Vereinbarung zur Auftragsverarbeitung

Regelungen zu Datenschutz und Datensicherheit in Auftragsverhältnissen

Präambel
Diese Vereinbarung zur Auftragsvereinbarung spiegelt die Vereinbarung der Parteien in Bezug auf die Bedingungen wider, die die Verarbeitung der personenbezogenen Daten des Kunden (nachfolgend „Auftraggeber“ genannt) durch die **Nemo GmbH, Auf dem Immel 8, 67685 Weilerbach** (nachfolgend „Auftragnehmer“ genannt) unter den zwischen den Parteien bestehenden Vertragsverhältnisses regeln. Die Vereinbarung zur Auftragsvereinbarung wird durch Bezugnahme in jeweiligen Vertragsdokumenten zwischen den Parteien rechtswirksam als Anlage in die zwischen den Parteien bestehenden Vertragsverhältnis aufgenommen.

Der Auftragnehmer verarbeitet im Zuge der im Rahmen des Hauptvertrages beauftragten Dienstleistungauch personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers.

Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung aus Art. 28 DSGVO zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

1 Gegenstand des Auftrags, Art und Zweck der Verarbeitung
1) Der Gegenstand des Auftrags sowie Art und Zweck der Verarbeitung ergeben sich aus **Anlage 1**.

(2) 2) Im Übrigen ergibt sich der Gegenstand des Auftrags aus dem Angebot, den AGB und allen weiteren dort in Bezug genommenen Dokumenten auf, die hier verwiesen wird (im Folgenden „Vertrag“).

2 Art der personenbezogenen Daten, Kategorien betroffener Personen
(1) Art der Daten:

Die Art der personenbezogenen Daten ergibt sich aus **Anlage 1**.

(2) Kreis der betroffenen Personen:

Der Kreis der betroffenen Personen ergibt sich aus **Anlage 1**.

3 Dauer des Auftrages
Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Vertrags.

4 Verantwortlichkeit und Weisungsbefugnis

(1) Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DSGVO). Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Etwas anderes gilt nur in dem in Absatz 2 genannten Umfang.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn es besteht eine anderweitige Verpflichtung durch Unionsrecht oder dem Recht des Mitgliedsstaates, dem der Auftragnehmer unterliegt. Im Falle einer anderweitigen Verpflichtung teilt der Auftragnehmer dem Auftraggeber vor der Verarbeitung unverzüglich die entsprechenden rechtlichen Anforderungen mit.

(3) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er gemäß Art. 28 Abs. 3 S. 3 DSGVO unverzüglich den Auftraggeber. Bis zur Bestätigung oder Änderung der entsprechenden Weisung ist der Auftragnehmer berechtigt, die Durchführung der Weisung auszusetzen.

5 Vertraulichkeit

Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO auf die Vertraulichkeit verpflichtet worden sind und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

6 Datensicherheit

(1) Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten gemäß Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Dazu wird der Auftragnehmer

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sicherstellen sowie
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung unterhalten.

Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(2) Die Vertragsparteien vereinbaren die in dem **Anlage 3** zu dieser Vereinbarung niedergelegten konkreten Datensicherheitsmaßnahmen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber schriftlich mitzuteilen.

