

Allgemeine Nutzungsbedingungen von Net at Work für den Service „Rimscout“

(Stand: April 2024)

Präambel

Rimscout ist ein Service der Net at Work GmbH, der das IT-Netzwerk des Unternehmens aus der Nutzerperspektive überwacht, um netzwerkbezogene Probleme zu erkennen und zu lösen. Rimscout besteht aus zwei Komponenten: Clients und dem Portal. Der Rimscout Client führt kontinuierlich Netzwerk-Konnektivitätstests aus, um nützliche Systeminformationen und Verbindungsdaten zu sammeln. Diese Daten werden an das Rimscout-Portal übermittelt. Das Rimscout Portal ist eine Web-Applikation, in der die Daten aller Clients analysiert werden können, um Trends und Anomalien zu erkennen.

1 Anwendungsbereich

1.1

Diese Nutzungsbedingungen gelten für alle Geschäftsbeziehungen zwischen der Net at Work GmbH mit Sitz in Paderborn (nachfolgend: „Net at Work“) und ihren Kunden betreffend die Nutzung der Software „**Rimscout**“ (nachfolgend: „Software“) als Software-as-a-Service („SaaS“).

Das Angebot von Net at Work richtet sich ausschließlich an Unternehmer (§ 14 BGB), juristische Personen des öffentlichen Rechts und an öffentlich-rechtliches Sondervermögen.

1.2

Diese Nutzungsbedingungen gelten stets und ausschließlich. Abweichende, entgegenstehende oder ergänzende Allgemeine Geschäftsbedingungen des Kunden werden nur dann und insoweit Vertragsbestandteil, als Net at Work ihrer Geltung ausdrücklich schriftlich zugestimmt hat.

Im Einzelfall getroffene, individuelle Vereinbarungen mit dem Kunden (einschließlich Nebenabreden, Ergänzungen und Änderungen) haben in jedem Fall Vorrang vor diesen Nutzungsbedingungen. Für den Inhalt derartiger Vereinbarungen ist, vorbehaltlich des Gegenbeweises, ein schriftlicher Vertrag bzw. die schriftliche Bestätigung von Net at Work maßgebend.

1.3

Hinweise auf die Geltung gesetzlicher Vorschriften haben nur klarstellende Bedeutung. Auch ohne eine derartige Klarstellung gelten daher die gesetzlichen Vorschriften, soweit sie in diesen Nutzungsbedingungen nicht unmittelbar abgeändert oder ausdrücklich ausgeschlossen werden.

2 Vertragsgegenstand

2.1

Gegenstand des Vertrages ist die entgeltliche und zeitlich auf die Dauer des Vertrages begrenzte Gewährung der Nutzung der Software durch den Kunden über das Internet sowie die Bereitstellung von Speicherplatz auf Servern von Net at Work oder einem von Net at Work beauftragten Subunternehmer.

Einzelheiten ergeben sich aus der jeweils aktuell gültigen Funktionsumfangbeschreibung, abrufbar unter www.rimscout.com (nachfolgend: „**Website**“), und den vereinbarten Verfügbarkeiten und weiteren Supportleistungen unter Ziffern 3, 5 und 6. Der nutzbare Funktionsumfang ergibt sich aus den vom Kunden lizenzierten Funktionsmodulen der Software.

2.2

Die Funktionsumfangbeschreibung ist maßgeblich für die Funktionen und Eigenschaften der Software. Net at Work schuldet nur die Anpassung an den Stand der Technik und nicht an die Bedürfnisse des Kunden.

3 Leistungen von Net at Work, Software, Speicherplatz

3.1

Net at Work gewährt dem Kunden die Nutzung der jeweils aktuellen Version der Software über das Internet für die vereinbarte Anzahl an Clients zum Einliefern von Messdaten und Portal-Usern mittels Zugriff auf einen Administrationsbereich (Rimscout Portal). Als Client zählt jedes Endgerät, das die Rimscout Software ausführt und Daten an das Rimscout Portal liefert. Als Portal User zählt jede natürliche Person, die über Zugangsdaten zum Rimscout Portal verfügt.

Die einem Endgerät zugewiesene Client-Lizenz kann frühestens nach 30 Tagen einem anderen Endgerät zugeordnet werden (Cool-Down-Periode).

Je Client ist die Anzahl der gleichzeitig ausgeführten Tests auf 20 beschränkt. Ein Test ist ein definierter Messvorgang. Die durchschnittliche Laufzeit eines Clients pro Tag ist auf 13 Stunden limitiert. Die Daten-API ist hinsichtlich der Menge und Geschwindigkeit der Datenabfragen limitiert. Details dazu finden sich in der Produktdokumentation. Messdaten werden über einen Zeitraum von 45 Tagen verfügbar gehalten. Sofern diese Werte überschritten werden, begrenzt Net at Work auf die limitierten Werte und lehnt über die Werte hinausgehende Leistungen ab.

Wird eine schädliche Nutzung des Systems festgestellt, kann Net at Work die Verarbeitung von Daten begrenzen oder andere geeignete Maßnahmen nach eigener Wahl ergreifen, um Schaden für den Kunden und die Software-Plattform Rimscout zu vermeiden.

Testversionen von Rimscout dürfen nicht produktiv oder zu Erwerbszwecken eingesetzt werden.

3.2

Net at Work gewährleistet die Funktionsfähigkeit und Verfügbarkeit der Software während der Dauer des Vertragsverhältnisses und wird diese in einem zum vertragsgemäßen Gebrauch geeigneten Zustand erhalten. Der Funktionsumfang der Software sowie die Einsatzbedingungen ergeben sich aus der jeweils aktuellen Funktionsumfangbeschreibung bzw. dem Produktblatt, abrufbar auf der Website.

3.3

Net at Work kann die Software jederzeit aktualisieren und/oder weiterentwickeln (insbesondere durch Patches, Updates und Upgrades) und insbesondere aufgrund einer geänderten Rechtslage, technischer Entwicklungen und zur Verbesserung der IT-Sicherheit anpassen. Net at Work kann zudem die Software anpassen, wenn (i) die Anpassungen für den Kunden von Vorteil sind und/oder (ii) die Anpassungen nur technischer oder verfahrenstechnischer Natur sind und keine wesentlichen Auswirkungen auf den Kunden haben.

Net at Work wird dabei die berechtigten Interessen des Kunden angemessen berücksichtigen und den Kunden -sofern möglich- rechtzeitig über notwendige Anpassungen informieren.

