Vereinbarung zur Auftragsverarbeitung (AVV)

Version 2026-09-15.1 - Stand 15. September 2026

Vertragsparteien und Stand

Verantwortlicher („Unternehmen“): das im Temivaro-for-Business-Konto bezeichnete Unternehmen mit den dort hinterlegten Vertretungs- und Kontaktdaten.

Auftragsverarbeiter: Naluvio UG (haftungsbeschränkt), Allensteiner Straße 25, 75031 Eppingen, Deutschland, vertreten durch den Geschäftsführer Robin Roland Volk („Naluvio“). Datenschutzkontakt: info@temivaro.com.

Stand: 15. September 2026. Diese Vereinbarung einschließlich ihrer drei Anlagen ist Bestandteil des Vertrages über Temivaro for Business. Sie gilt nur für Verarbeitungen, bei denen Naluvio personenbezogene Daten im Auftrag des Unternehmens verarbeitet.

1. Gegenstand und Geltungsbereich

Naluvio verarbeitet die in Anlage 1 beschriebenen personenbezogenen Daten zur Bereitstellung der vom Unternehmen konfigurierten Terminbuchungs- und Terminverwaltungsfunktionen. Gegenstand, Art, Zweck, Datenarten, betroffene Personen und Dauer der Verarbeitung ergeben sich aus dieser AVV, den AGB für Temivaro for Business, dem gewählten Tarif und den Einstellungen des Unternehmenskontos.

Diese AVV konkretisiert die Pflichten der Parteien nach Art. 28 DSGVO. Bei Widersprüchen über die Auftragsverarbeitung geht sie den Business-AGB vor. Zwingendes Datenschutzrecht bleibt unberührt.

2. Rollen und Abgrenzung

Das Unternehmen ist Verantwortlicher für die von ihm veranlasste Verarbeitung der Daten seiner Terminkunden, Interessenten, Beschäftigten und sonstigen Kontakte. Es entscheidet insbesondere über angebotene Leistungen, Pflicht- und Zusatzfelder, Ressourcen, Verfügbarkeiten, Reservierungen, Nachrichten und die Nutzung bereitgestellter Löschfunktionen. Naluvio verarbeitet diese Daten in diesem Umfang als Auftragsverarbeiter.

Reservierungsdaten dürfen innerhalb der Auftragsverarbeitung nur für Reservierungsanfrage, Terminorganisation, erforderliche Kommunikation, Vermeidung von Doppelbelegungen, zulässige Dokumentation und Rechtsverteidigung verarbeitet werden. Nutzt das Unternehmen Daten darüber hinaus für Werbung, Newsletter, Profilbildung, ein eigenes CRM oder andere eigene Zwecke, handelt es hierfür außerhalb der Weisungslage und in eigener Verantwortung.

Nicht von dieser AVV erfasst sind Verarbeitungen, für die Naluvio eigene Zwecke und Mittel festlegt. Dazu gehören insbesondere Vertrags- und Kontoverwaltung gegenüber dem Unternehmen, B2B-Abrechnung, Authentifizierung, Plattformsicherheit, Missbrauchsabwehr und eigene gesetzliche Nachweise. Naluvio legt außerdem die zentralen Such- und Veröffentlichungskriterien fest, bearbeitet öffentliche Inhaltsmeldungen und trifft Moderationsentscheidungen über gemeldete Bewertungen. Für diese plattformweiten Verarbeitungen handelt Naluvio eigenständig verantwortlich. Das Unternehmen verwaltet die Inhalte und Veröffentlichung seines eigenen Profils und kann Bewertungen beantworten oder melden. Über die eigenständigen Verarbeitungen informiert die Datenschutzerklärung.

Beim Anbieterwechsel verarbeitet Naluvio die im Unternehmensdatenpaket enthaltenen Auftragsdaten weiterhin nach Weisung des Unternehmens. Das Unternehmen bestimmt, ob es zusätzlich zum eigenen Download einen fallbezogenen technischen Lesezugang erzeugt und welchem Zielanbieter es den Token übergibt. Die Verwaltung des Wechselverfahrens, die Absicherung des Zugangs und eigene Vertrags-, Sicherheits- und gesetzliche Wechselnachweise verarbeitet Naluvio in eigener Verantwortlichkeit nach Maßgabe der Datenschutzerklärung.

3. Dauer

Die AVV gilt bei erstmaligem Vertragsschluss ab ihrer Annahme, bei einer Änderung ab dem ausdrücklich vereinbarten Beginn, für die Dauer des Business-Vertrages und darüber hinaus, solange Naluvio noch personenbezogene Daten im Auftrag des Unternehmens verarbeitet. Regelungen zur Vertraulichkeit, Löschung, Rückgabe und zu gesetzlichen Nachweisen wirken ihrem Zweck entsprechend fort.

4. Weisungen des Unternehmens

Mit „Karte erstellen“ oder „Karte neu erstellen“ weist ein berechtigter Unternehmensadministrator Naluvio an, die gespeicherte Unternehmensadresse zur Geocodierung und die ermittelten Koordinaten zur Erstellung eines Standortkartenbildes an Geoapify zu übermitteln, das Bild bei Temivaro zu speichern und auf der freigegebenen Buchungsseite anzuzeigen. Die Weisung umfasst keine Übermittlung von Kunden- oder Termindaten oder von Verbindungsdaten der Buchungsseitenbesucher. Das Unternehmen stellt die Rechtsgrundlage und die Information betroffener Personen sicher, soweit Standortangaben personenbezogen sind.

Naluvio verarbeitet Auftragsdaten ausschließlich auf dokumentierte Weisung des Unternehmens, einschließlich einer Übermittlung in ein Drittland, sofern nicht Unionsrecht oder das Recht eines Mitgliedstaats eine Verarbeitung verlangt. In diesem Fall informiert Naluvio das Unternehmen vor der Verarbeitung über die betreffende Rechtspflicht, soweit das Recht eine solche Mitteilung nicht aus wichtigem öffentlichem Interesse verbietet.

