Allgemeine Nutzungsbedingungen
von Net at Work
für die Software „NoSpamProxy Cloud“

(Stand: März 2026)

1. Präambel

NoSpamProxy Cloud ist ein Service der Net at Work GmbH, der ein- und ausgehende E-Mails einer Mail-Domäne automatisiert verarbeitet und Sicherheitsfunktionen bietet. Je nach vertraglich vereinbartem Umfang bietet der Service

- Spam- und Malwareschutz
- E-Mail-Verschlüsselung und -Signatur
- automatische Zertifikatsverwaltung
- sichere Übertragung großer Dateien
- automatisches Anfügen von Mail-Signatur und -Disclaimer Texten

NoSpamProxy Cloud fungiert dabei als E-Mail-Gateway und speichert die E-Mails lediglich für die Dauer der Verarbeitung, es stehen keine Postfachdienste zur Verfügung.

2. Anwendungsbereich

2.1

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 „NoSpamProxy Cloud“ (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.

2.2

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.

2.3

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.

3. Vertragsgegenstand

3.1

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 Leistung 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 https://www.nospamproxy.de/de/email-security-cloud/ (nachfolgend: „**Webseite**“), und den vereinbarten Verfügbarkeiten unter Ziffern 4 und 5. Der nutzbare Funktionsumfang ergibt sich aus den vom Kunden lizenzierten Funktionsmodulen der Software.

3.2

Der jeweilige Funktionsumfang der Software NoSpamProxy, die Net at Work zur Erbringung des Services NoSpamProxy Cloud nutzt, kann der jeweils aktuellen Funktionsbeschreibung bzw. dem Produktblatt entnommen werden. Der beschriebene Funktionsumfang ist nicht bindend, sondern kann sich aufgrund technischer Weiterentwicklungen ändern.

Die Funktionsbeschreibung zum Zeitpunkt des Vertragsbeginns 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.

4. Leistungen von Net at Work, Software, „Managed Certificates“

4.1

Net at Work gewährt dem Kunden die Nutzung der jeweils aktuellen Version der Software für die vereinbarte Anzahl an Mailboxen über das Internet mittels Zugriffes auf einen Administrationsbereich. Als Mailbox zählt dabei jede E-Mail-Adresse, die mit eigenem Postfach im E-Mail-System des Kunden angelegt ist. Darunter fallen auch z.B. Funktionsadressen. Mailboxen mit mehreren E-Mail-Adressen werden als eine Mailbox gewertet.

Werden bei ausgehenden E-Mails des Kunden als schädlich oder als Spam einzustufende E-Mails festgestellt, kann Net at Work die Verarbeitung von E-Mails einstellen oder andere geeignete Maßnahmen nach eigener Wahl ergreifen, um Schaden für den Kunden und der Software-Plattform NoSpamProxy Cloud (z.B. IP-Adressen auf Blocklisten) zu vermeiden.

Nutzt der Kunde E-Mail-Weiterleitungen (auch im Rahmen von Verteilerlisten) an externe E-Mail-Adressen, muss der Kunde sicherstellen, dass die Absender-Adresse nach dem Sender Rewrite Scheme (SRS) umgeschrieben wird. Weitergeleitete E-Mails ohne umgeschriebene Absende-Adresse werden abgewiesen.

4.2

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 Funktionsumfangsbeschreibung bzw. dem Produktblatt, abrufbar auf der Webseite von Net at Work.

4.3.

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.

4.4

Net at Work wird die Software regelmäßig warten und den Kunden über etwaige hiermit verbundene Einschränkungen rechtzeitig über die Statusseite informieren. Die Statusseite ist über die Adresse https://status.cloud.nospamproxy.com/ erreichbar. 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

4.5
Net at Work stellt dem Kunden für Zwecke der Nutzung der Software Leistung auf Servern bis zu dem im Auftrag vereinbarten Umfang zur Verfügung.

4.6
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. Für eine ausreichende (regelmäßige) Sicherung der Daten ist vielmehr der Kunde allein verantwortlich.