Im Falle einer wesentlichen Beeinträchtigung der berechtigten Interessen des Kunden steht diesem ein Sonderkündigungsrecht des Vertrages zum Änderungstermin zu. Die Kündigung muss innerhalb von zwei Wochen nach Erhalt der Nachricht über die Anpassung der Leistung/ Software durch den Kunden erfolgen.

3.4

Net at Work wird die Software regelmäßig warten und bietet dem Kunden die Möglichkeit sich über etwaige hiermit verbundene Einschränkungen informieren. Die Wartung wird regelmäßig außerhalb der üblichen Geschäftszeiten des Kunden durchgeführt, es sei denn, aufgrund zwingender Gründe muss eine Wartung zu einer anderen Zeit vorgenommen werden

3.5

Net at Work stellt dem Kunden für Zwecke der Nutzung der Software-Leistungen auf Servern bis zu dem im Auftrag vereinbarten Umfang zur Verfügung.

3.6

Es werden dem Stand der Technik entsprechende Maßnahmen zum Schutz der Daten von Net at Work vorgenommen. Net at Work treffen jedoch keine Verwahrungs- oder Obhutspflichten hinsichtlich der Daten.

3.7

Leistungs- und Erfüllungsort für die von Net at Work zu erbringenden Leistungen ist stets der Sitz von Net at Work.

4 Nutzungsumfang und -rechte an der Software

4.1

Eine physische Überlassung der Software an den Kunden erfolgt nicht.

4.2

Der Kunde erhält an der jeweils aktuellen Version der Software für die vertraglich festgelegte Anzahl an Clients und Portal Usern einfache, d.h. nicht unterlizenzierbare und nicht übertragbare, zeitlich auf die Dauer des Vertrags beschränkte Rechte, die Software mittels Zugriff auf einen Administrationsbereich nach Maßgabe der vertraglichen Regelungen zu nutzen. Dies gilt auch für verbundene Unternehmen nach § 15 Aktiengesetz.

4.3

Der Kunde darf die Software nur im Rahmen seiner eigenen geschäftlichen Tätigkeit durch eigenes Personal nutzen. Dem Kunden ist eine weitergehende Nutzung der Software nicht gestattet. Dies gilt auch für verbundene Unternehmen nach § 15 Aktiengesetz.

5 Support

5.1

Zum Support gehört die Beseitigung von reproduzierbaren Programmfehlern sowohl innerhalb des Programmcodes als auch innerhalb der Onlinedokumentation. Ein Programmfehler in diesem Sinne liegt vor, wenn die Software bei vertragsgemäßer Nutzung die in der Funktionsumfangsbeschreibung vereinbarten Leistungen nicht erbringt und sich dies auf deren vertragliche Gebrauchstauglichkeit nicht nur unwesentlich auswirkt. Die Fehlerbeseitigung kann nach Wahl von Net at Work auch durch die Zurverfügungstellung einer neuen Programmversion erfolgen.

Kann ein Fehler im Einzelfall nicht sofort behoben werden, so wird Net at Work bis zur endgültigen Fehlerbeseitigung eine Zwischenlösung herbeiführen, der gegebenenfalls die Beachtung besonderer Bedienungsvorschriften durch den Kunden erfordert.

5.2

Net at Work richtet für Anfragen des Kunden zu Funktionen der Software einen Support-Service ein. Anfragen können über die auf der Website angegebene Support-Hotline zu den dort angegebenen Zeiten oder per E-Mail gestellt werden. Die Anfragen werden grundsätzlich in zeitlicher Reihenfolge ihres Eingangs bearbeitet. Eine Supportanfrage muss eine nachvollziehbare Beschreibung der Fehlersymptome enthalten und sollte eine Reproduktion des Fehlers ermöglichen.

6 Service Levels und Störungsbehebung

6.1

Net at Work gewährt eine Gesamtverfügbarkeit im Jahresmittel der Leistungen (Software) von mindestens 99,5% am Übergabepunkt bei einer Vertragslaufzeit von einem oder mehr Jahren. Der Übergabepunkt ist der Routerausgang des Rechenzentrums von Net at Work. Bei Verträgen mit monatlicher Laufzeit gewährt Net at Work eine Gesamtverfügbarkeit im Monatsmittel von 99% am Übergabepunkt bezogen auf die Gesamtverfügbarkeit im Jahresmittel von 99,5%.

6.2

Als Verfügbarkeit gilt die Möglichkeit des Kunden, sämtliche Hauptfunktionen der Software zu nutzen. Wartungszeiten sowie Zeiten der Störung unter Einhaltung der Behebungszeit gelten als Zeiten der Verfügbarkeit der Software. Zeiten unerheblicher Störungen bleiben bei der Berechnung der Verfügbarkeit ebenso außer Betracht wie Zeiten der Nichtverfügbarkeit aufgrund von Umständen, die außerhalb der Kontrolle von Net at Work liegen, insbesondere Fälle höherer Gewalt. Für den Nachweis der Verfügbarkeit sind die Messinstrumente von Net at Work im Rechenzentrum maßgeblich.

6.3

Der Kunde hat Störungen unverzüglich an die von Net at Work dazu eingerichteten Kontaktstellen zu melden. Eine Störungsmeldung und -behebung ist Montag bis Freitag (ausgenommen bundesweite Feiertage) zwischen 9:00 Uhr und 17:00 Uhr gewährleistet („**Servicezeiten**“).

6.4

Erhebliche Störungen (Haupt- oder Nebenfunktionen der Software sind gestört, können aber genutzt werden; oder andere nicht nur unerhebliche Störungen) werden spätestens binnen 12 Stunden innerhalb der Servicezeiten behoben (Behebungszeit). Sofern absehbar ist, dass eine Behebung der Störung nicht innerhalb dieser Zeitspanne möglich ist, wird Net at Work den Kunden hierüber unverzüglich informieren und die voraussichtliche Überschreitung der Zeitspanne mitteilen.

6.5

Die Beseitigung von unerheblichen Störungen liegt im Ermessen von Net at Work.

7 Pflichten des Kunden

7.1

Der Kunde hat die ihm übermittelten Zugangsdaten dem Stand der Technik entsprechend vor Zugriff Dritter zu schützen und zu verwahren. Der Kunde wird dafür sorgen, dass eine Nutzung nur im vertraglich vereinbarten Umfang geschieht. Ein unberechtigter Zugriff ist Net at Work gegenüber unverzüglich in schriftlicher Form mitzuteilen.

7.2

Nutzt der Kunde die Software, um Leistungen für seine Kunden (Endkunde) zu erbringen, ist er verpflichtet, die Bedingungen dieser Nutzungsvereinbarung auch mit seinen Kunden zu vereinbaren.