Die erstmaligen Weisungen ergeben sich aus dieser AVV, den Business-AGB und der Nutzung sowie Konfiguration der Plattform. Weitere Weisungen können ausschließlich durch berechtigte Unternehmens-Admins über vorgesehene Kontofunktionen oder in Textform an info@temivaro.com erteilt werden. Mitarbeiter dürfen die innerhalb ihrer festen Rolle vorgesehenen operativen Termin- und Anfragefunktionen ausüben, aber keine vertrags- oder datenschutzbezogenen Weisungen gegenüber Naluvio erteilen. Verursacht eine zusätzliche Weisung Aufwand außerhalb des vereinbarten Leistungsumfangs, stimmen die Parteien die Umsetzung und eine angemessene Vergütung vorher ab.

Hält Naluvio eine Weisung für datenschutzrechtswidrig, informiert Naluvio das Unternehmen unverzüglich und darf ihre Ausführung bis zur Bestätigung oder Änderung aussetzen.

5. Pflichten des Unternehmens

Das Unternehmen stellt die Rechtmäßigkeit der Verarbeitung sicher, erfüllt Informationspflichten gegenüber betroffenen Personen und gewährleistet eine Rechtsgrundlage für Erhebung, Nutzung, Übermittlung und Weisungen. Es nutzt nur erforderliche Felder und hält Daten richtig. Es hinterlegt seine Datenschutzinformation als eigenen Text oder als Link auf eine eigene Datenschutzinformation. Temivaro stellt den hinterlegten Text beziehungsweise Link technisch bereit. Für Inhalt, Vollständigkeit und Aktualität dieser Information ist das Unternehmen verantwortlich. Die Datenschutzerklärung von Naluvio erläutert die dort beschriebenen Verarbeitungen durch Temivaro und ersetzt die Informationspflichten des Unternehmens nicht.

Das Unternehmen benennt mindestens einen erreichbaren und zur Kontoverwaltung berechtigten Unternehmens-Admin, hält dessen Kontaktadresse aktuell und stellt sicher, dass jede berechtigte Person ausschließlich einen eigenen persönlichen Zugang verwendet. Es prüft vor einer Einladung die betriebliche Berechtigung, beschränkt Zugänge auf erforderliche Personen und sperrt oder entfernt ausgeschiedene beziehungsweise nicht mehr berechtigte Mitarbeiter unverzüglich. Gemeinsam verwendete Mitarbeiterkonten sind unzulässig. Das Unternehmen informiert Naluvio unverzüglich über Fehler, Unregelmäßigkeiten oder Verdachtsfälle, die Auftragsdaten betreffen.

Die gezielte Erhebung oder Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO und von Daten über strafrechtliche Verurteilungen und Straftaten ist nicht Gegenstand dieser AVV oder der zum Start freigegebenen Temivaro-Funktionen. Das Unternehmen darf solche Daten weder über Zusatzfelder, Feldbezeichnungen, Nachrichten, Notizen, Bewertungen, Antworten noch über andere Temivaro-Funktionen abfragen, anfordern oder zum Gegenstand einer Weisung machen. Eine außerhalb der Plattform eingeholte Einwilligung oder eine einfache Zusatzvereinbarung erweitert den Auftragsgegenstand nicht.

Eigeninitiativ oder versehentlich eingegebene sensible Angaben lassen sich durch Hinweise und begrenzte technische Guardrails nicht vollständig ausschließen. Sie erweitern den vereinbarten Verarbeitungszweck nicht. Nach Kenntnis darf das Unternehmen den Inhalt nicht regulär weiterverwenden und muss ihn unverzüglich feldgenau redigieren oder Naluvio unter Angabe der Termin- und Feldkennung, jedoch ohne Wiederholung des sensiblen Inhalts, hierzu anweisen. Naluvio darf eine solche Redaktion als ständige Weisung ausführen; der Nachweis dokumentiert nur Art und Zeitpunkt der Redaktion, nicht den entfernten Inhalt. Eine umfassende Überwachung oder allgemeine KI-Analyse aller Freitexte ist nicht geschuldet.

6. Allgemeine Pflichten von Naluvio

Naluvio verarbeitet Auftragsdaten nur im vereinbarten Umfang, unterstützt das Unternehmen bei der Einhaltung seiner datenschutzrechtlichen Pflichten und führt die nach Art. 30 Abs. 2 DSGVO erforderlichen Verzeichnisse. Naluvio stellt sicher, dass der Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen angemessen berücksichtigt wird.

Naluvio berichtigt, löscht, beschränkt, anonymisiert oder übergibt Daten entsprechend den dokumentierten Weisungen und den vereinbarten Plattformfunktionen. Eigenmächtige Kopien oder Verwendungen zu eigenen Zwecken sind ausgeschlossen, soweit sie nicht gesetzlich vorgeschrieben oder als eigenständige Verarbeitung nach Ziffer 2 ausgewiesen sind.

7. Vertraulichkeit

Naluvio setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Sie erhalten Zugriff nur, soweit dies für ihre Aufgaben erforderlich ist, und werden über die maßgeblichen Datenschutz- und Sicherheitsanforderungen unterrichtet.

8. Sicherheit der Verarbeitung

Naluvio trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie der Risiken angemessene technische und organisatorische Maßnahmen nach Art. 32 DSGVO. Die zum Stand dieser AVV vorgesehenen Maßnahmen sind in Anlage 2 beschrieben.

Naluvio darf einzelne Maßnahmen weiterentwickeln oder durch gleichwertige beziehungsweise wirksamere Maßnahmen ersetzen, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche nachteilige Änderungen werden dem Unternehmen mitgeteilt.

9. Unterauftragsverarbeiter

Das Unternehmen erteilt Naluvio die allgemeine schriftliche Genehmigung, die in Anlage 3 genannten Unterauftragsverarbeiter einzusetzen. Naluvio verpflichtet diese vertraglich zu einem dieser AVV im Wesentlichen gleichwertigen Datenschutz- und Sicherheitsniveau und bleibt gegenüber dem Unternehmen für die Erfüllung der Auftragsverarbeiterpflichten verantwortlich.

