Auftragsverarbeitungsvertrag (AVV) Nexis QSEC (SaaS)

Anlage 1 zu den QSEC Plattform AGB – Auftragsverarbeitungsvertrag („Vertrag“), Version 1.4

Stand: 16.11.2026 | **Status:** Freigegeben

Inhaltsverzeichnis

1. Gegenstand der Verarbeitung 1
2. Verarbeitung nur auf Weisung des Verantwortlichen 2
3. Wahrung der Vertraulichkeit 2
4. Sicherheit der Verarbeitung 2
5. Informationspflichten und Kontrollrechte 2
6. Unterauftragsverarbeiter 3
7. Beginn, Laufzeit, Kündigung 3
8. Rechtsfolgen der Beendigung 4
9. Sonstiges 4
Annex 1 5
Annex 2 6
Annex 3 9

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 QSEC 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 QSEC 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 QSEC Plattform AGB.

Für den Verantwortlichen:	**Für Nexis:**
Name:	Name:
Funktion:	Funktion:

Annex 1

Gegenstand der Verarbeitung

Gegenstand der Verarbeitung	Technischer Betrieb der Software QSEC
Zweck der Verarbeitung	Bereitstellung der Software QSEC 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)
Dauer der Verarbeitung	Gemäß Laufzeit des Hauptvertrags
Kategorien personenbezogenen 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)
Kategorien von betroffenen Personen	Mitarbeiter und Ansprechpartner 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:

Anhang A – Technisch-Organisatorische Maßnahmen des Auftragsverarbeiters (Art. 32 DS-GVO)

Gewährleistung der Vertraulichkeit und Pseudonymisierung und Verschlüsselung personenbezogener Daten

Zutrittskontrolle

- Zutritt zu Räumen nur mit Hilfe eines Schlüssels möglich
- Verwaltung des Zutritts (Schlüsselausgabe, Zutritt zu Räumen etc.)
- Begrenzter Mitarbeiterkreis

Zugangskontrolle

- Zentralisierte Verwaltung der Nutzer und Clients durch Systemadministrator
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Authentifikation mit Benutzername / Passwort
- Starke Abschottung des internen Netzes mit Hilfe eines gesicherten Tunnels (VPN-Zugang)
- Einsatz von Anti-Viren-Software auf Clients und Servern
- Einsatz mehrstufiger Firewalls im Netzwerk
- Einsatz von Festplatten- und Datenträgerverschlüsselung nach aktuellem Stand der Technik auf Clients und Servern
- Einsatz von TLS/SSL Verschlüsselung der internen und ggf. externen Kommunikationswege
- Regelmäßiges Einspielen von Sicherheitsupdates auf Clients und Servern
- Dedizierte Instanz für E-Mail-Dienst auf isoliertem virtuellem Server

Zugriffskontrolle

- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Zusätzliche Daten-Verschlüsselung streng vertraulicher Informationen, wenn nötig
- Sichere Aufbewahrung der Backups
- Verwaltung der Berechtigungen durch Systemadministrator

Trennungskontrolle

- Datenbankberechtigungen
- Verwendung virtualisierter Trennung pro interne Anwendung
- Logische Trennung von Kundendateien

Pseudonymisierung

- Pseudonymisierung von Kundendaten in Dateien, wenn anwendbar und technisch möglich

Weitergabekontrolle

- Starke Abschottung des internen Netzes mit Hilfe eines gesicherten Tunnels (VPN-Zugang)
- Begrenzter Mitarbeiterkreis
- Mitarbeiter geschult in Informationssicherheit und Datenschutz
- Verpflichtung der Mitarbeiter auf sorgfältigen Umgang mit Informationen und Geheimhaltung

Gewährleistung der Integrität & Eingabekontrolle

- Beschränkung von Zugang, Zutritt und Zugriff auf Informationen (siehe Punkt 1)
- Backup- und Restore-Prozesse zur Wiederherstellung der Integrität
- Protokollierung von Nutzeraktionen bei Eingabe von Daten
- Protokollierung von Nutzeraktionen bei Änderungen von Daten
- Protokollierung von Nutzeraktionen beim Löschen von Daten
- Bedarfsfallbezogene Auswertung der Protokolle

Gewährleistung der Belastbarkeit von Systemen

- Testen der Belastbarkeit
- Monitoring der Systeme

Gewährleistung der Verfügbarkeit und Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

- Brandmeldeanlange (BMA)
- Feuerlöschgeräte
- Backup- und Restore-Prozesse
- Testen von Datenwiederherstellung
- Zentrales Ablegen von Informationen auf Servern

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen / Wirksamkeitskontrolle

- Aufbau eines ISMS nach 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
- Prüfungen im Rahmen des Datenschutzes und der Anforderungen der DS-GVO
- Datenschutz-Management im Rahmen des Aufbaus des ISMS

Auftragskontrolle

- Dokumentation der Verarbeitungen im Verfahrensverzeichnis
- Einsatz von Unterauftragsverarbeitern ausschließlich gemäß Ziffer 6 und Annex 3
- Ausschließliche Verarbeitung personenbezogener Daten auf Basis von schriftlichen Weisungen

- Verpflichtung der Beschäftigten des Auftragsverarbeiters zur Vertraulichkeit

Annex 3

Autorisierte Unterauftragsverarbeiter

Unterauftragsverarbeiter	Adresse	Zweck
PlusServer GmbH	Venloer Str. 47 50672 Köln	Bereitstellung der virtualisierten Hardware für den SaaS Betrieb
Nexis GmbH	Rudolf-Vogt-Straße 6, 93053 Regensburg	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