Vertrag über die Auftragsverarbeitung personenbezogener Daten

zwischen der

Nica Software GmbH, Reisholzer Bahnstr. 41, 40599 Düsseldorf,

(im folgenden „Auftragnehmer“ oder „Nica Software“)

und

der Organisation, die den Testzugang zur Nica Cyber Suite beantragt

(im folgenden „Auftraggeber“)

Präambel

Dieser Vertrag regelt die Auftragsverarbeitung personenbezogener Daten im Rahmen der Nutzung des Testzugangs zur Nica Cyber Suite.

§1 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Verarbeitung personenbezogener Daten im Rahmen der Nutzung eines Testzugangs zur Nica Cyber Suite.

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers in dessen Auftrag verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU-Datenschutz-Grundverordnung zu verstehen. In diesem Sinne ist der Auftraggeber der „Verantwortliche“, der Auftragnehmer der „Auftragsverarbeiter“. Soweit in diesem Vertrag die Schriftform vorgesehen ist, genügt Textform, sofern gesetzlich nichts Abweichendes vorgeschrieben ist. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

(4) Dieser Vertrag gilt für die Verarbeitung personenbezogener Daten im Rahmen des Testzugangs zur Nica Cyber Suite. Mit der Nutzung des Testzugangs erkennt der Verantwortliche die Geltung dieses Vertrages an.

§2 Gegenstand und Dauer der Verarbeitung

(1) Der Auftragsverarbeiter erbringt im Auftrag des Verantwortlichen Leistungen im Bereich der Datenhaltung, Datenaufbereitung sowie Datenbereitstellung für den Betrieb der Nica Cyber Suite Software (nachfolgend „Software”). Alle personenbezogenen Daten, die im Rahmen des Betriebs der Software verarbeitet werden, werden von dem Verantwortlichen zuvor in das System des Auftragsverarbeiters eingetragen. Lediglich das zuvor vom Verantwortlichen festgelegte Personal „Administrator” sowie das Unternehmen werden vom Auftragsverarbeiter angelegt. Der Verantwortliche übermittelt die Administrationsdaten vor der Einrichtung der Software an den Auftragsverarbeiter. Die Administratoren haben während der Nutzung der Software ständigen Zugriff auf alle bereitgestellten Daten und können diese selbständig ergänzen, löschen und bearbeiten. Die Verarbeitung der Daten wird unter Einhaltung der geltenden Datenschutzgesetze und Vorschriften erbracht.

(2) Neben dem Hauptzweck werden personenbezogene Daten auch zum Zwecke der Bearbeitung von Supportanfragen, der technischen Administration sowie der Fehleranalyse und -behebung erhoben, verarbeitet und genutzt.

(3) Dieser Vertrag endet mit der Beendigung der beauftragten Datenverarbeitung.

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

(1) Die Verarbeitung personenbezogener Daten umfasst das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Abgleichen oder Verknüpfen, Einschränken, Löschen oder Vernichten von Daten und Dokumenten.

(2) Die Verarbeitung personenbezogener Daten erfolgt zur Bereitstellung und zum Betrieb einer Softwarelösung zur Unterstützung von Informations-, Kommunikations- und Alarmierungsprozessen sowie zur Verwaltung von Nutzerkonten, Berechtigungen, Schulungen, Dokumenten und Inhalten im Auftrag des Verantwortlichen.

(3) Folgende Datenkategorien können je nach ausgewählten Funktionsumfang vom Administrator durch direkte Eingabe oder durch hochladen in der Software verarbeitet werden:

- Personalstammdaten (z.B. Vor- und Zuname, organisatorische Zuordnung, Rollen und Berechtigungen),
- Kontakt- und Kommunikationsdaten (z. B. E-Mail-Adresse, Telefonnummer sowie Inhalte und Metadaten von Nachrichten, Benachrichtigungen und Alarmierungen),
- Unternehmens- und organisationsbezogene Daten (z.B. Name, Standorte, Telefonnummer, Mailadresse, Notfalldaten, Prozesse, Handlungsanweisungen, Notfallhandbücher, Wiederanlaufpläne)
- Technische Protokoll- und Systemdaten (z. B. Zugriffszeitpunkte, Änderungen, Fehlermeldungen, Geräteinformationen, Authentifizierungsdaten)
- Nutzerinhalte (z. B. vom Auftraggeber bereitgestellte oder in die Software eingebrachte Dokumente, Freitexteingaben oder sonstige nutzergenerierte Inhalte; die inhaltliche Bestimmung obliegt allein dem Auftraggeber)
- Nutzungs- und Protokolldaten (z. B. Teilnahme an Schulungen, Ergebnisse von Abfragen, Zustellstatus sowie technische System- und Fehlerdaten)

(4) Von der Verarbeitung betroffen sind: Beschäftigte, externe Partner sowie Drittparteien des Verantwortlichen.