Beauftragt oder ersetzt Naluvio selbst einen Unterauftragsverarbeiter, informiert Naluvio das Unternehmen mindestens 15 Tage vorher an die zuletzt hinterlegte Unternehmens- oder Administrator-E-Mail-Adresse. Das Unternehmen kann innerhalb dieser Frist aus konkreten datenschutzrechtlichen Gründen widersprechen. Änderungen weiterer Unterauftragsverarbeiter innerhalb einer bereits genehmigten Verarbeitungskette teilt Naluvio unverzüglich nach Eingang der Anbieterinformation und so rechtzeitig vor deren Einsatz mit, dass das Unternehmen die Änderung prüfen und widersprechen kann. Die Mitteilung nennt den betroffenen Anbieter, die Änderung, ihren vorgesehenen Beginn und den Widerspruchsweg. Reicht der vom Anbieter gewährte Vorlauf hierfür nicht aus, muss Naluvio vor dem Einsatz eine Verschiebung, eine geeignete Alternative oder eine Unterbrechung der betroffenen Verarbeitung sicherstellen; eine verspätete Mitteilung ersetzt die vorherige Widerspruchsmöglichkeit nicht. Können die Parteien keine zumutbare Lösung finden, kann jede Partei den betroffenen Dienst zum Änderungszeitpunkt außerordentlich beenden.

Nebenleistungen ohne Zugriff auf Auftragsdaten, etwa Telekommunikations-, Transport-, Wartungs- oder Entsorgungsleistungen, gelten nicht als Unterauftragsverarbeitung. Naluvio stellt auch bei ihnen einen angemessenen Schutz sicher.

10. Drittlandübermittlungen

Übermittlungen personenbezogener Auftragsdaten in ein Drittland einschließlich entsprechender Zugriffe erfolgen auf dokumentierte Weisung des Unternehmens und nur, wenn zusätzlich die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind. Die in Ziffer 4 beschriebene Ausnahme bei einer Verarbeitungspflicht nach Unionsrecht oder dem Recht eines Mitgliedstaats betrifft ausschließlich das Weisungserfordernis; sie ersetzt keine erforderliche Transfergrundlage. Naluvio dokumentiert die Grundlage für die konkrete Empfänger- und Verarbeitungskette. In Betracht kommen insbesondere ein einschlägiger Angemessenheitsbeschluss – bei Nutzung des EU-US Data Privacy Framework einschließlich einer gültigen, die betreffende Verarbeitung erfassenden Zertifizierung des Empfängers – oder geeignete Garantien wie die Standardvertragsklauseln der Europäischen Kommission. Soweit erforderlich, werden die tatsächlichen Transferumstände bewertet und zusätzliche Schutzmaßnahmen getroffen. Ausnahmen nach Art. 49 DSGVO dürfen nur bei Vorliegen ihrer jeweiligen Voraussetzungen genutzt werden und dienen nicht als pauschale Grundlage regelmäßiger Übermittlungen.

11. Unterstützung bei Betroffenenrechten

Naluvio unterstützt das Unternehmen unter Berücksichtigung der Art der Verarbeitung durch geeignete technische und organisatorische Maßnahmen dabei, Anträge auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und weitere Betroffenenrechte zu beantworten. Geht ein Antrag erkennbar zu Auftragsdaten unmittelbar bei Naluvio ein, leitet Naluvio ihn ohne unangemessene Verzögerung an das Unternehmen weiter und antwortet nicht eigenständig, sofern keine gesetzliche Pflicht besteht.

12. Verletzungen des Schutzes personenbezogener Daten

Naluvio informiert das Unternehmen unverzüglich, nachdem Naluvio eine Verletzung des Schutzes von Auftragsdaten bekannt geworden ist. Die Mitteilung enthält, soweit verfügbar, Art und Umfang des Vorfalls, betroffene Daten und Personen, wahrscheinliche Folgen, ergriffene oder vorgeschlagene Abhilfemaßnahmen sowie eine Kontaktstelle. Fehlende Informationen werden ohne unangemessene Verzögerung nachgereicht.

Naluvio unterstützt das Unternehmen angemessen bei Untersuchung, Eindämmung, Dokumentation und den Pflichten aus Art. 33 und 34 DSGVO. Die Entscheidung, ob eine Meldung an die Aufsichtsbehörde oder Benachrichtigung betroffener Personen erforderlich ist, trifft das Unternehmen, soweit es Verantwortlicher ist.

13. Datenschutz-Folgenabschätzung und Aufsichtsbehörden

Naluvio unterstützt das Unternehmen unter Berücksichtigung der verfügbaren Informationen und der Art der Verarbeitung angemessen bei Datenschutz-Folgenabschätzungen, vorherigen Konsultationen und der Zusammenarbeit mit Aufsichtsbehörden, soweit die Auftragsverarbeitung betroffen ist.

14. Nachweise und Kontrollen

Naluvio stellt dem Unternehmen die zur Darlegung der Einhaltung von Art. 28 DSGVO erforderlichen Informationen zur Verfügung. Vorrangig können aktuelle geeignete Zertifikate, Prüfberichte, Sicherheitsdokumentationen oder Selbstauskünfte verwendet werden.

Das Unternehmen oder ein zur Verschwiegenheit verpflichteter unabhängiger Prüfer darf nach angemessener Vorankündigung während üblicher Geschäftszeiten eine erforderliche Kontrolle durchführen. Kontrollen dürfen den Betrieb, die Sicherheit anderer Kunden, Geschäftsgeheimnisse und personenbezogene Daten Dritter nicht unangemessen beeinträchtigen. Anlasslose Prüfungen sind grundsätzlich auf eine pro Jahr beschränkt; bei einem konkreten Sicherheitsvorfall, einer behördlichen Anordnung oder begründeten Zweifeln gilt diese Beschränkung nicht. Jede Partei trägt ihre eigenen Kosten, sofern eine Prüfung keinen wesentlichen von Naluvio zu vertretenden Verstoß feststellt.

15. Rückgabe, Export und Löschung

Während des Vertrages kann das Unternehmen die bereitgestellten Export- und Löschfunktionen nutzen. Nach der E-Mail-Bestätigung wird die Unternehmenslöschung ohne zusätzliche Sicherheitsfrist ausgeführt; sie kann nicht über einen internen Wiederherstellungslink widerrufen werden. Noch offene Leistungen, ein laufender Anbieterwechsel, eine offene Datenschutzanfrage, ein ungeklärter Inhaltsfall oder eine aktive Aufbewahrungssperre können die Ausführung im erforderlichen Umfang verhindern. Bei der Ausführung entfernt Naluvio das operative Profil, Medien, Leistungen, Ressourcen, Verfügbarkeiten und nicht mehr erforderliche Freitexte. Die Unternehmenszuordnungen werden entfernt; ein persönlicher Zugang mit weiteren Unternehmenszuordnungen bleibt für diese erhalten.