7 Einbeziehung weiterer Auftragsverarbeiter (Subunternehmer)

(1) Als Subunternehmer im Sinne dieser Regelung gelten vom Auftragnehmer beauftragte Auftragsverarbeiter, deren Dienstleistungen sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht dazu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen und Reinigung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer erteilt dem Auftraggeber hiermit die allgemeine Genehmigung zur Hinzuziehung von Subunternehmern: Die Liste (Anlage 2) findet sich im Trustcenter unter (https://www.nemo-ai.com/trust-center). Über den geplanten Einsatz eines weiteren Subunternehmers oder den Austausch eines bestehenden Subunternehmers hat der Auftragnehmer den Auftraggeber rechtzeitig vorab zu informieren. Die Information erfolgt durch Bekanntgabe im Kundenportal bzw. via Newsletter sowie im Trustcenter. Die Zustimmung zur Untervergabe gilt als erteilt, wenn der Auftraggeber nicht innerhalb von 6 (sechs) Wochen, beginnend mit Zugang der Information in vorstehendem Sinne, dem Einsatz des betreffenden Subunternehmers widerspricht. Ein solcher Widerspruch ist nur aus berechtigten Gründen zulässig, wie z. B. nicht ausreichende Zuverlässigkeit des Subunternehmers. Widerspricht der Auftraggeber dem Einsatz eines vom Auftragnehmer gewünschten Subunternehmers, so ist der Auftragnehmer berechtigt, den Hauptvertrag ohne Einhaltung einer Kündigungsfrist und mit sofortiger Wirkung zu kündigen.

(3) Mit dem Subunternehmer ist eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 3 und 4 DSGVO abzuschließen, die den Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit dieser Vereinbarung entspricht.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subunternehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Die Verarbeitung der Daten durch den Auftragsverarbeiter und die vom Verantwortlichen genehmigten Subdienstleister findet grundsätzlich in Mitgliedstaaten der Europäischen Union, Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und/oder solchen Ländern statt, für die ein gültiger, auf die Verarbeitung anwendbarer Angemessenheitsbeschluss der Kommission im Sinne des Art. 45 Abs. 3 DSGVO vorliegt. Es ist dem Auftragsverarbeiter gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb der EU/ des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und sicherstellt, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU- Standarddatenschutzklauseln). Die Regelung aus 7 (2) dieser Vereinbarung gilt somit auch für die Beauftragung von Subdienstleistern im Drittstaat.

(6) Eine weitere Auslagerung durch den Subunternehmer bedarf der Genehmigung des Auftragnehmers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Subunternehmer aufzuerlegen.

8 Unterstützung bei der Wahrung von Betroffenenrechten

(1) Der Auftragnehmer ist verpflichtet, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Wahrung der in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen zu unterstützen (Art. 28 Abs. 3 S. 2 lit. e DSGVO). Insbesondere wird der Auftragnehmer den Auftraggeber darin unterstützen, Ansprüche Betroffener auf Löschung ihrer personenbezogenen Daten gemäß Art. 17 DSGVO zu erfüllen.

(2) Der Auftragnehmer darf personenbezogene Daten nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken (Art. 28 Abs. 3 S. 2 lit. g DSGVO). Auskünfte an Dritte oder den betroffenen Personen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(3) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, um ihre Rechte gemäß Art. 12 bis 22 DSGVO geltend zu machen, wird der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterleiten.

9 Unterstützung bei Dokumentations- und Meldepflichten

(1) Ist der Auftragnehmer nach Art. 37 DSGVO, § 38 BDSG gesetzlich dazu verpflichtet, einen Datenschutzbeauftragten zu benennen, teilt der Auftragnehmer dem Auftraggeber die Kontaktdaten des Datenschutzbeauftragten auf Anfrage zum Zweck der direkten Kontaktaufnahme mit.

(2) Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Auftraggeber unverzüglich Art. 28 Abs. 3 lit. f, Art. 33 Abs. 2 DSGVO. Das Gleiche gilt, wenn beim Auftragnehmer beschäftigte Personen gegen diese Vereinbarung verstoßen.

(3) Nach Absprache mit dem Auftraggeber trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen.

(4) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Erfüllung der Informationspflichten gegenüber der zuständigen Aufsichtsbehörde gemäß Art. 33 DSGVO und ggf. gegenüber den von der Verletzung des Schutzes personenbezogener Daten Betroffenen gemäß Art. 34 DSGVO.

(5) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei einer vorherigen Konsultation der zuständigen Aufsichtsbehörde gemäß Art. 36 DSGVO.