7.3

Der Kunde ist verpflichtet, auf dem zur Verfügung gestellten Speicherplatz keine Daten abzulegen, deren Nutzung gegen geltendes Recht, behördliche Anordnungen, Rechte Dritter oder Vereinbarungen mit Dritten verstößt. Der Kunde wird Net at Work von Ansprüchen, die Dritte aufgrund eines Verstoßes gegen diese Ziffer geltend machen, auf erstes Anfordern freistellen.

7.4

Der Kunde wird die Daten vor deren Ablage oder Nutzung in der Software auf Viren oder sonstige schädliche Komponenten prüfen und hierfür dem Stand der Technik entsprechende Maßnahmen (z.B. Virenschutzprogramme) einsetzen.

8 Zahlungsbedingungen

8.1

Die Preise und Kosten verstehen sich zuzüglich der jeweils geltenden Umsatzsteuer.

8.2

Sofern nichts anderes vereinbart, rechnet Net at Work zu Beginn des vereinbarten Abrechnungsintervalls der Vertragslaufzeit über ihre Leistungen ab. Zahlungen sind sofort und ohne Abzug fällig. Skonto wird nur bei ausdrücklicher schriftlicher Vereinbarung gewährt.

Bei Zahlungsverzug des Kunden schuldet dieser Verzugszinsen in Höhe des jeweils geltenden gesetzlichen Verzugszinssatzes.

8.3

Erfüllungsort für an Net at Work zu leistende Zahlungen ist der Sitz von Net at Work.

8.4

Der Kunde kann nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen aufrechnen.

9 Gewährleistung

9.1

Die zur Verfügung gestellte Software entspricht im Wesentlichen der jeweils aktuellen Funktionsumfangbeschreibung bzw. dem Produktblatt, abrufbar unter der Website. Bei Anpassungen sind die Mängelansprüche des Kunden auf die Neuerungen gegenüber dem vorherigen Stand der Software beschränkt.

9.2

Hinsichtlich der Gewährung der Nutzung der Software sowie der Zurverfügungstellung des vereinbarten Speicherplatzes gelten die Gewährleistungsvorschriften des Mietrechts (§§ 535 ff. BGB), soweit sich aus diesen Nutzungsbedingungen nicht etwas anderes ergibt. Die Regelungen in § 536b BGB (Kenntnis des Mieters vom Mangel bei Vertragsschluss oder Annahme) und in § 536c BGB (während der Mietzeit auftretende Mängel, Mängelanzeige durch den Mieter) finden Anwendung. Die Anwendung des § 536a Abs. 2 BGB (Selbstbeseitigungsrecht des Mieters) ist jedoch ausgeschlossen.

9.3

Die Gewährleistung für nur unerhebliche Minderungen der Tauglichkeit der Leistung/Software wird ausgeschlossen.

Die verschuldensunabhängige Haftung gemäß § 536a Abs. 1 BGB für Mängel, die bereits bei Vertragsschluss vorlagen, ist ebenfalls ausgeschlossen.

9.4

Etwaige Schadenersatzansprüche des Kunden unterliegen den in Ziffer 10 genannten Beschränkungen.

10 Sonstige Haftung von Net at Work

10.1

Soweit in diesen Nutzungsbedingungen nichts anderes bestimmt ist, sind vorbehaltlich nachstehender Ziffer 10.2 Schadens- und Aufwendungsersatzansprüche des Kunden gleich aus welchem Rechtsgrund gegen Net at Work ausgeschlossen. Dies gilt insbesondere auch für Schadenersatzansprüche aus Delikt (z.B. § 823 BGB).

Soweit die Haftung ausgeschlossen oder beschränkt ist, gilt dies auch für die persönliche Haftung der Angestellten, Arbeitnehmer, Mitarbeiter, Vertreter und Erfüllungsgehilfen von Net at Work.

10.2

Die Haftungsbeschränkungen in diesen allgemeinen Geschäftsbedingungen gelten nicht

- (i) soweit die Schadensursache auf Vorsatz oder grobe Fahrlässigkeit von Net at Work oder ihrer Vertreter oder Erfüllungsgehilfen beruht;
- (ii) bei schuldhaftem Verstoß gegen wesentliche Vertragsverpflichtungen, wobei in diesem Fall der Schadenersatz auf den bei Vertragsschluss vorhersehbaren vertragstypischen Schaden beschränkt ist. Wesentliche Vertragspflichten sind solche Verpflichtungen, die vertragswesentliche Rechtspositionen des Vertragspartners schützen, die ihm der Vertrag nach seinem Inhalt und Zweck gerade zu gewähren hat; wesentlich sind ferner solche Vertragspflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglichen und auf deren Einhaltung der Kunde regelmäßig vertraut hat und vertrauen darf;
- (iii) bei Schäden aus der Verletzung von Leben, Körper und Gesundheit;
- (iv) bei Verzug, soweit ein fixierter Liefertermin vereinbart ist;
- (v) bei arglistigem Verschweigen eines Mangels;
- (vi) bei Übernahme einer Garantie und/oder des Beschaffungs- oder Herstellerrisikos im Sinne von § 276 BGB durch Net at Work;
- (vii) in Fällen der zwingenden gesetzlichen Haftung, insbesondere nach dem Produkthaftungsgesetz.

Eine Beweislastumkehr zulasten des Kunden ist mit den vorstehenden Regelungen nicht verbunden.

10.3

Die verschuldensunabhängige Haftung für anfängliche Mängel (§ 536a Abs. 1 BGB) ist ausgeschlossen.

11 Vertragslaufzeit und Beendigung

11.1

Sofern nichts anderes vereinbart wurde, beträgt die Vertragslaufzeit 12 Monate ab Vertragsbeginn, das Abrechnungsintervall 12 Monate und die Kündigungsfrist 3 Monate. Die Vertragslaufzeit verlängert sich automatisch um die ursprünglich abgeschlossene Vertragslaufzeit, wenn die Vereinbarung nicht innerhalb der definierten Kündigungsfrist von einer Partei gekündigt wird.

11.2

Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt. Unberührt bleibt auch das Recht des Kunden zur Kündigung nach Ziffer 3.3 (Sonderkündigung im Fall bestimmter Leistungsänderungen) und das Recht von Net at Work zur Kündigung nach Ziffer 13 (Sonderkündigung bei Widerspruch zu Änderungen dieser Nutzungsbedingungen).

11.3

Jede Kündigung bedarf in jedem Fall der Schriftform (vgl. § 126 BGB).

