Serverraum
- Backup & Recovery-Konzept (ausformuliert)
- Regelmäßige Kontrolle von Back-Up-Maßnahmen
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Serverräumlichkeiten in unterschiedlichem Brandabschnitt
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums
- Getrennte Partitionen für Betriebssysteme und Daten
- Vorhandener Katastrophen- bzw. Notfallplan
- Zutrittsbegrenzung zum Serverraum
- Regelmäßige Schwachstellenanalyse

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO)

- ISMS unter Berücksichtigung ausgewählter Anforderungen der ISO/IEC 27001
- Strukturiertes Risikomanagement nach ISO/IEC 27001 und BSI
- Regelmäßige interne und externe Audits im Rahmen des Aufbaus eines ISMS nach ISO/IEC 27001
- Datenschutz-Management-Software
- Interne Verfahrensverzeichnisse werden mind. jährlich aktualisiert.
- Prozess zur Meldung neuer Verarbeitungsverfahren
- Auswahl datenschutzfreundlicher Voreinstellungen
- Prozess zur Einbindung des Datenschutzbeauftragten
- Überprüfung der getroffenen Maßnahmen nach dem PDCA-Zyklus (Plan, Do, Check, Act)
- Prozess zur Reaktion auf Datenschutzverletzungen

6. Auftragskontrolle

- Vertragsgestaltung gem. DSGVO (Art. 26, 28 DSGVO)
- Zentrale Erfassung vorhandener Dienstleister
- Vertragsmanagement und regelmäßige Aktualisierung der Verträge

7. KI-spezifische Maßnahmen

- Serverseitige Aufrufe der LLM-Komponente über eine zentrale, gekapselte Integrationsschicht; kein direkter Aufruf des LLM-Anbieters aus dem Browser des Nutzers
- Betrieb der lokalen ML-Komponente als interner Dienst ohne externe Schnittstellen
- Mandantengetrennte Führung von RAG-Indizes und semantischen Stores; Retrieval ausschließlich innerhalb des jeweiligen Mandantenkontexts
- Serverseitige Zusammenstellung von System-Prompts und mandantenspezifischen Prompt-Komponenten; kein Zugriff der

Nutzer auf System-Prompts

- Keine Nutzung von Kundendaten, Prompts, Outputs oder RAG-Inhalten zum Training, Fine-Tuning oder zur Verbesserung von Foundation Models
- Keine Übernahme von RAG-Inhalten in Modellgewichte; kein Fine-Tuning oder kundenspezifisches Training mit Kunden- oder personenbezogenen Daten ohne gesonderte datenschutzrechtliche Prüfung und vertragliche Grundlage
- Prompt-Injection-Erkennung, Filterung schädlicher Eingabemuster sowie Längen- und Strukturprüfungen von Eingaben
- Einsatz eines mehrschichtigen System-Prompt-Konzepts zur Identitäts-, Verhaltens-, Scope- und Sicherheitssteuerung
- Plausibilitäts-, Schema- und Output-Prüfung von LLM-Ausgaben vor Rückgabe an den Nutzer
- Mandantenspezifische API-Quotas und Rate-Limiting zur Vermeidung missbräuchlicher Nutzung und DDoS-Muster
- Aktivierung von Azure AI Content Safety zur Prüfung von Eingaben und Ausgaben auf schädliche Inhalte zur Laufzeit
- Kennzeichnung von NICO-Interaktionspunkten als KI-Funktion sowie visuelle Markierung KI-generierter Inhalte
- Anzeige eines Informationshinweises vor der erstmaligen Nutzung mit Hinweis auf KI-Charakter, mögliche Ungenauigkeiten und Nutzerverantwortung
- Bereitstellung von NICO-Ergebnissen als Vorschläge, Hinweise, Zusammenfassungen, Klassifikationen oder Findings; Möglichkeit für Nutzer, KI-Vorschläge abzulehnen, zu bearbeiten oder zu verwerfen
- Speicherung von Roh-Prompts nur, soweit für Workflow-Kontext, Nachvollziehbarkeit oder Audit-Trail erforderlich; zeitbasierte Löschung nach Maßgabe der kundenseitig konfigurierten Aufbewahrungsfristen

Annex 3

Autorisierte Unterauftragsverarbeiter

Unterauftragsverarbeiter	Adresse	Zweck
Microsoft Ireland Operations Limited	70 Sir John Rogerson's Quay Dublin 2D02 R296, Irland	Bereitstellung virtualisierter Infrastruktur über die Microsoft-Azure-Plattform zum Betrieb der SaaS-Anwendung sowie Bereitstellung und Ausführung von LLM-/KI-Modellen innerhalb der Azure-Umgebung
Nexis GRC GmbH	Hans-Henny-Jahnn-Weg 53, 22085 Hamburg	Erbringung von Support- und Beratungsleistungen gegenüber Kunden, Bereitstellung der Softwareanwendung sowie Betrieb der hierfür erforderlichen Hosting- und IT-Infrastruktur
Nexis Group GmbH	Rudolf-Vogt-Straße 6, 93053 Regensburg	Überwachung, Entwicklung und Verbesserung der bereitgestellten Dienstleistung