(6) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

10 Beendigung des Auftrages

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, vor Beginn der Verarbeitungsleistungen und währenddessen regelmäßig die technischen und organisatorischen Maßnahmen sowie die Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zu kontrollieren. Dazu kann der Auftraggeber oder ein beauftragter Prüfer die Datenverarbeitungsanlagen und die Datenverarbeitungsprogramme des Auftragnehmers inspizieren.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, nach Anmeldung und unter Berücksichtigung einer angemessenen Vorlaufzeit (mindestens 72 Zeitstunden, werktäglich) durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem direkten Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist diejenigen Auskünfte zu erteilen, die zum Nachweis der Einhaltung der Pflichten unter diesem Auftragsverarbeitungsvertrag sowie zum Nachweis der technischen und organisatorischen Maßnahmen erforderlich sind. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, ITSicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit vorlegen. Der Auftraggeber hat dem Auftragnehmer den durch die Erteilung der Auskünfte entstehenden Aufwand zu vergüten.

12 Haftung

Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schäden, die eine Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind sowohl der Auftraggeber als auch der Auftragnehmer für einen solchen Schaden gemäß Art. 82 Abs. 2 DSGVO verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadensersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit es ihrem Anteil an der Verantwortung entspricht.

13 Schlussbestimmungen

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

(2) Sollten einzelne oder mehrere Regelungen dieser Vereinbarung unwirksam sein, so wird die Wirksamkeit der übrigen Vereinbarung hiervon nicht berührt. Für den Fall der Unwirksamkeit einzelner oder mehrere Regelungen werden die Vertragsparteien die unwirksame Regelung unverzüglich durch eine solche Regelung ersetzen, die der unwirksamen Regelung wirtschaftlich und datenschutzrechtlich am ehesten entspricht.

(3) Im Falle eines Widerspruchs zwischen dem Hauptvertrag und dieser Vereinbarung geht diese Vereinbarung vor, soweit der Widerspruch die Verarbeitung personenbezogener Daten betrifft.

(4) Die folgenden Anhänge sind Bestandteil dieser Vereinbarung:

- Anlage 1: Angaben zur Datenverarbeitung
- Anlage 2: Genehmigte Subunternehmer
- Anlage 3: Technische und organisatorische Maßnahmen

Anlage 1

Angaben zur Datenverarbeitung (Art. 28 Abs. 3 S. 1 DSGVO)

Nemo

Der Auftragnehmer betreibt unter der Bezeichnung „Nemo“ verschiedene Applikationen, hinsichtlich deren Nutzung ein Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer besteht. Diese Applikationen betreffen insbesondere den Bereich „Business Intelligence / Advanced Analytics“ und enthalten anonymisierte Transaktionsdaten entlang der Wertschöpfungskette des Unternehmens (Angebot, Auftrag, Lieferung, Rechnung). Die Art und der Umfang der Nutzung bzw. Bereitstellung der Daten liegt in der Entscheidung des Auftraggebers und somit in dessen Sphäre.

Gegenstand der Verarbeitung	Art der Daten	Kreis der Betroffenen	Zweck
Administrative Module: Austausch personenbezogener Daten zwischen Auftragnehmer und Auftraggeber	Userdaten (insbes. Name, E-Mail-Adresse)	Beschäftigte des Auftraggebers	Benutzerverwaltung und Bereitstellung von Funktionalitäten
Nemo-Module: Aufbau von Datenstrukturen nach Weisung des Auftraggebers; Anonymisierung von Datensätzen zum Zwecke der Analyse nach Weisung des Auftraggebers	Sämtliche Daten, die im Rahmen der auftraggeberseitig bereitgestellten Datenstrukturen verarbeitet werden.	Beschäftige, Kunden, Lieferanten des Auftraggebers	Konfiguration von Analysefaktoren Entspricht dem jeweils vom Auftraggeber im Einzelfall festgelegten Zweck.
Support, Wartung und Consulting: Nicht auszuschließende Einsicht in verarbeitete Datensätze im Falle von Fernzugriffen durch Beschäftigte des Auftragnehmers	Sämtliche Daten, die im Rahmen der auftraggeberseitig bereitgestellten Datenstrukturen verarbeitet werden.	Beschäftige, Kunden, Lieferanten des Auftraggebers	Durchführung von erforderlichen Wartungen und Supportdienstleistungen, bei denen ein Zugriff auf personenbezogene Daten des Auftraggebers nicht ausgeschlossen werden kann.