4.7 Limitierung des Dienstes – Je Mailbox ist der Versand von Mails an 800 Empfänger pro Stunde und 8.000 Empfänger in 24 Stunden limitiert. Der Empfang je Mailbox ist auf 3.600 Mails je Stunde limitiert. Sofern dieser Wert überschritten wird, begrenzt Net at Work ausgehende Mails auf diese Werte und lehnt über die Werte hinausgehende Mails ab.

4.8
Ist die Nutzung von Managed Certificates vereinbart, ermächtigt der Kunde damit Net at Work, in dessen Namen Zertifikate für Mitarbeiter des Kunden bei angeschlossenen Trust-Centern zu beantragen, zu verwalten, erforderliche Validierungen durchzuführen und im Namen des Kunden die vom jeweiligen Trust-Center vorgegebenen Vertragsbedingungen dafür zu akzeptieren. Der Kunde ist verpflichtet, die in der **Anlage 1** enthaltenen jeweiligen Nutzungsbedingungen für die Zertifikate einzuhalten.

4.9
Leistungs- und Erfüllungsort für die von Net at Work zu erbringenden Leistungen ist stets der in Ziff. 6.1 definierte Übergabepunkt.

4.10
Ein Produktsupport, also insbesondere Fragen zu den Funktionen oder der Bedienung der Software, ist im Leistungsumfang nicht enthalten, sondern wird nur auf der Grundlage eines separaten Supportvertrages gegen gesonderte Vergütung von Net at Work erbracht.

5. Nutzungsumfang und -rechte an der Software, Beachtung von Restriktionen

5.1
Eine physische Überlassung der Software an den Kunden erfolgt nicht.

5.2
Der Kunde erhält an der jeweils aktuellen Version der Software für die vertraglich festgelegte Anzahl an E-Mailboxen einfache, d.h. nicht unterlizenzierbare und nicht übertragbare, zeitlich auf die Dauer des Vertrags beschränkte Rechte („**Lizenz**“), die Software mittels Zugriffes durch von Net at Work benannte Authentifizierungsmöglichkeiten nach Maßgabe

der vertraglichen Regelungen zu nutzen. Die Nutzung der Software durch verbundene Unternehmen im Sinne von § 15 AktG des Kunden ist von der Lizenz erfasst, sofern der Kunde die verbundenen Unternehmen entsprechend zur Einhaltung dieser Nutzungsbedingungen verpflichtet hat.

Für Distributoren und Reseller (zusammen nachfolgend: „**Partner**“) von Net at Work gilt, dass diese die Software in ihrem gewöhnlichen Geschäftsgang im Umfang der Lizenz an ihre Kunden unterlizenzieren dürfen, sofern der Partner seinen Kunden entsprechend zur Einhaltung dieser Nutzungsbedingungen verpflichtet hat.

5.3

Der Kunde darf im Übrigen die Software nur im Rahmen seiner eigenen geschäftlichen Tätigkeit durch eigenes Personal nutzen. Dem Kunden ist eine weitergehende Nutzung der Software nicht gestattet.

5.4

Der Kunde hat alle geltenden Exportbeschränkungen oder sonstigen handelsrechtlichen Beschränkungen, wie Embargos, (zusammen: „**Restriktionen**“) bei der Nutzung bzw. im Falle eines Partners auch beim Vertrieb der Software einzuhalten. Im Falle eines Verstoßes gegen Restriktionen behält sich Net at Work das Recht vor, ihre Leistungen unverzüglich einzustellen und/oder den Vertrag fristlos aus wichtigem Grund zu kündigen.

6. Service Levels und Störungsbehebung

6.1

Net at Work gewährt eine Gesamtverfügbarkeit im Jahresmittel der Leistungen (Software) von mindestens 99,9% am Übergabepunkt bei einer Vertragslaufzeit von einem oder mehreren 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 99,9%.

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

Schwerwiegende Störungen (die Nutzung der Software insgesamt oder eine Hauptfunktion der Software ist nicht möglich) wird Net at Work auch außerhalb der Servicezeiten spätestens binnen 4 Stunden ab Eingang der Meldung der Störung – sofern die Meldung innerhalb der Servicezeiten erfolgt – beheben („**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

Sonstige 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).