12 Datenschutz und Geheimhaltung

12.1

Die Parteien werden, die für sie jeweils geltenden anwendbaren datenschutzrechtlichen Bestimmungen einhalten.

12.2

Die Parteien schließen den gesonderten **Auftragsverarbeitungsvertrag** ab, der diesem Vertrag als **Anlage** beigefügt ist. Net at Work wird die entsprechenden personenbezogenen Daten allein nach den dort festgehaltenen Bestimmungen und nach den Weisungen des Kunden verarbeiten.

12.3

Net at Work verpflichtet sich, über alle vertraulichen Informationen (einschließlich Geschäftsgeheimnissen), die sie im Zusammenhang mit diesem Vertrag und dessen Durchführung erfährt, Stillschweigen zu bewahren und diese nicht gegenüber Dritten offenzulegen, weiterzugeben oder auf sonstige Art zu verwenden. Vertrauliche Informationen sind dabei solche, die als vertraulich gekennzeichnet sind, unabhängig davon, ob sie in schriftlicher, elektronischer, verkörperter oder mündlicher Form mitgeteilt worden sind. Die Geheimhaltungsverpflichtung gilt nicht, soweit Net at Work gesetzlich oder aufgrund bestands- bzw. rechtskräftiger Behörden- oder Gerichtsentscheidung zur Offenlegung der vertraulichen Information verpflichtet ist. Sie gilt ebenfalls nicht, sollten die Daten bereits offenbart sein oder nachfolgend ohne Verstoß gegen diese Vertraulichkeitsvereinbarung offenbart werden.

13 Änderungsvorbehalt für Nutzungsbedingungen

Net at Work ist berechtigt, die Nutzungsbedingungen zu ändern oder zu ergänzen (zusammen: „**Änderungen**“).

Dazu wird Net at Work die Änderungen dem Kunden per E-Mail mit einer Vorlaufzeit von sechs Wochen ankündigen. Widerspricht der Kunde den geänderten Nutzungsbedingungen nicht innerhalb von vier Wochen nach Empfang der E-Mail, in schriftlicher Form, gelten die geänderten

Nutzungsbedingungen als akzeptiert. Im Fall des form- und fristgerechten Widerspruchs gelten die ursprünglichen Nutzungsbedingungen fort; in diesem Fall ist Net at Work berechtigt, den Vertrag mit einer Frist von vier Wochen nach Zugang des Widerspruchs zum Monatsende zu kündigen (Sonderkündigungsrecht).

14 Überschriften/ Definition

14.1

Überschriften in diesen Nutzungsbedingungen dienen lediglich der leichteren Lesbarkeit und haben keinen Einfluss auf die Bedeutung und Auslegung der einzelnen Regelungen.

14.2

Als schriftliche Willens- und Wissenserklärungen im Sinne dieser Nutzungsbedingungen sind auch solche Erklärungen anzusehen, die per Telefax oder E-Mail übermittelt werden.

15 Schlussbestimmungen

15.1

Die Abtretung oder Übertragung von Forderungen durch den Kunden ist nur mit Zustimmung von Net at Work zulässig.

15.2

Ist der Kunde Kaufmann i.S.d. Handelsgesetzbuchs, juristische Person des öffentlichen Rechts oder ein öffentlich-rechtliches Sondervermögen, ist ausschließlicher – auch internationaler Gerichtsstand – für alle sich aus dem Vertragsverhältnis unmittelbar oder mittelbar ergebenden Streitigkeiten der Geschäftssitz von Net at Work in Paderborn.

Net at Work ist jedoch in allen Fällen auch berechtigt, Klage am allgemeinen Gerichtsstand des Kunden zu erheben. Vorrangige gesetzliche Vorschriften, insbesondere zu ausschließlichen Zuständigkeiten, bleiben unberührt.

15.3

Es gilt ausschließlich das Recht der Bundesrepublik Deutschland unter Ausschluss internationalen Einheitsrechts, insbesondere des UN-Kaufrechts (CISG).

15.4

Sollte eine Bestimmung dieser Nutzungsbedingungen oder eine später in sie aufgenommene Bestimmung ganz oder teilweise unwirksam, nichtig oder nicht durchführbar sein oder werden oder sollte sich eine Lücke in diesen Nutzungsbedingungen herausstellen, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. § 306 Abs. 2 und 3 BGB bleiben davon unberührt.

Anlage zu den Allgemeine Nutzungsbedingungen von Net at Work für die Software „Rimscout“

Auftragsverarbeitungsvertrag

(Stand: Februar 2022)

Präambel

Dieser Auftragsverarbeitungs-Vertrag (AV-Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien.

§ 1 Definitionen

Es gelten die Begriffsbestimmungen entsprechend Art. 4 DS-GVO, § 2 UWG und § 2 TMG sowie § 2 BDSG (neu). Sollten in den Artikeln bzw. Paragrafen sich widersprechende Darstellungen zu finden sein, gelten die Definitionen in der Rangfolge DS-GVO, UWG und TMG. Weiterhin gelten folgende Begriffsbestimmungen:

- 1. Anonymisierung:**
Prozess, bei dem personenbezogene Daten entweder vom für die Verarbeitung der Daten Verantwortlichen allein oder in Zusammenarbeit mit einer anderen Partei unumkehrbar so verändert werden, dass sich die betroffene Person danach weder direkt noch indirekt identifizieren lässt. (Quelle: DIN EN ISO 25237)
- 2. „Pseudonymisierung“**
die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. (Quelle: DSGVO Art. 3)
- 3. Unterauftragnehmer:**
Vom Auftragnehmer beauftragter Leistungserbringer, dessen Dienstleistung und/oder Werk der Auftragnehmer zur Erbringung der in diesem Vertrag beschriebenen Leistungen gegenüber dem Auftraggeber benötigt.
- 4. Verarbeitung im Auftrag:**
Verarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch einen Auftragnehmer im Auftrag des Auftraggebers.
- 5. Weisung:**
Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch einen Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2 Gegenstand des Auftrags

Messung von Kennzahlen zur Qualität von Netzwerkverbindungen und Erfassen von Systemparametern auf Endgeräten; zentrale Speicherung und Aufbereitung dieser Daten und Funktionen zur Analyse der gesammelten Daten.