Optionale Module:			
Nemo Genius und Nemo GenAIzer: Tools zur Erweiterung und Unterstützung der KI-basierten Datenbankanalyse durch Anbindung an OpenAI.	Per Default werden nur statistisch ermittelte, sowie Metadaten oder Sample-Daten übergeben. Nach individueller Konfiguration des Kunden, können Daten auch personenbezogen sein.	Beschäftige, Kunden, Lieferanten des Auftraggebers	Dynamische Generierung von Inhalten

InfoZoom

Der Auftragnehmer bietet unter der Bezeichnung „InfoZoom“ eine Software-Applikation zur Bearbeitung und Analyse von Massendaten an. Hinsichtlich der Nutzung besteht ein Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer. Diese Applikation betrifft insbesondere die Bereiche „Datenanalyse / Ad-hoc Reporting“. Die Art und der Umfang der Nutzung bzw. Bereitstellung der Daten liegt in der Entscheidung des Auftraggebers und somit in dessen Sphäre.

Gegenstand der Verarbeitung	Art der Daten	Kreis der Betroffenen	Zweck
Support, Wartung und Consulting: Nicht auszuschließende Einsicht in verarbeitete Datensätze im Falle von Fernzugriffen durch Beschäftigte des Auftragnehmers	Sämtliche Daten, die im Rahmen der auftraggeberseitig bereitgestellten Datenstrukturen verarbeitet werden.	Beschäftige des Auftraggebers	Durchführung von erforderlichen Wartungen und Supportdienstleis-tungen, bei denen ein Zugriff auf personenbezogene Daten des Auftraggebers nicht ausgeschlossen werden kann.

Academy

Der Auftragnehmer stellt dem Auftraggeber ein E-Learning-Angebot zur Verfügung, um Nutzern systemspezifische Fachschulungen zu ermöglichen und deren Durchführung zu dokumentieren.

Gegenstand der Verarbeitung	Art der Daten	Kreis der Betroffenen	Zweck
Bereitstellung von E-Learning-Angeboten	Personenstammdaten Lernfortschritt	Nutzer des E-Learning-Angebots	Durchführung und Dokumentation von fachlichen Schulungen

Anlage 2

Genehmigte Subunternehmer

Subunternehmer	Verarbeitungs-tätigkeit	Ort der Datenverarbeitung	Geeignete Garantien, Art. 44 ff. DSGVO (falls erforderlich)	Zusätzliche Maßnahmen zum Schutz personen-bezogener Daten (falls erforderlich)
AWS Europe SARL 38, avenue John F. Kennedy, L-1855 Luxembourg	Bereitstellung Serverlandschaft für Cloudbetrieb „Nemo“	EU	n/a	Serverstandort Frankfurt am Main (ISO/IEC) 27001-zertifiziert)
Proalpha Group GmbH, Auf dem Immel 8, 67685 Weilerbach	Shared Service Center des Auftragnehmers	DE	n/a	
WIBU-SYSTEMS AG, Zimmerstraße 5, 76137 Karlsruhe	Verwaltung der Lizenzen	DE	n/a	
ServiceNow Nederland B.V., Hoekenrode 3, Amsterdam 1102 BR	Verwaltung von Supportcases, Casebearbeitung	EU	EU Standardvertrags-klauseln	

Subdienstleister bei Nutzung von Nemo GenAIzer und Nemo Genius (optional auswählbar):				
OpenAI Ireland Ltd 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Irland	KI-gestützte Datenbankauswertung	EU/USA	EU-Standardvertrags-klauseln	

Anlage 3

1. Technische und organisatorische Maßnahmen

Die Proalpha-Gruppe verfolgt ein übergreifendes Standortsicherheitskonzept. Dieses ist, mit Aus-nahme einer standortspezifischen Zutrittskontrolle, hinsichtlich der weiteren TOM übergreifend verbindlich definiert.