6.6

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 Zugriffen 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 entsprechend zu vereinbaren.

7.3

Der Kunde ist verpflichtet, die Leistungen von Net at Work nicht dafür zu verwenden, gegen geltendes Recht, behördliche Anordnungen, Rechte Dritter oder Vereinbarungen mit Dritten zu verstoßen. 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 Nutzung in der Software auf Viren oder sonstige schädliche Komponenten prüfen und hierfür dem Stand der Technik entsprechende Maßnahmen (z.B. Virenschutzprogramme) einsetzen.

7.5

Nutzt der Kunde die Option Managed Certificates, stimmt er den in Anlage 1 aufgeführten Vertragsbedingungen des jeweiligen Trust-Centers automatisch zu.

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. Skonto wird nur bei ausdrücklicher schriftlicher Vereinbarung gewährt.

8.3

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

8.4

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

8.5

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 Webseite von Net at Work.

9.2

Hinsichtlich der Gewährung der Nutzung der Software 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.

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, -beginn und Beendigung

11.1

Sofern nicht etwas anderes vereinbart ist, beträgt die Vertragslaufzeit 12 Monate ab Vertragsbeginn. Der Vertragsbeginn ergibt sich aus dem Auftrag. Die Vertragslaufzeit verlängert sich jeweils automatisch um die ursprünglich abgeschlossene Vertragslaufzeit, wenn der Vertrag nicht innerhalb der definierten Kündigungsfrist von einer Partei gekündigt wird. Sofern keine gesonderte Kündigungsfrist vereinbart ist, beträgt die Kündigungsfrist 3 Monate.

11.2

Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

Unberührt bleibt auch das Recht des Kunden zur Kündigung nach Ziffer 4.3 (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 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 einen gesonderten Auftragsverarbeitungsvertrag ab, der diesem Vertrag als **Anlage 2** 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, Stilschweigen 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 Vorlauffrist von vier Wochen ankündigen. Widerspricht der Kunde den geänderten Nutzungsbedingungen nicht innerhalb von zwei Wochen nach Empfang der E-Mail, in schriftlicher Form, gelten die geänderten Nutzungsbedingungen als akzeptiert. Im Falle 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). Unberührt davon bleiben etwaig kürzere zwischen den Parteien vereinbarte ordentliche Kündigungsfristen.

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 1 zur Nutzungsvereinbarung für NoSpamProxy Cloud

Auftragsverarbeitungsvertrag

zwischen

dem in der Bestellung des Software-Services NoSpamProxy Cloud bezeichneten Kunden

(Verantwortlicher im Sinne der DS-GVO, nachfolgend ***„Auftraggeber"*** genannt)

und

Net at Work GmbH
Am Hoppenhof 32 A
33104 Paderborn
(Auftragsverarbeiter im Sinne der DS-GVO, nachfolgend ***„Auftragnehmer"*** genannt)

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 TDDDG 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 TDDDG. 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. ***Unterauftragnehmer***:
   Vom Auftragnehmer beauftragter Leistungserbringer, dessen Dienstleistung und/oder Werk der Auftragnehmer zur Erbringung der in diesem Vertrag beschriebenen Leistungen gegenüber dem Auftraggeber benötigt.

3. ***Verarbeitung im Auftrag***:
   Verarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch einen Auftragnehmer im Auftrag des Auftraggebers.

4. ***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

- Analyse von eingehenden und ausgehenden E-Mails von Mitarbeitern des Auftraggebers zur Erkennung von Spam, Malware und anderen Sicherheitsrisiken, sowie die Ver- und Entschlüsselung von E-Mails.