Der Auftragnehmer erhält Zugriff auf folgende personenbezogene Daten (dadurch, dass der Auftraggeber die Client-Software auf seinen Endgeräten einsetzt und die erhobenen Daten an ein zentrales Speicher- und Analysesystem übermittelt), bzw. der Auftraggeber erlaubt dem Auftragnehmer, folgende personenbezogene Daten zu verarbeiten:

- Name
- E-Mail-Adressen
- Name und IP-Adresse der genutzten Endgeräte

Dem Auftraggeber ist bekannt, dass es sich bei dem Service Rimscout um eine weitgehend standardisierte und automatisierte Erhebung, Aufbereitung und Speicherung der Daten nach Stand der Technik durch ein mit dem Auftraggeber abgestimmtes Regelwerk erfolgt. Ein regelmäßiger Zugriff auf Daten des Auftraggebers findet durch den Auftragnehmer nicht statt. Anweisungen des Auftraggebers betreffend einzelner Datensätze sind aufgrund des großen Volumens und der marktüblichen Art des Dienstes nicht vorgesehen. Hiervon bleibt die gesetzliche Weisungsbefugnis des Auftraggebers unberührt. Der durch die Erteilung von Weisungen entstehende Aufwand ist dem Auftragnehmer durch den Auftraggeber zu marktgerechten Konditionen gesondert zu vergüten.

§ 3 Verantwortlichkeit

1. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung (bei Wahrung des Schutzes des Datengeheimnisses (Art. 28 DS-GVO) verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Ziff. 7 DS-GVO).
2. Die Inhalte dieses AV-Vertrages gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.
3. Auftraggeber sowie Auftragnehmer müssen gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Dazu müssen alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf das Datengeheimnis verpflichtet und über ihre Datenschutzpflichten belehrt werden. Dabei ist jede Partei für die Verpflichtung des eigenen Personals zuständig. Ferner müssen die eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht.
4. Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

§ 4 Dauer des Auftrags

1. Die Laufzeit dieses AV-Vertrages richtet sich nach der Laufzeit der bestehenden Verträge zwischen Auftraggeber und Auftragnehmer, sofern sich aus den Bestimmungen dieses AV-Vertrages nicht etwas anderes ergibt.
2. Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen AV-Vertrages z.B. bei Beendigung des vorliegenden Vertragsverhältnisses, keine (weitere) Auftragsverarbeitung durchgeführt werden darf.
3. Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.
4. Kündigungen bedürfen zu ihrer Wirksamkeit der Textform

§ 5 Weisungsbefugnis des Auftraggebers

1. Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und gegebenenfalls nach dokumentierter Weisung des Auftraggebers. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet soweit ihm möglich in derartigen Situationen den Auftraggeber vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann.
2. Die Weisungen des Auftraggebers müssen in Textform erteilt werden und werden vom Auftraggeber dokumentiert. Der Aufwand für die Umsetzung der Weisungen ist vom Auftraggeber gesondert zu marktgerechten Konditionen zu vergüten.
3. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind von der Weisungsbefugnis des Auftraggebers gedeckt und entsprechend zu dokumentieren. Bei einer wesentlichen Änderung des Auftrags steht dem Auftragnehmer ein Widerspruchsrecht zu. Besteht der Auftraggeber trotz des Widerspruchs des Auftragnehmers auf der Änderung, steht dem Auftragnehmer

ein ordentliches Kündigungsrecht bezüglich des von der Weisung betroffenen AV-Vertrages sowie der von der AV-Vereinbarung betroffenen Bestandteile des entsprechenden Hauptvertrages zu. Verweigert der Auftragnehmer, die Änderung durchzuführen, steht auch dem Auftraggeber ein ordentliches Kündigungsrecht zu. Erfolgt eine Kündigung, so ist für die restliche Vertragslaufzeit weiterhin die vertraglich vereinbarte Leistung durch den Auftragnehmer zu erbringen.

§ 6 Leistungsort

1. Der Auftragnehmer wird die vertraglichen Leistungen in der Europäischen Union (EU) erbringen.

§ 7 Pflichten des Auftragnehmers

1. Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.
2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Anforderungen der entsprechenden datenschutzrechtlichen Bestimmungen entsprechen; diese Maßnahmen muss der Auftragnehmer auf Anfrage dem Auftraggeber und ggfs. Aufsichtsbehörden gegenüber nachweisen. Dieser Nachweis beinhaltet insbesondere die Umsetzung der aus Art. 32 DSGVO resultierenden Maßnahmen. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative, nachweislich adäquate Maßnahmen umzusetzen. Dabei muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren. Eine Darstellung dieser technischen und organisatorischen Maßnahmen erfolgt in Anlage 2 zu diesem Vertrag.
3. Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein aussagekräftiges und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsverarbeitung zur Verfügung.
4. Der Auftragnehmer selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DS-GVO. Er stellt auf Anforderung dem Auftraggeber die für die Übersicht nach Art. 30 DS-GVO notwendigen Angaben zur Verfügung. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.
5. Der Auftragnehmer unterstützt den Auftraggeber gegen marktgerechte Vergütung bei der Datenschutzfolgenabschätzung mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde unterstützt der Auftragnehmer den Auftraggeber auch hierbei.
6. Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von fremden Geheimnissen, oder ein Betriebs- oder Geschäftsgeheimnis sowie Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln.
7. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Art. 33, 34 DS-GVO.
8. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
9. Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer betroffenen Person verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereitzustellen, vorausgesetzt der Auftraggeber hat den Auftragnehmer hierzu schriftlich aufgefordert.

10. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde bei dem Auftragnehmer ermittelt.
11. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.
12. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichen im Sinne der DS-GVO liegen.
13. Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung und setzt auch keine Mittel zur Verarbeitung ein, die nicht vom Auftraggeber zuvor genehmigt wurden.
14. Der Auftragnehmer speichert keine Patientendaten auf Systemen, die außerhalb der Verfügungsgewalt des Auftraggebers liegen bzw. die nicht dem Beschlagnahmeschutz unterliegen.
15. Sofern der Auftragnehmer durch das Recht der Union oder Mitgliedstaaten verpflichtet ist, die Daten auch auf andere Weise zu verarbeiten, so teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit. Die Mitteilung hat zu unterbleiben, wenn das einschlägige nationale Recht eine solche Mitteilung aufgrund eines wichtigen öffentlichen Interesses verbietet.
16. Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren, zu dokumentieren und in geeigneter Weise gegenüber dem Auftraggeber auf Anforderung nachzuweisen.