Vertragsnachweise werden nach Anlage 1 auf die für bestehende Zwecke notwendigen Inhalte beschränkt. Soweit ein Beleg für den Vertrag zwischen Unternehmen und Terminkunde oder für eine gesetzliche Pflicht des Unternehmens erforderlich bleibt, setzt Naluvio dessen Verarbeitung im Rahmen der dokumentierten Restaufbewahrungsweisung fort. Das Vertragsende allein begründet keine eigene Verantwortlichkeit Naluvios für diese Daten. Nur konkret erforderliche eigene Vertrags-, Abrechnungs-, Sicherheits- und Rechtsverteidigungsnachweise verarbeitet Naluvio in eigener Verantwortlichkeit nach der Datenschutzerklärung. Ein Export entbindet keine Partei von ihren jeweils anwendbaren Pflichten.

Ein gesperrter, nicht öffentlicher technischer Unternehmensrest bleibt nur bis zum Ende der letzten erforderlichen Abhängigkeit. Getrennte, zweckgebunden zugängliche Vertragsnachweise können den zur Zuordnung benötigten Kundennamen, die E-Mail-Adresse, Vertragsparteien und Kontaktangaben sowie ursprüngliche Vertragsbedingungen und Erklärungen enthalten. Diese Daten bleiben personenbezogen und stehen nicht für Kalender, Werbung oder allgemeine Kundenhistorien zur Verfügung. Terminkunden erhalten auch ohne Kundenkonto einen gesicherten Zugang zu den erforderlichen Informationen und Erklärungsfunktionen. Das Unternehmensarchiv ist vor der Löschung als passwortbestätigtes ZIP verfügbar.

Für einen dokumentierten Anbieterwechsel kann das Unternehmen zusätzlich einen fallbezogenen, zeitlich begrenzten Lesezugang an einen von ihm autorisierten Zielanbieter übergeben. Dabei handelt es sich nicht um eine offene Wechsel-API: Manifest und ZIP-Export sind nur über HTTPS, die konkrete Vorgangskennung und einen vom Unternehmen weitergegebenen Bearer-Token lesbar. Der Token wird nur als Prüfsumme gespeichert, kann widerrufen oder ersetzt werden und wird bei Abschluss, Abbruch, Ablehnung oder Ablauf des Vorgangs entfernt. Zugriffe sind auf das betreffende Unternehmen und den Abrufzeitraum beschränkt; Daten anderer Mandanten, Passwörter, Sitzungen, MFA-Geheimnisse und interne Sicherheitsdaten sind ausgeschlossen.

Personenbezogene Antragsteller-, Zielkontakt-, Begründungs- und Ereignisdetails eines beendeten Anbieterwechsels werden nach höchstens 90 Tagen entfernt. Der danach verbleibende Sachnachweis enthält nur Fallnummer, Wechselart, Status, notwendige Zeitpunkte, Bestätigungs- und Löschstatus sowie Ereignisarten ohne Freitext und Akteurkennung. Er wird regulär mit Beginn des vierten Kalenderjahres nach Ende des Vorgangs gelöscht. Eine konkret dokumentierte Aufbewahrungssperre kann den erforderlichen Nachweis vorübergehend erhalten, niemals jedoch einen abgelaufenen Zugangstoken. Diese Fristen gelten unabhängig davon, ob das Unternehmenskonto zuvor gelöscht wird.

Sicherungskopien werden getrennt und verschlüsselt aufbewahrt und nicht für die gewöhnliche Nutzung oder neue Zwecke verwendet. Die reguläre Aufbewahrungsfrist beträgt 30 Tage ab Erstellung; fällige Kopien werden im täglichen Bereinigungslauf entfernt, im störungsfreien Betrieb innerhalb des folgenden Tages. Verhindert eine technische Störung die Bereinigung oder würde sie die letzte verwertbare Wiederherstellungsmöglichkeit beseitigen, wird der Fall unverzüglich geprüft. Eine längere Aufbewahrung ist nur im konkret erforderlichen Umfang und für die Dauer der Störungsbehebung zulässig. Grund, betroffene Kopien und nächster Prüftermin werden dokumentiert; die Notwendigkeit wird täglich überprüft. Nach Wegfall des Grundes werden die fälligen Kopien unverzüglich entfernt. Vor einer produktiven Nutzung wiederhergestellter Daten werden zwischenzeitliche Löschungen, feldbezogene Redaktionen, Berichtigungen und Berechtigungsänderungen abgeglichen und umgesetzt. Bis zum Abschluss bleibt der wiederhergestellte Bestand gesperrt.

16. Staatliche Offenlegungsanfragen

Naluvio informiert das Unternehmen über behördliche oder gerichtliche Anfragen nach Auftragsdaten, soweit dies rechtlich zulässig ist. Naluvio prüft die Zuständigkeit und Reichweite einer Anfrage, gibt nur die rechtlich erforderlichen Daten heraus und nutzt verfügbare Rechtsbehelfe gegen offensichtlich unverhältnismäßige oder rechtswidrige Anordnungen.

17. Haftung

Für die Haftung der Parteien gelten Art. 82 DSGVO und ergänzend die Haftungsregelungen der Business-AGB, soweit diese mit zwingendem Datenschutzrecht vereinbar sind. Eine Haftungsregelung gegenüber betroffenen Personen wird durch diese AVV nicht eingeschränkt.

18. Schlussbestimmungen

Inhaltliche Änderungen dieser AVV einschließlich der Anlagen werden nur durch ausdrückliche Vereinbarung wirksam und in Textform dokumentiert. Für Änderungsangebote gelten Mitteilung, Anpassungsfrist, die gesonderte Entscheidungsfrist, Zustimmung, getrennte Ablehnung und Sonderkündigung nach Ziffer 23 der Business-AGB entsprechend. Bis zum vereinbarten Beginn bleibt die bisher vereinbarte AVV mit ihren Weisungen maßgeblich. Eine neue Veröffentlichung oder eine noch nicht wirksame Annahme erlaubt insbesondere keine vorzeitige Anwendung neuer Löschfristen, Verarbeitungszwecke oder Drittlandübermittlungen. Reine Informationen über Unterauftragsverarbeiter innerhalb einer bereits erteilten allgemeinen Genehmigung folgen dem Mitteilungs- und Widerspruchsverfahren nach Ziffer 9; sie erfordern nicht allein wegen ihrer Mitteilung eine neue AVV-Annahme.