Der Auftragnehmer erhält Zugriff auf folgende personenbezogene Daten (dadurch, dass der Auftraggeber ihm die eingehenden E-Mails durch Bekanntmachen einer IP-Adresse des Auftragnehmers zustellen lässt und ihm ausgehende E-Mails von seinem Mail-Server zustellt), bzw. der Auftraggeber erlaubt dem Auftragnehmer, folgende personenbezogene Daten zu verarbeiten:

- Name
- E-Mail-Adresse
- Betreff
- Inhalt der E-Mails und der Anlagen
- Versand- und Empfangsdatum
- Verschlüsselungs- und Signierungsstatus der E-Mail
- IP-Adressen
- Weitere E-Mail-Metadaten für 32Guards
- Zertifikate (nur NoSpamProxy Managed Certificates)
- An E-Mails angefügte Dateien, die personenbezogene Daten enthalten können (nur NoSpamProxy Sandbox)

Betroffene Personengruppe:

- Alle Mitarbeitenden der Organisation oder sonstige Dritte wie Berater etc., die über ein E-Mail-Postfach verfügen oder Zugang dazu haben.
- Alle Personen, die E-Mails an die Organisation des Kunden senden

Dem Auftraggeber ist bekannt, dass es sich bei dem Service NoSpamProxy SaaS um eine weitgehend standardisierte Prüfung von Mails auf Viren, Malware und Spam, Verschlüsselung und andere Formen der Prüfung und Umwandlung handelt, die nach dem Stand der Technik durch ein mit dem Auftraggeber abgestimmtes Regelwerk erfolgt. Die Daten werden für einen Zeitraum von 3 Monaten gespeichert, ausschließlich zu Analysezwecken genutzt und nach Ablauf dieses Zeitraums automatisch und dauerhaft gelöscht. Bei Nutzung der Sandbox-Option werden Dateianhänge vollständig zur Analyse übertragen und anschließend unmittelbar gelöscht. Ein regelmäßiger Zugriff auf Daten des Auftraggebers findet durch den Auftragnehmer nicht statt. Anweisungen des Auftraggebers betreffend einzelne Mails oder Gruppen von Mails 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 DSGVO).

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) oder im Europäischen Wirtschaftsraum (EWR) erbringen. Bei Leistungserbringung, die in Teilen von Unterauftragsverarbeitern in einem Drittland erfolgt, garantiert der Auftragnehmer die Einhaltung der diesbezüglichen Vorgaben der DSGVO und weist dies auf Verlangen nach (Abschluss der EUStandardvertragsklauseln).

§ 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. Die Unterrichtung erfolgt an die bei Auftragserteilung und im CRM-System des Auftragnehmers hinterlegte E-Mail-Adresse. 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. Der Auftragnehmer ist nicht berechtigt, ohne Genehmigung des Auftraggebers Meldungen an die zuständige Aufsichtsbehörde zu machen.
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 in Anspruch zu nehmen, sofern hierdurch Zusicherungen aus diesem Vertrag, insbesondere der §§ 6 und 7, nicht verletzt werden (Allgemeine schriftliche Genehmigung). Der Auftragnehmer stellt dem Auftraggeber auf Anfrage eine Liste der aktuellen Unterauftragsnehmer zur Verfügung.
2. Die nachfolgenden Regelungen finden sowohl für den Unterauftragnehmer als auch für alle in der Folge eingesetzten weiteren Unterauftragnehmer entsprechende Anwendung.
3. Der Auftragnehmer informiert 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.

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 auferlegt, 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 Berichtigung, Beschränkung von Verarbeitung, Löschung und Rückgabe von Datenträgern

1. Während der laufenden Beauftragung berichtigt, löscht oder sperrt der Auftragnehmer die vertragsgegenständlichen Daten nur auf Anweisung des Auftraggebers.
2. Nach Abschluss der vertraglichen Arbeiten – oder früher nach Aufforderung durch den Auftraggeber – hat der Auftragnehmer Datenbestände auf Anweisung des Auftraggebers datenschutzkonform zu löschen bzw. zu vernichten, sofern keine gesetzliche Pflicht zur Aufbewahrung besteht. Das Protokoll der Löschung ist auf Anforderung vorzulegen
3. Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.
4. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.
5. Der Auftraggeber kann jederzeit, d. h. sowohl während der Laufzeit als auch nach Beendigung des Vertrages, die Berichtigung, Löschung, Verarbeitungseinschränkung (Sperrung) und Herausgabe von Daten durch den Auftragnehmer verlangen, solange der Auftragnehmer die Möglichkeit hat, diesem Verlangen zu entsprechen.
6. Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. 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.

