

Vertrag zur Auftragsverarbeitung gem. Art. 28 Abs. 3 DS-GVO

zwischen

Auftraggeber

Straße

PLZ Ort

Deutschland

- im Folgenden „Auftraggeber“ genannt -

und

Nexis GmbH

Rudolf-Vogt-Straße 6

93053 Regensburg

Deutschland

- im Folgenden „Auftragsverarbeiter“ genannt -

§0 Präambel

Es ist der ausdrückliche Wille beider Parteien, dass alle Voraussetzungen und Anforderungen an eine rechtskonforme Auftragsverarbeitung gemäß der Europäischen Datenschutzgrundverordnung erfüllt werden.

Zwischen den Parteien besteht neben diesem Auftragsverarbeitungsvertrag ein separater Vertrag (Hauptvertrag), der die nicht datenschutzbezogenen Leistungspflichten der Parteien regelt. Der Auftragsverarbeiter wird vom Auftraggeber mit der Erbringung bestimmter, im Hauptvertrag geregelter, Leistungen beauftragt.

Im Zusammenhang mit der Erbringung dieser Leistungen findet durch den Auftragsverarbeiter auch eine Verarbeitung von personenbezogenen Daten statt. Hierin liegt eine Auftragsverarbeitung im Sinne des Art. 28 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, „DS-GVO“).

Zur Erfüllung der Anforderungen der DS-GVO an derartige Konstellationen schließen die Parteien den nachfolgenden Vertrag, dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§1 Gegenstand und Dauer des Vertrages

1. Der Auftragsverarbeiter erbringt für den Auftraggeber Leistungen auf Grundlage des Hauptvertrags. Die personenbezogenen Daten, auf die der Auftragsverarbeiter währenddessen Zugriff erhält (Auftraggeberdaten), verarbeitet dieser ausschließlich im Auftrag und nach Weisung des Auftraggebers. Sofern diese Datenarten besonderen Kategorien personenbezogener Daten umfassen sollten, sind diese in § 2 Nr. 2 als solche gesondert gekennzeichnet.
2. Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten des Auftraggebers selbst oder von Dritten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.
3. Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union (EU) oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Jede Verlagerung der Dienstleistung oder von Teilarbeiten in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

4. Die Laufzeit dieses Vertrags

☐ beginnt am 29.07.2021 und endet am 29.07.2021.

☐ bemisst sich anhand der Laufzeit des Hauptvertrags [Klicken oder tippen Sie hier, um Text einzugeben.](#)

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzbestimmungen oder gegen Inhalte dieses Vertrages vorliegt, der Auftragsverarbeiter eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragsverarbeiter Kontrollrechte des Auftraggebers verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

5. Der Auftragsverarbeiter wird die Auftraggeberdaten nur so lange verarbeiten, wie dies für die Erreichung des jeweiligen Zwecks erforderlich ist. Dies bedeutet insbesondere, dass der Auftragsverarbeiter die Auftraggeberdaten nach Erreichen des Zwecks unverzüglich löschen wird, sofern er nicht aus anderen Gründen zu einer Speicherung verpflichtet ist; eine darüberhinausgehende Speicherung der Auftraggeberdaten beim Auftragsverarbeiter ist nicht erforderlich und nicht gestattet.

Dem Auftragsverarbeiter ist eine abweichende oder über die Festlegungen in der Anlage 1 hinausgehende Verarbeitung von Auftraggeberdaten untersagt. Dies gilt auch für die Verwendung anonymisierter Daten.

§2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

1. Im Rahmen der Auftragsverarbeitung werden vom Auftragsnehmer folgende Verarbeitungstätigkeiten durchgeführt:

[Klicken oder tippen Sie hier, um Text einzugeben.](#)

Es werden folgende Arten von personenbezogenen Daten verarbeitet:

[Klicken oder tippen Sie hier, um Text einzugeben.](#)

Die folgenden Kategorien von Personen sind betroffen:

[Klicken oder tippen Sie hier, um Text einzugeben.](#)

Der Auftragsverarbeiter verwendet die Daten ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers und den in diesem Vertrag definierten Bestimmungen.

§3 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragsverarbeiter verpflichtet, alle solche Anfragen, sofern sie erkennbar an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.
2. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragsverarbeiter abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
3. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen

sind auf Verlangen unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

4. Der Auftraggeber ist berechtigt, sich wie unter §5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
5. Der Auftraggeber informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Datenverarbeitung feststellt.
6. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

§4 Weisungsberechtigte des Auftraggebers und Weisungsempfänger des Auftragsverarbeiters

1. Weisungsberechtigte Personen des Auftraggebers gegenüber des Auftragsverarbeiters sind:

Name, Funktion, Telefonnummer

2. Weisungsempfänger beim Auftragsverarbeiter sind:

Name, Funktion, Telefonnummer

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Bis zum Zugang einer solchen Mitteilung gelten die benannten Personen weiter als berechtigt.

3. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

§5 Pflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).
2. Der Auftragsverarbeiter ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Die Auftraggeberdaten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

3. Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt
4. Der Auftragsverarbeiter sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
5. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden vom Auftragsverarbeiter dokumentiert.
6. Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten (Art. 30 DS-GVO) sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers (Art. 35 DS-GVO) hat der Auftragsverarbeiter im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an die in §4 Satz 1 genannten Personen des Auftraggebers weiterzuleiten.
7. Der Auftragsverarbeiter wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO).
8. Der Auftragsverarbeiter hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragsverarbeiters dem nicht entgegenstehen.
9. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen. Macht ein Betroffener Rechte, insbesondere auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragsverarbeiter geltend, wird er dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und dessen Weisungen abwarten. Ohne entsprechende Einzelweisung wird der Auftragsverarbeiter nicht mit der betroffenen Person in Kontakt treten.
10. Der Auftragsverarbeiter verpflichtet sich, alle erforderlichen Maßnahmen gem. Art. 32 DS-GVO zu ergreifen und diese für die Dauer der Verarbeitung der Auftraggeberdaten aufrecht zu erhalten. Auf Verlangen des Auftraggebers wird der Auftragsverarbeiter dem Auftraggeber die Einhaltung der gemäß Art. 32 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen durch geeignete Nachweise nachweisen. Eine Übersicht über die technischen und organisatorischen Maßnahmen finden sich in Anlage 1 dieses Vertrags, wobei die dort aufgeführten Maßnahmen lediglich das vertraglich vereinbarte Minimum hinsichtlich der zu erfüllenden Vorkehrungen darstellen.
11. Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften

und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO). Der Auftragsverarbeiter wird hierbei im erforderlichen Umfang mitwirken. Weiter wird der Auftragsverarbeiter dem Auftraggeber unverzüglich, spätestens aber innerhalb von 3 Werktagen, jede gewünschte Auskunft über die Verarbeitung der Auftraggeberdaten geben und entsprechende Nachweise zur Verfügung stellen, sofern der Auftraggeber nicht selbst über die entsprechenden Informationen verfügt. Der Auftraggeber wird Überprüfungen nur im erforderlichen Umfang durchführen und angemessene Rücksicht auf die Betriebsabläufe des Auftragsverarbeiters nehmen. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig.

12. Der Auftragsverarbeiter stellt sicher und kontrolliert regelmäßig, wenigstens einmal jährlich, dass die Datenverarbeitung und -nutzung im Rahmen dieses Vertrags und des möglichen Hauptvertrags in Übereinstimmung mit den jeweils geltenden datenschutzrechtlichen Vorschriften erfolgt.
13. Der Auftragsverarbeiter bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften, insbesondere der DS-GVO bekannt sind.
14. Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.
15. Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter werden zudem regelmäßig, wenigstens einmal jährlich hinsichtlich der einzuhaltenden datenschutzrechtlichen Vorgaben geschult. Auf Verlangen des Auftraggebers wird der Auftragsverarbeiter dem Auftraggeber die Verpflichtung der Mitarbeiter schriftlich oder in elektronischer Form nachweisen.
16. Beim Auftragsverarbeiter ist für den Datenschutz bestellt:

clever datenschutz GmbH
Frau Mandy Hruby
privacy@nexis-secure.com

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

§6 Mitteilungspflichten des Auftragsverarbeiters bei Störungen der Verarbeitung und bei Verletzung des Schutzes personenbezogener Daten

1. Der Auftragsverarbeiter teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten unverzüglich, spätestens aber innerhalb von

24 Stunden in Schriftform oder elektronischer Form mit. Dasselbe gilt für Prüfungen des Auftragsverarbeiters durch die Datenschutz-Aufsichtsbehörde. Die Meldungen gemäß Satz 1 enthalten jeweils zumindest die in Art. 33 Abs. 3 DS-GVO genannten Angaben. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO.

2. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:
 - a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
 - b. eine Beschreibung der vom Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
3. Der Auftragsverarbeiter trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und informiert hierüber den Auftraggeber.
4. Der Auftragsverarbeiter sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO).
5. Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. §4 dieses Vertrages durchführen.
6. Sollten die Auftraggeberdaten beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragsverarbeiter wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegen.