Vertragsbezogene Mitteilungen werden an die zuletzt hinterlegte Unternehmens- oder Administrator-E-Mail-Adresse gesendet; das Unternehmen hält diese Adressen aktuell. Eine Übertragung des Unternehmenskontos auf einen anderen Rechtsträger erfasst die AVV nur mit vorheriger Zustimmung von Naluvio; eine gesetzliche Gesamtrechtsnachfolge bleibt unberührt.

Es gilt deutsches Recht, soweit das Datenschutzrecht keine abweichenden zwingenden Regelungen enthält. Sollte eine Bestimmung unwirksam sein oder werden, gelten an ihrer Stelle die gesetzlichen Vorschriften; die übrigen Bestimmungen bleiben wirksam.

Anlage 1

Beschreibung der Verarbeitung

1. Gegenstand, Zweck und Dauer

Bereitstellung der vom Unternehmen konfigurierten Online-Terminreservierung, Anfrage- und Terminverwaltung, Kalender- und Ressourcenplanung, reservierungsbezogenen Kommunikation, Bewertungsabwicklung sowie zugehöriger Support-, Export-, Anbieterwechsel-, Sicherheits- und Löschfunktionen. Die Verarbeitung dauert grundsätzlich bis zum Ende des Business-Vertrages zuzüglich der vereinbarten Export-, Lösch- und Sicherungsfristen.

2. Art der Verarbeitung

Bei beauftragter Standortkartenerstellung zusätzlich: Geocodierung der Unternehmensadresse durch den in Anlage 3 genannten Anbieter, Erstellung und Speicherung eines Kartenbildes sowie dessen Auslieferung durch Temivaro. Seitenaufrufe und Adressänderungen erzeugen keine erneute externe Kartenerstellung.

Erheben, Erfassen, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln an vom Unternehmen bestimmte Empfänger, Abgleichen, Einschränken, Exportieren, Anonymisieren und Löschen. Die konkrete Verarbeitung richtet sich nach den aktivierten Funktionen und Weisungen des Unternehmens.

3. Betroffene Personen

- Terminkunden, Interessenten und sonstige Kontakte des Unternehmens
- Unternehmensinhaber und sonstige natürliche Personen, auf die sich die für eine Standortkarte verwendete Geschäftsanschrift bezieht
- Beschäftigte, freie Mitarbeitende, Ressourcenverantwortliche und Administratoren des Unternehmens
- Personen, die Nachrichten, Bewertungen oder Termininformationen mit Bezug zum Unternehmen übermitteln

4. Datenarten

- Stamm- und Kontaktdaten, insbesondere Name, E-Mail-Adresse und optional Telefonnummer
- Bei Standortkarten: Unternehmensadresse, daraus ermittelte Koordinaten, Kartenbild sowie zugehörige Erstellungs- und Zuordnungsdaten, soweit personenbezogen
- Termin-, Reservierungs-, Leistungs-, Ressourcen-, Verfügbarkeits- und Statusdaten
- Versionierte Angebots-, Vertrags-, Verbraucherinformationen-, Annahme-, Leistungsbeginn-, Zustell- und Widerrufsnachweise einschließlich Zeitpunkten und Integritätsprüfwerten
- Kommunikationsinhalte, freiwillige Nachrichten, Antworten und vom Unternehmen konfigurierte Zusatzfelder
- Kundenhistorie, Stornierungen, Verschiebungen, Bewertungen und Bearbeitungsvermerke
- Technische Zuordnungs-, Protokoll- und Sicherheitsdaten, soweit sie der Auftragsverarbeitung zuzurechnen sind
- Beim Anbieterwechsel: exportierbare Unternehmens-, Termin- und Kundendaten sowie Fall-, Ziel-, Frist-, Abruf- und Übergabeinformationen

5. Besondere Kategorien

Die gezielte Erhebung oder Verarbeitung von Daten nach Art. 9 DSGVO oder von Daten über strafrechtliche Verurteilungen und Straftaten ist nicht vereinbart und für die zum Start freigegebene Produktfassung ausgeschlossen. Eine einfache gesonderte Vereinbarung lässt diese Verarbeitung im bestehenden Produkt nicht zu. Eine künftige Nutzung wäre nur mit einer dafür ausdrücklich freigegebenen Produktfassung sowie einem zuvor neu festgelegten Rechts-, Sicherheits- und Vertragskonzept möglich. Versehentliche Eingaben werden nach Kenntnis nach dem in Ziffer 5 beschriebenen Redaktionsverfahren behandelt.

6. Löschfristen und Weisungsmöglichkeiten

Standortkarten werden mit zugehöriger Adresse bis zum Entfernen, Ersetzen durch eine neu erstellte Karte oder zur Löschung des Unternehmensprofils gespeichert. Eine Adressänderung blendet die alte Karte aus, löscht sie jedoch nicht automatisch. Mit „Karte entfernen“ weist das Unternehmen die Löschung von Bild und zugehörigen Kartenmetadaten an. Für Sicherungskopien gelten die vorstehend geregelte reguläre Aufbewahrungsfrist von 30 Tagen, der tägliche Bereinigungslauf und die begrenzte Störungsregelung. Die Anbieterfristen für Anfragedaten bei Geoapify ergeben sich aus Anlage 3.

Mit Wirksamwerden dieser AVV weist das Unternehmen Temivaro an, die folgenden Standardfristen automatisch anzuwenden: sechs Monate für operative personenbezogene Termindaten, Anfragen ohne Vertragsschluss, interne Terminnotizen und Tagesnotizen. Beim erstmaligen Vertragsschluss gelten die Standardfristen ab Annahme dieser AVV. Bei einer Vertragsänderung gelten sie erst ab deren vereinbartem Beginn. Eine gesonderte Aktivierung in den Einstellungen ist nicht erforderlich. Diese Standardwerte sind keine gesetzlichen Vorgaben; das Unternehmen prüft ihre Eignung für seine Zwecke und Pflichten und kann sie in „Aufbewahrung & Löschung“ ändern. Bereits ausdrücklich festgelegte Unternehmensfristen bleiben erhalten.