§ 8 Pflichten des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z. B. durch Einholung von Einwilligungserklärungen für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.
2. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
3. Der Auftraggeber ist hinsichtlich der vom Auftragnehmer eingesetzten und vom Auftraggeber genehmigten Verfahren zur automatisierten Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich und hat - neben der eigenen Verpflichtung des Auftragnehmers - ebenfalls die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.
4. Dem Auftraggeber obliegen die aus Art. 33, 34 DS-GVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen.
5. Der Auftraggeber legt die Maßnahmen zur Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.
6. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.
7. Der Auftraggeber stellt sicher, dass die aus Art. 32 DS-GVO resultierenden Anforderungen bzgl. der Sicherheit der Verarbeitung seinerseits eingehalten werden. Insbesondere gilt dies für Fernzugriffe des Auftragnehmers auf die Datenbestände des Auftraggebers.
8. Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen. Sofern der vereinbarte Leistungsumfang überschritten wird, ist hierzu vorab eine gesonderte schriftliche Vereinbarung zu treffen.

§ 9 Kontrollrechte des Auftraggebers

1. Der Auftraggeber hat den Auftragnehmer unter dem Aspekt ausgewählt, dass dieser hinreichende Garantien dafür bietet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Er dokumentiert das Ergebnis seiner Auswahl. Hierfür kann er beispielsweise datenschutzspezifische Zertifizierungen oder Datenschutzsiegel und -prüfzeichen berücksichtigen, schriftliche Selbstauskünfte des Auftragnehmers einholen, sich ein Testat eines Sachverständigen vorlegen lassen oder sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich oder durch einen sachkundigen Dritten, der nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen darf, von der Einhaltung der vereinbarten Regelungen überzeugen.
2. Liegt ein Verstoß des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden. Eine Störung des Betriebsablaufs beim Auftragnehmer sollte auch hierbei weitestgehend vermieden werden.
3. Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftraggeber im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags wird vom Auftragnehmer unterstützt. Insbesondere verpflichtet sich der Auftragnehmer, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind. Die dem Auftragnehmer aufgrund einer Prüfung entstehenden Aufwände sind durch den Auftraggeber gesondert zu marktgerechten Konditionen zu vergüten.
4. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

§ 10 Unterauftragnehmer

1. Der Auftragnehmer erbringt den Service unter Nutzung eines international anerkannten Hyperscalers (Rechen-Dienstleister). Der Auftragnehmer ist berechtigt, andere Unterauftragnehmer ohne vorherige explizite schriftliche oder allgemeine schriftliche Genehmigung des Auftraggebers in Anspruch zu nehmen, sofern hierdurch Zusicherungen aus diesem Vertrag, insbesondere der §§ 6 und 7, nicht verletzt werden. Der Auftragnehmer stellt dem Auftraggeber auf Anfrage eine Liste der aktuellen Unterauftragnehmer zur Verfügung.
2. Die nachfolgenden Regelungen finden sowohl für den Unterauftragnehmer als auch für alle in der Folge eingesetzten weiteren Unterauftragnehmer entsprechende Anwendung.
3. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragnehmer den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Verweigert der Auftraggeber durch seinen Einspruch die Zustimmung aus anderen als aus wichtigen Gründen, kann der Auftragnehmer den Vertrag zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen.
4. Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht. Hierbei muss jedoch jeder Unterauftragnehmer (verbundenes Unternehmen) vor Beauftragung dem Auftraggeber schriftlich angezeigt werden, sodass der Auftraggeber bei Vorliegen wichtiger Gründe die Beauftragung untersagen kann.
5. Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind, die in der Anlage 1 zu diesem Vertrag bezeichneten Unternehmen als Unterauftragnehmer für Teilleistungen für den Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für diese Unterauftragnehmer gilt die Einwilligung für das Tätigwerden als erteilt.
6. Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen.
7. Ist der Auftragnehmer im Sinne dieser Vereinbarung befugt, die Dienste eines Unterauftragnehmers in Anspruch zu nehmen, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem Unterauftragnehmer im Wege eines Vertrags dieselben Pflichten

aufgelegt, die in dieser Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages sowie den in diesem AV-Vertrag beschriebenen Kontroll- und Überprüfungsrechten des Auftraggebers. Hierbei müssen ferner hinreichend Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt.

8. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.
9. Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers.

§ 11 Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.

§ 12 Haftung

1. Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wird, gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.
2. Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der
 - a. er den aus der DSGVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
 - b. er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder
 - c. er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.
3. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.
4. Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er 1. seinen ihm speziell durch die DS-GVO auferlegten Pflichten nicht nachgekommen ist oder 2. unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.
5. Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

§ 13 Schriftformklausel

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile- einschließlich etwaiger Zusicherungen des Auftragnehmers- bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Regelungen handelt. Das Schriftformerfordernis gilt auch für den Verzicht auf dieses Formerfordernis.

§ 14 Rechtswahl, Gerichtsstand

1. Es gilt deutsches Recht.
2. Gerichtsstand ist Paderborn.

Anlage 1 zum Auftragsverarbeitungs-Vertrag

Net at Work hat folgende Unterauftragsverarbeiter im Rahmen des o.g. AV-Verhältnisses beauftragt:

Unterauftragnehmer: Microsoft [Azure Deutschland]

Anlage 2 zum Auftragsverarbeitungsvertrag

Bei der Net at Work GmbH sind nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO getroffen worden:

1. Vertraulichkeit

Zutrittskontrolle

Die Büroräume von Net at Work befinden sich in einem geschlossenen Bürogebäude auf allen vier Etagen. Der sichere Zutritt in das jeweilige Etagenbüro wird über einen personalisierten E-Token ermöglicht. Jeder Mitarbeiter besitzt zur Öffnung der elektronisch verschlossenen Türen einen E-Token.

Der Haupteingang zum Bürogebäude ist verschlossen. Hier ist der Zutritt ebenfalls nur mit einem E-Token möglich.

Die mechanischen Schlüssel für den Serverraum, die Aktenschränke und die Archive befinden sich in einem Schlüsseltresor.

Alle Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, befinden sich somit in zugriffskontrollierten Zonen.

Die Server- und Firewallsysteme inkl. der zentralen Netzwerktechnik sind im Serverraum platziert. Der Serverraum ist abgeschlossen. Der Zutritt ist ebenfalls nur mit dem personalisierten E-Token oder einem Schlüssel möglich. Ausgewählte Personen sind berechtigt, den Serverraum zu betreten. Alle Rackschränke im Serverraum sind verschlossen. Die Zugangsberechtigung zum Serverraum und die Schlüssel von den Serverschränken werden von der Geschäftsführung und von dem Director Modern Workplace verwaltet.