§4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, sofern er nicht durch Unionsrecht oder das Recht der Mitgliedstaaten zu einer anderen Verarbeitung verpflichtet ist; in diesem Fall informiert er den Verantwortlichen vorab, sofern dies rechtlich zulässig ist.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt.

(3) Der Auftragsverarbeiter ergreift geeignete technische und organisatorische Maßnahmen, um die Sicherheit der verarbeiteten Daten gemäß Art. 32 DSGVO zu gewährleisten.

(4) Im Falle einer Datenschutzverletzung informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich.

(5) Der Auftragsverarbeiter setzt Unterauftragsverarbeiter nur im Einklang mit Art. 28 DSGVO ein. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter ergeben sich aus Anhang 1. Über deren Hinzuziehung oder Austausch informiert der Auftragsverarbeiter den Verantwortlichen mindestens 14 Tage vor Einsatz in Textform; erfolgt bis dahin kein Widerspruch aus wichtigem datenschutzrechtlichem Grund, gilt die Änderung als genehmigt.

(6) Die Verarbeitung personenbezogener Daten erfolgt grundsätzlich innerhalb der EU oder des EWR. Eine Übermittlung personenbezogener Daten in Drittländer kann erfolgen, sofern die Voraussetzungen der Art. 44 ff. DSGVO eingehalten werden, insbesondere durch geeignete Garantien gemäß Art. 46 DSGVO (z. B. Standardvertragsklauseln).

(7) Der Auftragsverarbeiter setzt zur Verarbeitung personenbezogener Daten nur Personen ein, die zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(8) Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen soweit möglich bei der Erfüllung von Anträgen betroffener Personen sowie bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO.

§5 Rechte und Pflichten des Verantwortlichen

(1) Die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie die Wahrung der Rechte der Betroffenen obliegen ausschließlich dem Verantwortlichen.

(2) Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

(3) Der Verantwortliche ist verpflichtet, sicherzustellen, dass die Administratoren in Übereinstimmung mit den geltenden Datenschutzgesetzen und den Bestimmungen dieses Vertrages handeln. Sollten durch das Handeln der Administratoren Verstöße gegen Datenschutzgesetze oder Vertragsbestimmungen entstehen, so liegt die Verantwortung hierfür beim Verantwortlichen.

(4) Der Verantwortliche ist für die rechtmäßige Nutzung der Software sowie die hinterlegten Inhalte, Nutzerdaten und Dokumente verantwortlich und muss sicherstellen, dass diese im System hinterlegt werden dürfen.

(5) Der Verantwortliche trägt die Verantwortung für Auswahl, Schulung, Berechtigungsvergabe und Überwachung seiner Administratoren. Handlungen der Administratoren innerhalb der Software gelten als Handlungen des Verantwortlichen.

(6) Der Verantwortliche stimmt der Beauftragung der in Anhang 1 vor Beginn der Verarbeitung mitgeteilten Subunternehmen zu.

(7) Der Verantwortliche ist berechtigt, die zur Prüfung der Einhaltung dieses Vertrages erforderlichen Auskünfte und geeigneten Nachweise zu verlangen. Weitergehende Überprüfungen einschließlich Inspektionen sind nur bei konkreten Anhaltspunkten für einen erheblichen Datenschutzverstoß und nach angemessener Vorankündigung zulässig.

§6 Sicherheit der Verarbeitung

(1) Die technischen und organisatorischen Maßnahmen zur Datensicherheit sind in Anhang 2 zu diesem Vertrag dokumentiert. Sie definieren das vom Auftragsverarbeiter geschuldete Minimum.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragsverarbeiter unverzüglich umzusetzen.

(3) Kopien oder Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

§7 Beendigung und Datenlöschung

(1) Im Rahmen der verarbeiteten Daten wird der Auftragsverarbeiter nur entsprechend der getroffenen vertraglichen Vereinbarung modifizieren, löschen oder sperren.

(2) Die Administratoren des Verantwortlichen sind berechtigt, Daten eigenständig zu modifizieren, zu ergänzen oder zu löschen. Der Verantwortliche trägt die volle Verantwortung für die Rechtmäßigkeit und Korrektheit dieser Änderungen. Der Auftragsverarbeiter haftet nicht für Datenschutzverstöße oder Schäden, die aus solchen Änderungen durch den Verantwortlichen oder dessen Administratoren resultieren.