Änderungen werden nach Anzeige ihrer Auswirkungen ausdrücklich bestätigt und gelten ab Speicherung für vorhandene und künftige Daten. Die Standardweisung wird mit der AVV-Annahme, ihrer Version, den Fristen, dem Annahmezeitpunkt, dem Anwendungsbeginn und der handelnden Benutzerkennung dokumentiert; individuelle

Änderungen werden ebenfalls versioniert. Fällige Daten werden im regelmäßigen Löschlauf bereinigt. Eine Verlängerung stellt bereits gelöschte Daten nicht wieder her. Das Unternehmen hält seine Datenschutzhinweise entsprechend aktuell.

Noch offene Leistungen, erforderlicher Erklärungszugang und konkrete Bearbeitungs- oder Rechtsfälle gehen für die jeweils erforderlichen Daten vor. Nicht mehr benötigte Notizen, Telefonnummern, Zusatzfelder und Ressourcenbezüge werden entfernt. Eine manuelle Kalenderentfernung beendet die Kalenderanzeige und entfernt nicht mehr erforderliche operative Inhalte, lässt jedoch notwendige Vertragsnachweise bestehen. Laufende Buchungen können nicht durch diese Funktion gelöscht werden. Die personenbezogene Kundenkontohistorie wird grundsätzlich 24 Monate nach Terminende entfernt; ein früheres Löschverlangen wird gesondert geprüft. Diese Betriebsfrist ist ein zweckbezogener Standard, keine gesetzliche Mindestfrist.

Nach der operativen Bereinigung bleiben ausschließlich die noch notwendigen Belege: Buchungsnummer, Parteien und Kontakt für den Nachweiszugang, Leistung, Preis, Termin, ursprüngliche Vertragsbedingungen, Dokumentversionen, Erklärungsinhalt und erklärende Person sowie die notwendigen Ereignis- und Zustellzeitpunkte. Nicht benötigte operative Zusatzdaten werden entfernt. Die Nachweise bleiben personenbezogen beziehungsweise pseudonymisiert; sie sind nicht anonym. Historische Prüfwerte bezeichnen den früheren Originalzustand. Der minimierte Datensatz erhält einen eigenen aktuellen Prüfwert; allein die Hash-Prüfung rechtfertigt keine weitere Originalkopie.

Die folgenden Standardregeln werden mit dieser AVV vereinbart und automatisch angewendet. Eine gesonderte Einrichtung, Begründung oder Bestätigung im Unternehmenskonto ist nicht erforderlich. Minimale Anspruchsnachweise entgeltlicher Buchungsverträge werden grundsätzlich drei Jahre ab Ende des maßgeblichen Leistungs- oder Abwicklungsjahres aufbewahrt. Dies ist eine begründete Standardweisung zur Anspruchssicherung, keine gesetzliche Speicherpflicht aus §§ 195, 199 BGB. Kostenlose Buchungen und nicht angenommene Anfragen erhalten ohne weiteren erforderlichen Zweck keine automatische Dreijahresfrist. Notizen, Telefonangaben und sonstige nicht erforderliche Inhalte folgen unabhängig ihren kürzeren Löschregeln. Soweit das Unternehmen Handels- oder Geschäftsbriefe nach § 257 HGB oder § 147 AO sechs Jahre aufbewahren muss, sichert es die erforderlichen Unterlagen rechtzeitig über den Datenexport in seinem eigenen Archiv oder vereinbart mit Naluvio eine dokumentierte abweichende Weisung. Die Standardfrist ersetzt diese gesetzliche Pflicht nicht; eine ungeklärte Einordnung begründet aber auch keine pauschale Sechsjahresfrist in Temivaro. Bereits dokumentierte abweichende Weisungen und bestehende Nachweisfristen werden nicht automatisch überschrieben. Konkrete Streitfälle und gesetzliche Verlängerungen werden durch begrenzte, regelmäßig überprüfte Aufbewahrungssperren behandelt. Rechnungs- und Buchführungsunterlagen unterliegen ihren eigenen gesetzlichen Fristen und rechtfertigen keine vollständige Kontoaufbewahrung.

Technische Kontaktdatensätze ohne Verknüpfung zu einem Termin werden im regelmäßigen Bereinigungslauf entfernt, sobald kein Termin mehr darauf verweist und keine konkrete Aufbewahrungssperre für den Kontakt oder das Unternehmen besteht. Hierfür wird keine eigene Aufbewahrungsfrist eingestellt. Erforderliche Buchungsnachweise und eigenständige Kundenkonten bleiben davon unberührt.

Tagesnotizen folgen dem Ende des notierten Tages, Terminnotizen dem Ende des letzten Termintags, jeweils Europe/Berlin. Bearbeitungen der Notiz verlängern die Frist nicht. Terminnotizen werden spätestens zusammen mit den zugehörigen operativen Termindaten entfernt. Aktive Löschsperren sowie die vereinbarte Abwicklung nach Vertragsende werden gesondert berücksichtigt.

Nach bestätigter Unternehmenslöschung endet die operative Nutzung. Mitgliedschaften und unternehmensbezogene Einstellungen werden gelöscht, während Zugänge zu anderen Unternehmen erhalten bleiben. Vertrags- und Betroffenenrechte sowie konkret erforderliche Nachweise dürfen durch Kaskaden nicht verloren gehen. Solange ein offener Fall eine abhängige Datenstruktur noch benötigt, kann deren Löschung eingeschränkt sein. Nach Abschluss oder ausdrücklicher Freigabe wird die reguläre Bereinigung nachgeholt; eine Sperre erlaubt keine allgemeine weitere Nutzung.

Mit der Annahme dieser AVV weist das Unternehmen die auf notwendige Vertragsbelege und den gesicherten Erklärungszugang begrenzte Restverarbeitung nach diesen Regeln an. Es teilt Naluvio eine abweichende gesetzliche Einordnung oder einen konkreten Rechtsfall in Textform mit. Naluvio klärt noch nicht eingeordnete Altbestände und die anwendbare Nachweisklasse vor einer Verkürzung mit dem Unternehmen. Die Restverarbeitung endet mit Wegfall

des letzten tragfähigen Zwecks; die Unternehmenslöschung verlängert keine Frist. Einzelfallverlängerungen erfordern einen dokumentierten Grund und einen überprüfbaren Umfang.

Aktive Aufbewahrungssperren werden mindestens alle 90 Tage zur manuellen Prüfung fällig. Eine überfällige Prüfung wird der Systemadministration angezeigt, beendet die Sperre aber niemals automatisch. Erst eine ausdrückliche Freigabe lässt die reguläre Löschung wieder greifen.