Zugangskontrolle

Generell müssen sich alle Benutzer eindeutig mit eigener personalisierter Kennung und eigenem Passwort im Netzwerk über die DV-Arbeitsplätze authentifizieren. Die Benutzerverwaltung erfolgt über das Microsoft Windows Active Directory. Die verwendeten Passwörter unterliegen einer Passwortkonvention. Sie müssen mindestens 8 Zeichen lang sein und mindestens ein Sonderzeichen und eine Zahl enthalten. Eine Passworthistorie von 10 Kennwörtern wird vorgegeben. Jeder Benutzer kann jederzeit sein Kennwort ändern. Das Benutzerkonto sperrt sich nach fünfmaliger falscher Eingabe. Bei Inaktivität wird der Arbeitsplatz automatisch nach einem definierten Zeitintervall gesperrt. Des Weiteren sind alle Konten bei Cloud Anwendungen mit der Multi-Faktor-Authentifizierung abgesichert.

Entsprechend den Empfehlungen von BSI und Microsoft hat das Passwort kein Ablaufdatum und es wird keine automatische Passwortänderung beim User initiiert. Das Passwort wird bei einem Angriff oder im kompromittierten Fall umgehend gesperrt. Um dies sicherzustellen, wurden erweiterte Monitoring und Überwachungsfunktionen ("Defender for Endpoint") implementiert.

Alle "Default Kennwörter", z.B. auf Switchen etc. sind geändert.

Die Systemadministrationskennwörter für den Domänenhauptbenutzer „Administrator“ sind nur zwei leitenden Angestellten bekannt.

Der Bereich „Modern Workplace“ verwaltet und administriert die Domäne. Nur wenige weitere Mitarbeiter besitzen besondere Domänen-Administrationsrechte. Die Zugriffsrechte für Azure AD werden mittels Azure AD Privileged Identity Management verwaltet.

Als Schutz von Bedrohungen aus dem Internet wird das UTM-System Sophos eingesetzt. Die Appliance wird als Firewall und als Reverse-Proxy genutzt. Durch die Proxy-Funktionalität schützt das System die Benutzer vor webbasierten Gefahren durch Schadsoftware als auch vor gefährlichen Sites.

Remote-Desktop Verbindungen über die Microsoft-Terminal-Services werden über https mit einem öffentlichen Zertifikat verschlüsselt. Der Zugriff von externen Firmennotebooks ist über ein VPN mit Client-Zertifikat abgesichert. Fremde Systeme können kein VPN aufbauen.

Auf die Serversysteme direkt haben nur Administratoren Zugang, die in der entsprechenden Sicherheitsgruppe über Berechtigungen autorisiert sind.

Die Notebooksysteme sind über Bitlocker (Festplattenverschlüsselung) geschützt. Zudem existiert eine schriftliche Richtlinie, die zu einer Verschlüsselung mobiler Datenträger (USB-Sticks, externe Festplatten) verpflichtet.

Fehlerhafte Anmeldeversuche im Netzwerk werden im Windows-Eventlog protokolliert. Sämtliche Veränderungen im Active Directory werden ebenfalls im Windows-Eventlog protokolliert und sind aufgrund der personengebundenen Administrationsrechte nachvollzieh- und können zugeordnet werden.

Bei ausgeschiedenen Mitarbeitern werden die Benutzerkonten sofort durch die Administration gesperrt.

Das WLAN-Netzwerk im Bürogebäude ist WPA-Enterprise verschlüsselt.

Für die Clients (PC und mobile Geräte) werden die Patches direkt vom Hersteller bezogen und, sobald veröffentlicht, über eine integrierte Updateroutine automatisch installiert. Sicherheitsupdates für Server, Firewall und Netzwerksysteme werden, sobald bekannt, manuell installiert. Dies gilt für on premises als auch Cloud Systeme, z.B. virtuelle Maschinen. Software as a Service Systeme (SaaS) in der Cloud werden in erster Linie von den Herstellern direkt aktualisiert. Für Dynamics 365 werden Aktualisierungen nach einem Funktionstest auf einem Testsystem im Produktivsystem manuell freigegeben.

Zugriffskontrolle

Im Netzwerk von Net at Work werden folgende Anwendungen und Verfahren zur Verarbeitung von personenbezogenen Daten verwendet:

Warenwirtschaftssystem (ERP)

- Microsoft Business Solutions Dynamics NAV

Customer Relation Management (CRM)

- Microsoft Dynamics 365 CRM

Lohnbuchhaltung

- Lexware Lohn & Gehalt

IT-Bürokommunikation

- Microsoft Teams (Chat, Meeting, Telefonie), Microsoft Exchange (Mail), Microsoft Sharepoint-Services (Daten)

Bis auf die Lohnbuchhaltung erfolgen der Zugriff und die Anmeldung auf die Anwendungen zentral über die Benutzerverwaltung des Active Directory. Hier sind entsprechende Sicherheitsgruppen definiert, in denen die Benutzer folglich Ihrer Aufgaben zugeordnet sind. Bei Einstellung eines Mitarbeiters wird über Checklisten definiert, wer auf welche Anwendungen in welchen Maße Zugriff haben muss. Für die Erteilung der Berechtigungen ist der Director Modern Workplace verantwortlich.

Trennung

Alle Verfahren, bei denen Mandantentrennung eine Rolle spielt, sind bekannt. Systeme, die Kunden angeboten werden, sind mandantenfähig. Die Mandantenfähigkeit ist für jedes Verfahren durchgängig umgesetzt.

Pseudonymisierung & Verschlüsselung

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

Darüber hinaus werden Daten auf Server- und Clientsystemen auf verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Festplattenverschlüsselungssysteme (Bitlocker) im Einsatz.

2. Integrität

Eingabekontrolle

Bei den verschiedenen Anwendungen mit personenbezogenen Daten ist eine angemessene Eingabekontrolle über verschiedene Mechanismen gegeben.

Bei den Personaldaten haben zwei Personen die Möglichkeit, die Daten zu ändern. Generell muss sich ein Benutzer am Personalverwaltungssystem authentifizieren und anmelden.

Die Eingabe der Daten im CRM- und ERP-System wird über entsprechende Benutzerauthentifizierungen reglementiert. Zudem ist in der Berechtigungsverwaltung der einzelnen Systeme genau zu erkennen, wer welche Berechtigungen in den einzelnen Modulen oder Bereichen besitzt. Eine Protokollierung der einzelnen Eingaben in den verschiedenen Masken und Feldern im CRM- und ERP-System ist zurzeit nicht aktiviert. Aufgrund der unkritischen personenbezogenen Daten ist diese Maßnahme angemessen. Wesentliche Veränderungen, wie z.B. wer ein Datensatz (Ansprechpartner) oder einer Notiz angelegt hat, werden im Frontend selber angezeigt und sind nachvollziehbar.