In der hier vorliegenden Beschreibung über den aktuellen Stand der grundlegenden Maßnahmen zum Schutz der Daten wird einschränkend darauf hingewiesen, dass verständlicherweise nicht alle Sicherheitsmaßnahmen im Detail offengelegt werden können. Gerade in Bezug auf Datenschutz und Datensicherheit ist der Verzicht auf vertrauliche und detaillierte Beschreibungen unabdingbar, da der Schutz der Sicherheitsmaßnahmen gegen unbefugte Offenlegung mindestens genauso wichtig ist wie die Sicherheitsmaßnahmen selbst.

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

- Sicherheitsschlösser
- Zutrittsberechtigungskonzept / Zonenschutzkonzept
- Manuelles Schließsystem
- Schließsystem mit Codesperre
- Chipkarten-Schließsystem
- Rechenzentren mit Standort in Deutschland oder der EU
- Rechenzentren zertifiziert nach ISO 27001
- separate IT-Verteilerräume
- Personenkontrolle beim Pförtner / Empfang
- Protokollierung der Besucher / Besucherbuch

2.2 Zugriffskontrolle

Das Eindringen Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung ist zu verhindern.

- Security Operation Center mit 24/7 SIEM vorhanden
- Berechtigungskonzept: Privilege Access Management (PAM) nach Need-to-Use und Need-to-Know-Prinzip
- Getrenntes Gäste-WLAN
- Personalisierte Benutzerprofile
- Authentifikation mit Benutzer + Passwort sowie MFA

- Passwortregelungen entsprechen den aktuellen BSI-Empfehlungen
  - Verwendung von individuellen Passwörtern
  - Passwörter mit einer Mindestlänge und voller Komplexität. PW-Länge ist abhängig von der privilegierten Rolle, jedoch min. 10 Zeichen.
  - Anzahl von aufeinanderfolgenden Fehlversuchen ist begrenzt
  - Passworthistorie
- Schlüsselregelung gem. Krypto-Richtlinie
- Verschlüsselung von mobilen Datenträgern
  - Für Windows: Bitlocker
  - Für MAC: Vault
- Autonome Fernwartung
- Bestandteil des Sicherheitskonzeptes der Pa-Gruppe
- Global Secure Access sowie VPN
- Regelmäßige Prüfung der Accounts
- Protokollierung der Serverzugriffe auf Benutzerebene
- Versschlüsselung sowohl bei Übertragung als auch Data-at-Rest
- Physische Löschung von Datenträgern vor deren Wiederverwendung
- Einsatz von VPN-Technologie
- Einsatz von Next Generation Firewalls und Web Application Firewalls
- Einsatz von Anti-Viren-Software

2.3 Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

- Festlegung von Datenbankrechten über PAM
- VLAN-Konzept für eine logische Trennung der Netzsegmentierung
- Trennung von Produktiv-, Test- und Prüfumgebung
- Logische Mandantentrennung (softwareseitig)
- Regelmäßige Audits (intern/extern)

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Weitergabekontrolle

- Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln.
- Elektronische Übertragung, Datentransport, sowie deren Kontrolle.
- Einsatz von verschlüsselten Verbindungen (z.B. VPN, HTTPS, SMIME, SFTP, TLS 1.2/1.3)
- Shredder für die sichere Vernichtung von Daten
- Datenschutzboxen für die Entsorgung von vertraulichen Papierdokumenten

3.2 Eingabekontrolle

- Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.
- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten auf Benutzerebene für z.B. File Shares
- Protokollierung der Änderung und Löschung von Daten
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Dezidierter Logserver und Security Operation Center (SOC)

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

4.1 Verfügbarkeitskontrolle und Belastbarkeit

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen. Systeme müssen die Fähigkeit besitzen mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.