Für Anbieterwechsel gilt ergänzend: Der technische Token-Nachweis wird mit Beendigung des Vorgangs entfernt. Personen-, Zielkontakt-, Begründungs- und Ereignisdetails werden nach höchstens 90 Tagen minimiert. Der verbleibende Sachnachweis wird regulär mit Beginn des vierten Kalenderjahres nach Ende des Vorgangs gelöscht. Eine konkrete Aufbewahrungssperre darf nur erforderliche Nachweise verlängern und reaktiviert keinen technischen Zugang.

Bei einer feldgenauen Redaktion wird der ausgewählte Freitext aus den aktiven Produktivdaten entfernt; Termin, Status und notwendige Vertragsnachweise bleiben bestehen. Das Redaktionsereignis enthält keinen entfernten Inhalt. In getrennten Sicherungskopien kann der Wert bis zur Bereinigung nach der vorstehend beschriebenen Backupregelung verbleiben, wird dort aber nicht regulär verwendet. Vor einer produktiven Nutzung wiederhergestellter Daten sind zwischenzeitliche Redaktionen einschließlich betroffener interner Kopien erneut anzuwenden.

Anlage 2

Technische und organisatorische Maßnahmen (TOMs)

1. Organisation und Zutrittskontrolle

- Direkter Serverzugriff und administrative Anbieter-Konten sind auf die für den Betrieb berechtigten Personen beschränkt. Der administrative Serverzugriff wird durch SSH-Schlüssel geschützt.
- Naluvio verantwortet den technischen Betrieb, die Vergabe und den Entzug von Berechtigungen sowie die regelmäßige Überprüfung der Schutzmaßnahmen.
- Zugriffe auf Produktionssysteme und Auftragsdaten erfolgen nach Aufgabenbezug und Erforderlichkeit. Support- und Systemverwaltungsaktionen werden soweit technisch vorgesehen protokolliert.
- Zur Verarbeitung werden nur Personen eingesetzt, die einer vertraglichen oder gesetzlichen Vertraulichkeitspflicht unterliegen.
- Physischer Rechenzentrumsschutz wird durch den bestätigten Hostinganbieter erbracht.

2. Zugangs- und Authentifizierungsschutz

- Passwörter werden mit einem speicherintensiven Scrypt-Verfahren gehasht; Sitzungskennungen werden zufällig erzeugt und nur gehasht gespeichert.
- HTTP-only-, SameSite-Strict- und im Produktivbetrieb Secure-Cookies, begrenzte Sitzungsdauer sowie getrennte Sitzungen für Systemadministration, Unternehmens- und Kundenkonten.
- Unternehmensnutzer verwenden persönliche Konten. Mitarbeiter werden über einen nur einmal verwendbaren, 48 Stunden gültigen Einladungslink eingeladen; das Einladungsgeheimnis wird ausschließlich gehasht gespeichert. Bestehende Konten werden nach Passwortprüfung sicher zugeordnet, neue Nutzer legen ihr Passwort selbst fest.
- Bei Sperrung oder Entfernung eines Mitarbeiterzugangs werden dessen Sitzungen für das betreffende Unternehmen unmittelbar ungültig gemacht. Passwortzurücksetzungen erfolgen nur über den persönlichen, zeitlich begrenzten Passwort-Reset-Ablauf.
- Systemadministratoren verwenden Mehrfaktor-Authentifizierung. Persistente Rate-Limits schützen relevante öffentliche Eingänge.
- Cloudflare Turnstile ist mit Produktivschlüsseln für die vorgesehenen Kunden-, Reservierungs- und Unternehmenszugänge konfiguriert.

- Persönliche Verwaltungslinks werden kryptografisch signiert, an den jeweiligen Termin gebunden und sind bis 90 Tage nach Terminende gültig. Bei einer Terminverschiebung wird ihre Gültigkeit automatisch angepasst.

3. Zugriffs- und Mandantentrennung

- Mandantenzuordnung erfolgt über eindeutige Unternehmenskennungen, serverseitige Berechtigungsprüfungen und referenzielle Datenbankregeln.
- Getrennte Endpunkte und Berechtigungsprüfungen schützen Systemadministration, Unternehmensnutzer und Terminkunden. Direkte URLs, manipulierte Objektkennungen und API-Aufrufe unterliegen denselben serverseitigen Rollen- und Mandantenprüfungen wie die Navigation.
- Im Unternehmensbereich bestehen die festen Rollen Unternehmens-Admin und Mitarbeiter. Mitarbeiter erhalten nur die für Übersicht, Kalender und Anfragen notwendigen Lese- und Bearbeitungsfunktionen; Leistungs-, Ressourcen-, Einstellungs-, Veröffentlichungs-, Abrechnungs-, Vertrags-, Export- und Anbieterwechselfunktionen bleiben Unternehmens-Admins vorbehalten.
- Die maximale Zahl von fünf Mitarbeiterzugängen wird unter Einbeziehung aktiver und gesperrter Zugänge sowie gültiger offener Einladungen transaktionsgeschützt je Unternehmen geprüft. Mindestens ein aktiver Unternehmens-Admin bleibt geschützt.
- Der gezielte interne Abruf von Vertragsnachweisen erfordert eine entsprechende Systemadministrationsberechtigung und die vollständige Buchungsnummer; er wird protokolliert. Terminkunden können notwendige Nachweise und Erklärungsfunktionen über einen an die Buchung gebundenen, 30 Minuten gültigen Zugang nach erfolgreicher E-Mail-Codeprüfung erreichen.
- Laufende Anwendung und Datenbankmigrationen verwenden getrennte Rollen. Die Anwendungsrolle besitzt keine Superuser-, Rollenverwaltungs- oder Datenbankerstellungsrechte. Die höher privilegierte Migrationsrolle wird nicht von der laufenden Anwendung verwendet.

4. Übertragungs- und Systemschutz

- Transportverschlüsselung über TLS, HSTS und Sicherheitsheader schützt den öffentlichen Zugang. Firewall und Reverse-Proxy begrenzen den öffentlichen Zugriff auf die dafür vorgesehenen Dienste.
- Datenbank und interne Dienste sind nicht unmittelbar öffentlich erreichbar.
- Frontend und API laufen als nicht privilegierter Benutzer in schreibgeschützten Containern mit entfernten Linux-Capabilities und deaktivierter Rechteausweitung.
- Zugangsdaten und Schlüssel werden getrennt vom ausgelieferten Programmcode verwaltet. Dateisystemberechtigungen beschränken den Zugriff auf den berechtigten Serverbenutzer und die notwendige Systemadministration.