Veränderungen in der Netzwerkverwaltung im Microsoft-Umfeld werden im Event-Log protokolliert. Generell werden alle Veränderungen im Netzwerk in einem zentralen Dokument von den jeweiligen Administratoren dokumentiert.

Protokolle zur Eingabekontrolle werden nach dem Vier-Augen-Prinzip durch den Administrator und den Datenschutzbeauftragten regelmäßig geprüft.

Weitergabekontrolle

Eine automatisierte Weitergabe von personenbezogenen Daten erfolgt nur im Bereich Sozialversicherungsangelegenheiten der Angestellten. Andere personenbezogene Daten von Kunden, Lieferanten oder Partnern werden nicht automatisiert weitergegeben.

Eine Weitergabe von personenbezogenen Daten erfolgt im Wesentlichen zu Marketingzwecken. Hierbei geht es um die Weitergabe an Unternehmen im Bereich des Tele-, Email- und Briefmarketings. Alle Datenübermittlungsaktivitäten werden in verschiedensten Formen protokolliert. Zudem erfolgt die Übergabe verschlüsselt über https.

Erfolgt die Weitergabe von personenbezogenen Daten per Mail, so werden diese sicher mit der eigenen Softwarelösung NoSpamProxy Encryption verschlüsselt.

Datenträger werden vor der Entsorgung oder vor der Weitergabe sicher über Wipe-Mechanismen gelöscht oder sind durch Bitlocker verschlüsselt

3. Verfügbarkeit und Belastbarkeit

Die Verantwortlichkeit für die Datensicherung liegt bei dem Director Modern Workplace und ist wie folgt geregelt.

Lokale Daten werden täglich über eine automatisierte Datensicherung auf Festplatten und auf Bänder übertragen.

Zusätzlich erfolgt alle 15 Minuten über die Sicherungssoftware Microsoft Data Protection Manager eine Sicherung der Daten auf Festplatten. Zur konsistenten Sicherung von Files und Datenbanken wird hier die SnapShot-Technik verwendet.

Die tägliche Bandsicherung ist auf dem Prinzip der Großvater-Vater-Sohn-Sicherung aufgebaut. Die Entnahme der Bänder erfolgt täglich durch definierte Personen. Die entnommenen Bänder werden in einem getrennten Gebäude zugriffssicher aufbewahrt.

Zur Überwachung und Überprüfung der Datensicherung wird mit dem Microsoft System Center Operations Manager durchgeführt. Durch regelmäßige Rücksicherungen auch von den Bändern ist eine Lesbarkeit der Bänder gewährleistet.

Die Datensicherung der Cloud-Dienste wie Exchange Online, SharePoint Online, OneDrive for Business, etc. wird über die in Office 365 zur Verfügung stehenden Bordmittel realisiert.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Bei der Net at Work GmbH ist ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.

Alle Mitarbeiter sind zum Datengeheimnis verpflichtet worden. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

Alle Mitarbeiter wurden durch den Datenschutzbeauftragten in Sachen Datenschutz geschult. Folgende Inhalte wurden vermittelt:

- Was sind personenbezogene Daten?
 - o Vertrauenswürdige Datenverarbeitung
 - o Personenbezogenen Daten
 - o Besondere Kategorien personenbezogener Daten
 - o Lebenszyklus personenbezogener Daten
- Wo fallen sie an?
 - o Wo finden sich personenbezogene Daten?
- Wie muss dann mit ihnen umgegangen werden?
 - o Grundregeln des Datenschutzes
 - Rechtmäßigkeit
 - Einwilligung
 - Erforderlichkeit
 - Zweckbindung
 - Transparenz
 - Datensicherheit
 - Kontrolle der Datenverarbeitung
 - Rechenschaftspflicht
- Wer ist verantwortlich?
- Wo bekomme ich Informationen über den Datenschutz?

Am Ende der Schulung wurde eine Verständniskontrolle durchgeführt, bei denen die Teilnehmer Fragen zum Datenschutz beantworteten.

5. Auftragskontrolle

Die Verarbeitung der Daten erfolgt ausschließlich in der Europäischen Union.

Bei der Net at Work GmbH ist ein externer Datenschutzbeauftragter benannt.

Der Datenschutzbeauftragte verfügt über eine Übersicht sämtlicher Fälle von Auftragsdatenverarbeitung.

Alle bisherigen Auftragnehmer sind langjährige Partner von Net at Work.

Eine entsprechende Überprüfung der Auftragsdatenverarbeiter findet durch den Datenschutzbeauftragten im angemessenen Umfang stattfinden.

Bei Net at Work werden folgende Cloud-Dienste genutzt, bei denen die eine Verarbeitung von personenbezogenen Daten stattfindet.

- Microsoft Office365 (OneDrive for Business, Exchange Online, SharePoint Online, Yammer und weitere Dienste)
- Microsoft Dynamics 365
- Microsoft Azure Active Directory

Die oben aufgeführten Cloud Lösungen Microsoft Office 365, Dynamics 365 und Azure sind nach deutschem und europäischem Datenschutzrecht, datenschutzkonform einsetzbar. Diese Aussage stützt sich auf erfüllte Anforderungen aus der ISO 27001 oder den EU-Datenschutzrichtlinien 95/46/EG. Microsoft als Auftragnehmer hält technische und organisatorische Maßnahmen ein und verfügt über eine standardisierte Erklärung zur Auftragsdatenverarbeitung. Ebenfalls existieren EU-Standardvertragsklauseln für die legale Übermittlung personenbezogener Daten an Auftragsverarbeiter außerhalb der EU.

Somit bietet Microsoft in Sachen Cloud-Diensten ein sehr hohes Maß an Datensicherheit, das von vielen Unternehmen so selbst nicht vorgehalten werden kann. Nähere Informationen zum Datenschutz und zur Datensicherheit sind bei Microsoft im Office 365 – Trust Center unter <https://products.office.com/de-de/business/office-365-trust-center-welcome> erhältlich.

Microsoft ist Auftragsverarbeiterin der in ihren Cloud Lösungen gespeicherten personenbezogenen Daten. Die DSGVO-konformen Regelungen dazu finden sich in den aktuellen Datenschutzbestimmungen der „Bestimmungen für Onlinedienste“, die unter <https://www.microsoft.com/licensing/docs> abgerufen werden können.

Durch entsprechend ausgearbeiteter Checklisten kann zudem nachgewiesen werden, dass die Cloud-Dienste rechts- und regelkonform in die Organisation integriert wurden. Unter den rechtlichen Gesichtspunkten eines Risikomanagements sind die Cloud-Dienste daher ohne Bedenken zu empfehlen