(3) Nach Beendigung des Testzugangs werden die im Rahmen des Testzugangs gespeicherten personenbezogenen Daten grundsätzlich spätestens 30 Tage nach Beendigung des Testzeitraums gelöscht, sofern kein kostenpflichtiges Vertragsverhältnis zustande kommt oder gesetzliche Aufbewahrungspflichten entgegenstehen. Daten, die sich in Backups befinden, werden nicht sofort gelöscht, sondern mit dem nächsten regulären Löschzyklus der Backups; während dieser Zeit bleiben sie gesperrt und sind nicht mehr produktiv zugänglich.

§8 Haftung

(1) Verantwortlicher und Auftragsverarbeiter haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn / soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Absatz 5 DSGVO.

(3) Im Übrigen entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

§9 Schlussbestimmungen

(1) Für Nebenabreden ist die Textform und die ausdrückliche Bezugnahme auf diese Vereinbarung erforderlich, sofern gesetzlich nichts Abweichendes vorgeschrieben ist.

(2) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anhang 1

Zugelassene Subdienstleister

Firma	Anschrift	Auftragsinhalt
Local Planet UG (haftungsbeschränkt)	Neuhaustraße 15, 85134 Stammham	Wartung und Weiterentwicklung der Software
Sendinblue GmbH	Köpenicker Straße 126, 10179 Berlin	Versand von E-Mails (z.B. Erinnerungsmails, etc.)
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855 Luxembourg	Hosting aller Daten für den Betrieb der Software (Region: AWS Frankfurt)
Google Ireland Limited	Gordon House, Barrow Street, Dublin 4, Irland	Bereitstellung von Push-Benachrichtigungen sowie Verarbeitung technischer Zustell-, Fehler-, Diagnose- und Geräteinformationen

Anhang 2

Technisch-organisatorische Maßnahmen

1 Technische und organisatorische Sicherheitsmaßnahmen

Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

2 Innerbehördliche oder innerbetriebliche Organisation des Auftragsverarbeiters

Der Auftragsverarbeiter wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

3 Konkretisierung der Einzelmaßnahmen

(1) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

Nr.	Maßnahme	Umsetzung der Maßnahme
1.	**Datenverschlüsselung**	Alle personenbezogenen Daten werden sowohl bei der Übertragung (Transportverschlüsselung mittels TLS) als auch bei der Speicherung (Speicherverschlüsselung) verschlüsselt. Der Auftragsverarbeiter nutzt hierfür die durch die verwendeten Cloudlösungen* bereitgestellten Services & Verschlüsselungstechnologien.
2.	**Datensicherheit und Datenintegrität**	Der Auftragsverarbeiter nutzt AWS-Dienste zur regelmäßigen Sicherung der Daten sowie zur Gewährleistung ihrer Integrität. Hierzu gehören automatisierte Backup-Lösungen und die Verwendung von AWS-S3, um vor unbeabsichtigtem Datenverlust zu schützen.

3.	**Zugriffskontrolle**	Der Auftragsverarbeiter implementiert durch den Einsatz von AWS IAM (Identity and Access Management) detaillierte Zugriffskontrollen, die den Zugriff auf Daten und Systeme streng auf autorisierte Nutzer und Prozesse beschränken. Außerdem wird der Zugriff durch Benutzerkennungen mit Passwörtern geschützt.
4.	**Protokollierung & Überwachung**	Zugriffe und Veränderungen auf die Systeme und Daten werden protokolliert und überwacht. Der Auftragsverarbeiter überprüft regelmäßig die Protokolle, um verdächtige Aktivitäten zu identifizieren und darauf zu reagieren.
5.	**Verfügbarkeitskontrolle**	Der Auftragsverarbeiter implementiert mittels Cloudlösungen* für Datensicherung Maßnahmen, die eine hohe Verfügbarkeit der Daten und Dienste gewährleisten.
6.	**Innerbetriebliche organisatorische Maßnahmen**	Rollenbasiertes Berechtigungskonzept nach dem Need-to-know-Prinzip, Einsatz geeigneter Authentifizierungsmechanismen (z. B. Mehrfaktor-Authentifizierung) für administrative Zugriffe sowie grundlegende Sicherheitsmaßnahmen auf Entwicklungs- und Arbeitsrechnern (z. B. Virenschutz und Firewall).

*Unter Cloudlösung fallen unter anderem Dienste wie AWS.

Stand: April 2026