- Backup- & Recoverykonzept nach 3-2-1 Prinzip (Immutable Backups)
- Testen von Datenwiederherstellung
- On-Prem-Systeme sind redundant über zwei Rechenzentren ausgelegt
- Jährliche Pen-Tests
- Klimaanlage in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Serverräume mit Wassersensor ausgestattet
- Unterbrechungsfreie Stromversorgung (USV)

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

5.1 Kontrollverfahren

Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren.

- Information Security Management System (ISMS) vorhanden
- Unternehmensrichtlinien (Code of Conduct) vorhanden
- Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten
- Es werden datenschutzfreundliche Voreinstellungen gewählt
- Datenschutz-Management vorhanden
- Datenschutz-Konzept vorhanden
- Auftragskontrolle: Vertragsgestaltung gem. gesetzlichen Vorgaben (§ 11 BDSG; Art. 28 DSGVO)

6. Technische und Organisatorische Maßnahmen im Home Office

Die Proalpha-Gruppe ermöglicht ihren Mitarbeitenden, anfallende Arbeiten via Remote-Zugang durchzuführen. Hierfür wurden Maßnahmen ergriffen, die dem Stand der Technik entsprechen.
Die Maßnahmen unterteilen sich jeweils in **technische** Maßnahmen, sowie in **organisatorische** Maßnahmen

6.1 Technische Maßnahmen

Für den Zugriff auf das System aus dem „Home Office“ oder „Remote“ hat Proalpha folgende Maßnahmen getroffen:

- Zugang ausschließlich über dienstliche Endgeräte erlaubt
- Endgeräte unterliegen regelmäßigen Updates
- Applikationen werden ausschließlich über Unternehmensportal von der IT zur Verfügung gestellt.
- Ein Zugriff erfolgt generell über Global Secure Access. Für einzelne Anwendungen zusätzlich über eine verschlüsselte VPN-Verbindung sowie MFA
- Windows- und MacOS Clients werde über MDM verwaltet
- Endpoint Security
  - Antivirus Software
  - Systemverschlüsselung
  - Systemhärtung
- Proxy zur Domainfilterung
  - restriction policy
    - nicht vertrauenswürdige Zertifikate können nicht manuell akzeptiert werden
    - keine Diagnosedaten an Apple
    - Benutzer kann keinen 3rd-Party Apps manuell vertrauen

6.2 Organisatorische Maßnahmen

In organisatorischer Hinsicht wurden in Ergänzung zu den Maßnahmen der allgemeinen TOM verschiedene Zusatzvereinbarungen sowie interne Richtlinien (in Abstimmung mit dem Betriebsrat) erlassen. Dies umfasst unter anderem Folgende Regelungen und Verpflichtungen:

- IT Policy: regelt den sicheren Umgang mit IT-Assets (Auch Privatnutzung)
- Verpflichtung auf interne Richtlinie zur Nutzung technischer Einrichtungen
- Verpflichtung zum Schutz des Zugriffs unbefugter Dritter auf Arbeitsmittel
- Untersagung der Verwendung eigener technischer Einrichtungen (Ausgenommen WLAN, Peripheriegeräten wie Tastatur und Maus ohne Treiberinstallation)
- Verpflichtung, vertrauliche dienstliche Dokumente unter Verschluss zu halten
- Verpflichtung auf Vertraulichkeit / zur Geheimhaltung
- Verpflichtung, Wohnortswechsel mitzuteilen
- Jährlich stattfindende Schulungen