7. Sollte dem Auftraggeber eine Rücknahme der Daten nicht möglich sein, wird er den Auftragnehmer rechtzeitig schriftlich informieren. Der Auftragnehmer ist dann berechtigt, personenbezogene Daten im Auftrag des Auftraggebers zu löschen.
8. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung bzgl. einer Löschung nicht erforderlich, diese müssen gelöscht werden.

§ 12 Zurückbehaltungsrecht

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

§ 13 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.

§ 14 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.

§ 15 Rechtswahl, Gerichtsstand

1. Es gilt deutsches Recht.

2. Gerichtsstand ist Paderborn.

Anlage 2 zur Nutzungsvereinbarung für NoSpamProxy Cloud

Nutzungsbedingungen der Unterauftragsnehmer im Rahmen des Auftragsverarbeitungsvertrags

Bitdefender SRL.

Die Nutzungsbedingungen der Bitdefender SRL sind unter folgender URL abrufbar: https://www.bitdefender.com/site/Main/view/end-user-license-minimum-terms.html

Amazon EU S. à r.l.

Die Nutzungsbedingungen der Amazon EU S. à r.l. Sind unter folgender URL abrufbar: https://d1.awsstatic.com/legal/aws-customer-agreement/AWS%20Customer%20Agreement_DE_(2024-01-12).pdf

GlobalSign

Im Rahmen des Produktes Managed Certificates werden Zertifikate von der GlobalSign CA bezogen. Die Bedingungen, unter denen Zertifikate ausgestellt, verlängert und revoziert werden, sind im Certification Practice Statement (CPS) von GlobalSign festgehalten. Die jeweils aktuelle Version des CPS liegt unter https://www.globalsign.com/en/repository.

Anlage 1 zum Auftragsverarbeitungsvertrag

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

Unterauftragnehmer: Bitdefender SRL.

Übermittelte Daten	Zweck	Ort der Verarbeitung
Metadaten von Mails u. Dateien	Erkennung von Spam- und Malware Mails	EU

Unterauftragnehmer: Amazon EU S. à r.l. (AWS)

Übermittelte Daten	Zweck	Ort der Verarbeitung
Metadaten von Mails u. Dateien	Erkennung von Spam- und Malware Mails	EU

Unterauftragnehmer: Varist ehf.

Übermittelte Daten	Zweck	Ort der Verarbeitung
Dateien	Erkennung von Spam- und Malware Mails	EWR

Anlage 2 zum Auftragsverarbeitungsvertrag:

Nachweis der allgemeinen technischen und organisatorischen Maßnahmen

Beschreibung der technischen und organisatorischen Maßnahmen

Angaben zum Verantwortlichen (Art. 30 Abs. 1 lit. a DS-GVO):

Verantwortlicher:

Net at Work GmbH

Am Hoppenhof 32A, 33104 Paderborn (Deutschland)

Tel: +49 5251 304600, Web: https://www.netatwork.de/

Gesetzlicher Vertreter:

Uwe Ulbrich

Tel: +49 5251 304600

E-Mail: uwe.ulbrich@netatwork.de

Datenschutzbeauftragter:

Paul Köhler

Tel: 02953 39699 20

E-Mail: datenschutz@bitsic.de

Einleitung

Die SaaS-Lösung NoSpamProxy ist durch umfassende technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO geschützt. Zu den technischen Maßnahmen zählen unter anderem Verschlüsselung von Daten bei der Übertragung (TLS 1.2+) und Speicherung (AES-256), rollenbasierte Zugriffskontrollen, Multi-Faktor-Authentifizierung, regelmäßige Sicherheitsupdates sowie ein zentrales Logging- und Monitoring-System zur Erkennung und Analyse sicherheitsrelevanter Ereignisse. Die organisatorischen Maßnahmen beinhalten ein rollenbasiertes Berechtigungskonzept, regelmäßige Schulungen der Mitarbeitenden, definierte Prozesse zur Incident-Response, sowie vertragliche Regelungen mit Auftragsverarbeitern. Darüber hinaus erfolgt ein regelmäßiges Risikomanagement und eine kontinuierliche Verbesserung der Sicherheitsmaßnahmen im Rahmen unseres ISMS.