§7 Unterauftragsverhältnisse mit Subunternehmern

1. Ein Unterauftragsverhältnis mit Subunternehmern liegt vor, wenn der Auftragsverarbeiter weitere Auftragsverarbeiter mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistungen beauftragt.
2. Der Auftragsverarbeiter ist nicht zur Beauftragung von Subunternehmern befugt, es sei denn der Auftraggeber hat eine explizite Beauftragung eines bestimmten, vom Auftragsverarbeiter festgelegten Subunternehmers oder Subunternehmern genehmigt. In diesem Fall ist ein Unterauftragsverhältnis ausschließlich mit den genehmigten Subunternehmern erlaubt, solange diese analog zu diesem Auftragsverarbeitungsvertrag zur Einhaltung der Pflichten vertraglich verpflichtet werden. Eine Ersetzung bestehender genehmigter Subunternehmer gilt als Neubeauftragung im Sinne dieser Klausel. Die Weiterleitung von Daten an den

Subunternehmer ist erst dann zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO erfüllt hat.

3. Der Auftragsverarbeiter hat dem Auftraggeber mindestens den Namen und die Anschrift mitzuteilen sowie für welche Tätigkeit der Subunternehmer eingesetzt werden soll. Der Auftragsverarbeiter hat die Eignung des Subunternehmers insbesondere unter Berücksichtigung der technischen und organisatorischen Maßnahmen zum Schutz der Datenverarbeitung sorgfältig zu prüfen und die Unterlagen hierzu dem Auftraggeber zur Verfügung zu stellen.
4. Bei einer Beauftragung von Subunternehmern in Drittstaaten gilt zusätzlich § 1 Nr. 3 dieses Vertrags.
5. Der Auftragsverarbeiter haftet gegenüber dem Auftraggeber für die Einhaltung der datenschutzrechtlichen Pflichten durch den Subunternehmer.
6. Zum Zeitpunkt des Vertragsschlusses sind für den Auftragsverarbeiter die folgenden Subunternehmer tätig:

a. Name, Anschrift, Auftragsinhalt (Tätigkeitsbereich)

b. ...

Der Auftraggeber erklärt sich mit deren Beauftragung einverstanden.

§8 Technische und Organisatorische Maßnahmen

1. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.
2. Das im Anhang A beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragsverarbeiter dar.
3. Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO).
4. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragsverarbeiter und Auftraggeber abzustimmen.
5. Soweit die beim Auftragsverarbeiter getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftragsverarbeiter unverzüglich.
6. Die Maßnahmen beim Auftragsverarbeiter können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen

aber die vereinbarten Standards nicht unterschreiten. Wesentliche Änderungen muss der Auftragsverarbeiter mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

§9 Verpflichtung des Auftragsverarbeiters nach Beendigung des Auftrags

1. Der Auftragsverarbeiter wird dem Auftraggeber nach Beendigung des Vertrags alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Die Parteien werden bei Bedarf die Art und Weise der Löschung abstimmen. Die Löschung hat in jedem Fall datenschutzgerecht zu erfolgen. Der Auftragsverarbeiter wird die Löschung und Rückgabe auf Wunsch schriftlich bestätigen.
2. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

§11 Schlussbestimmungen

1. Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.
2. Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
3. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Die Parteien werden sich bemühen, die unwirksamen Teile der Vereinbarung durch solche zu ersetzen, die dem Willen der Parteien im Zeitpunkt des Vertragsschlusses am nächsten kommt, aber wirksam ist. Dasselbe gilt im Falle der Undurchsetzbarkeit einer Vorschrift oder bei Regelungslücken.
4. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Selbiges gilt für Nebenabreden zu diesem Vertrag. Mündliche Nebenabreden haben zum Zeitpunkt des Vertragsschlusses nicht bestanden.
5. Diese Vereinbarung unterliegt deutschem Recht. Alleiniger Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist Regensburg.

Regensburg, den 20. Oktober 2026

Dr. Michael Kunz

Geschäftsführer, Nexis GmbH

Regensburg, den 20. Oktober 2026

Max Mustermann

Geschäftsführer

Anhang A – Technisch-Organisatorische Maßnahmen des Auftragsverarbeiters

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)

Zutrittskontrolle

- 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

Zugangskontrolle

- Login mit Benutzername & Passwort
- Login mit 2-Faktor-Authentifizierung
- Anti-Virus-Software Server
- Anti-Virus-Software Clients
- Firewall
- Verschlüsselung von Datenträgern
- Automatische Desktopsperrung
- Benutzerberechtigungskonzept
- Administrierte Benutzerverwaltung
- Zwingende Passwortanforderungen
- Clean Desk Richtlinie
- Mobile Device Policy
- Remote Working Policy

Zugriffskontrolle

- 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 Severraum
- RAID-System / Festplattenspiegelung
- Videoüberwachung Severraum
- Alarmmeldung bei unberechtigtem Zutritt zum Severraum
- 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 Verzeichnisse 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