Die SaaS-Lösung wird in einem ISO27001 zertifizierten Rechenzentrum gehostet.

Die genaueren Maßnahmen werden im Folgenden beschrieben.

M.1 Maßnahmen zur Vertraulichkeit

M.1.1 Beschreibung der Zutrittskontrolle:

- Chipkarten - Vorhandenes Chipkarten-/Transponder-Schließsystem
- Empfang - Besucherkontrolle am Empfang
- Manuelles Schließsystem - Manuelles Schließsystem mit Schließzylinder
- Schließanlage - Einsatz einer Schließanlage
- Schlüsselverwaltung - Schlüsselregelung mit Dokumentation der Schlüssel

Die zuvor aufgeführten Maßnahmen sind für den Geltungsbereich des Firmenstandortes Paderborn festgelegt worden.

M.1.2 Beschreibung der Zugangskontrolle:

- Authentifikation mit Benutzer + Passwort - 2 MFA mit Microsoft Authenticator
- Benutzerberechtigungen - Benutzerberechtigungen werden verwaltet (z.B. bei Eintritt, Änderung, Austritt)
- Firewall - Einsatz von Firewalls zum Schutz des Netzwerkes
- MDM - Einsatz von Mobile Device Management
- Sorgfältige Personalauswahl - Sorgfältige Auswahl von Reinigungspersonal und Sicherheitspersonal
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren

M.1.3 Beschreibung der Zugriffskontrolle:

- Berechtigungskonzept - Erstellen und Einsatz eines Berechtigungskonzepts für Anwendungen
- Datenlöschung - Sichere Löschung von Datenträgern vor deren Wiederverwendung (z.B. durch mehrfaches Überschreiben)
- Einsatz von Aktenvernichtern - Verwendung von Aktenvernichtern in jeder Abteilung.
- Passwortlichtlinien - Passwortrichtlinie inkl. Länge, Komplexität und Wortfilter
- Sichere Aufbewahrung - Sichere Aufbewahrung von Datenträgern
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren
- Verschlüsselung von Smartphones - Verschlüsselung von Smartphones mit dem Stand der Technik entsprechenden Verfahren

M.1.4 Beschreibung der Weitergabekontrolle:

- E-Mail-Verschlüsselung - E-Mail-Verschlüsselung mit S/MIME Verfahren.
- TLS-Verschlüsselung - Einsatz von TLS-Verschlüsselung bei der Datenübertragung im Internet
- VPN-Tunnel - Einrichtungen von VPN-Tunneln zur Einwahl ins Netzwerk von außen

M.1.5 Beschreibung des Trennungsgebots:

- Logische Mandantentrennung - Logische softwareseitige Mandantentrennung.
- Produktiv- und Testsystem - Trennung von Produktiv- und Testsystem

M.1.6 Beschreibung der Pseudonymisierung:

- Kennziffern - Verwendung von Kennziffern anstatt Namen.

M.1.7 Beschreibung der Verschlüsselung:

- Speicherung - Verschlüsselte Datenspeicherung mit Dateiverschlüsselung nach AES256 Standard
- Übertragung - Verschlüsselte Datenübertragung:
    - E-Mailverschlüsselung S/MIME,
    - VPN, zertifikatsbasierte, verschlüsselte Verbindungen mittels AES.

M.1.8 Beschreibung der Datenträgerkontrolle:

- Anonymisierung - Weitergabe von anonymisierten Daten
- Pseudonymisierung - Weitergabe von pseudonymisierten Daten
- Sichere Aufbewahrung - Sichere Aufbewahrung von Datenträgern
- Vernichtung - Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Verschlüsselung - Verschlüsselung von mobilen Datenträgern

M.1.9 Beschreibung der Benutzerkontrolle:

- Passwortvergabe - Schutz der Benutzeraccounts durch Passwörter
- Sperrung von Ex-Mitarbeitern – automatisches Sperren/Löschen von Benutzeraccounts ausgeschiedener Mitarbeiter
- Zweifaktor-Authentifizierung - Authentifikation mit Benutzername / Passwort und einem zweiten Faktor (Microsoft Authenticator oder FIDO-Token)

M.1.10 Beschreibung der Übertragungskontrolle:

- Empfängerdokumentation - Dokumentation der Empfänger von Daten sowie deren Bereitstellungsdauer
- Protokollierung - Protokollierung aller Abruf- und Übermittlungsvorgänge

M.2 Maßnahmen zur Integrität

M.2.1 Beschreibung der Eingabekontrolle:

- Personalisierte Benutzernamen - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen.
- Protokollierung - Protokollierung der Eingabe, Änderung und Löschung von Daten
- Zugriffsrechte - Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe.

M.2.2 Beschreibung der Datenintegrität:

- Datensicherungskonzept - Erstellen eines Backup- und Wiederherstellungskonzeptes
- Dokumentensignatur - Signatur von Dokumenten, um deren Integrität sicherzustellen
- E-Mail-Signatur - Signatur von E-Mails mittels S/MIME, um deren Integrität sicherzustellen

M.2.3 Beschreibung der Speicherkontrolle:

- Berechtigungskonzept - Festlegung von Berechtigungen in einem Berechtigungskonzept
- Need-to-Know Prinzip - Anzahl der Berechtigungen und Administratoren auf das Notwendigste reduziert
- Protokollierung - Anzahl der Berechtigungen und Administratoren auf das Notwendigste reduziert

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

M.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Antivirensoftware - Einsatz von Antivirensoftware zum Schutz vor Malware
- Auslagerung Datensicherung - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Backup- und Recoverykonzept - Erstelltes Backup- und Recoverykonzept
- Hausalarm - Verwendung von Feuermeldeanlagen am Firmenstandort Paderborn
- Feuerlöschgeräte - Verwendungen CO2 Feuerlöschgeräte in kritischen Büroräumen
- IT-Notfallplan - Erstellung und Anwendung von IT-Notfallplänen

M.3.2 Beschreibung der raschen Wiederherstellbarkeit:

- Datenwiederherstellungen - Regelmäßige und dokumentierte Datenwiederherstellungen
- Notfallpläne - IT-Notfallpläne und Wiederanlaufpläne

M.4 Weitere Maßnahmen zum Datenschutz

M.4.1 Beschreibung der Auftragskontrolle:

- Audits - Regelmäßige Datenschutzaudits durch den betrieblichen Datenschutzbeauftragten.
- Auswahl - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- AV-Vertrag - Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO.
- Laufende Überprüfung - Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

M.4.2 Beschreibung des Managementsystems zum Datenschutz:

- Audits - Durchführung regelmäßiger interner Audits
- DSB - Benennung eines Datenschutzbeauftragten
- Incident-Response-System - Incident-Response-System zur Nachvollziehbarkeit von Sicherheitsverstößen und Problemen
- Managementsystem Datenschutz - Managementsystem zum Datenschutz in Anlehnung an ISO 27701.
- Schwachstellenanalysen - Durchführung regelmäßiger IT-Schwachstellenanalysen (z.B. Penetrationstest)
- Software Voreinstellungen - Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. (Art. 25 Abs. 2 DS-GVO)
- Softwaregestützte Tools - Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen (z.B. audatis MANAGER)
- Verpflichtung - Verpflichtung auf die Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, Art. 29, Art. 32 Abs. 4 DS-GVO

M.4.3 Beschreibung der Organisationskontrolle:

- Datenschutzbeauftragter - Ein Datenschutzbeauftragter ist benannt, gemeldet und seine Kontaktdaten sind veröffentlicht
- Dokumentation der Verarbeitung - Aller Verarbeitungstätigkeiten sind dokumentiert und werden regelmäßig überprüft
- Richtlinien - Es existieren verbindliche Richtlinien für den Umgang mit personenbezogenen Daten
- Sensibilisierung - Mitarbeiter werden regelmäßig zum Datenschutz sensibilisiert und geschult

Paderborn, im März 2026