5. Eingabe-, Weitergabe- und Integritätskontrolle

- Serverseitige Eingabe-, Herkunfts-, Dateityp-, Größen- und Berechtigungsprüfungen; parametrisierte Datenbankabfragen und begrenzte Anfragegrößen.
- Transaktionen, Eindeutigkeits- und Konfliktprüfungen schützen zentrale Reservierungs- und Terminänderungen.
- Einladungen, Annahmen, erneute Versendungen, Widerrufe, Sperrungen, Reaktivierungen und Entfernungen von Mitarbeiterzugängen sowie relevante Terminänderungen werden nachvollziehbar protokolliert.
- Profilbilder werden validiert und neu codiert; Stripe-Webhooks werden signaturgeprüft und idempotent verarbeitet.

6. Verfügbarkeit und Wiederherstellung

- Zustandsprüfungen und strukturierte Fehlerprotokolle unterstützen die Störungserkennung.
- Technische Überwachung erfasst den Zustand von Anwendung, Datenbank, Monitoring-Gateway und Backups. Erkannte Störungen werden über die eingerichteten Alarmwege gemeldet.
- Tägliche verschlüsselte Datenbank- und Konfigurationssicherungen werden an eine getrennte Hetzner Storage Box übertragen. Für ihre Bereinigung gelten die reguläre 30-Tage-Frist, der tägliche Bereinigungslauf und die vorstehend geregelten begrenzten Störungsausnahmen.
- Prüfsummen und kryptografische Signaturen schützen die Integrität der Sicherungen. Wiederherstellungstests erfolgen isoliert vom Produktivbetrieb.

7. Trennung, Datenminimierung und Löschung

- Fachliche Daten werden mandantenbezogen getrennt. Der reguläre Unternehmensdatenexport erfordert eine erneute Passwortbestätigung und enthält keine Passworthashes, Sitzungen, Sicherheitstoken oder fremden Mandantendaten. Die heruntergeladene ZIP-Datei ist selbst nicht passwortverschlüsselt; das Unternehmen schützt sie bei Speicherung und Weitergabe vor unberechtigtem Zugriff.
- Mitarbeiter erhalten in Übersicht, Kalender und Anfragen nur die für den laufenden Terminbetrieb erforderlichen Kunden-, Leistungs-, Ressourcen-, Verfügbarkeits- und Termindaten. Persönliche Kalenderbreiten, Stundenhöhen und Ressourcenspalten-Reihenfolgen sind dem jeweiligen Konto zugeordnet und ändern weder Unternehmensressourcen noch Ansichten anderer Nutzer.
- Die persönliche Terminansicht erhält nur die für die jeweilige Funktion erforderlichen Daten. Name und E-Mail-Adresse des Terminkunden werden nicht mit der allgemeinen Terminansicht an den Browser übermittelt; soweit eine ausdrücklich ausgelöste Funktion diese Daten benötigt, werden sie serverseitig nur für diesen Vorgang verwendet.
- Operative Daten werden nach den Fristen und Zweckgrenzen aus Anlage 1 entfernt. Erforderliche Belege und der Zugang für Terminkunden werden getrennt aufbewahrt; pseudonymisierte Kennungen und Restbelege gelten weiterhin als personenbezogen.
- Historische Originalprüfwerte und aktuelle Prüfwerte minimierter Nachweise werden getrennt geführt. Ein historischer Hash wird nicht als Beleg dafür dargestellt, dass die gelöschte vollständige Kopie weiterhin technisch verifiziert werden könne.
- Bei einer Unternehmenslöschung werden operative Unternehmensdaten und Mitgliedschaften entfernt, sobald die in Anlage 1 genannten laufenden Zwecke und Fälle dies erlauben. Andere Unternehmensmitgliedschaften desselben persönlichen Zugangs bleiben erhalten. Profil- und Ressourcenbilder werden mit ihren aktiven Datensätzen entfernt; erforderliche Fallnachweise werden gesondert geprüft.
- Restbelege ermöglichen keinen Zugriff auf das gelöschte operative Profil. Ihre zweckgebundenen Kontakt- und Vertragsdaten werden nur bis zum Ende der jeweiligen Nachweis- und Zugangszwecke geführt; danach werden sie tatsächlich gelöscht.
- Ein täglicher Bereinigungsprozess arbeitet die fälligen Daten nach ihren Zwecken ab. Wiederholte Läufe, Transaktionen, Zähler, Fehlerstatus und die Anzeige überfälliger Sperrprüfungen unterstützen die kontrollierte Ausführung.
- Einzelne versehentlich übermittelte Freitextwerte können feldgenau redigiert werden. Der Änderungsverlauf speichert keinen entfernten Inhalt. Wiederhergestellte Sicherungen bleiben bis zum Abgleich zwischenzeitlicher Löschungen, Redaktionen und Berechtigungsänderungen vom Anwendungszugriff gesperrt; eine automatische Teilwiederanwendung ersetzt die Freigabeprüfung nicht.
- Die installierbare Web-App speichert keine Termin- oder Kundendaten für eine Offline-Nutzung.

8. Überprüfung und Vorfallbehandlung

- Automatisierte Tests, Abhängigkeits- und Konfigurationsprüfungen begleiten Änderungen an sicherheitsrelevanten Funktionen.
- Technische Protokollierung und geregelte Abläufe zur Vorfallbehandlung unterstützen Erkennung, Eingrenzung, Behebung, Nachbereitung und die erforderlichen Benachrichtigungen.
- Naluvio überprüft die Wirksamkeit der technischen und organisatorischen Maßnahmen regelmäßig in risikogerechten Abständen sowie anlassbezogen bei wesentlichen Änderungen, Sicherheitsvorfällen oder erheblichen neuen Risiken. Erforderliche Folgemaßnahmen werden umgesetzt.
- Wiederherstellungstests erfolgen regelmäßig in risikogerechten Abständen und bei wesentlichen Änderungen des Sicherungs- oder Wiederherstellungsverfahrens. Durchführung und Ergebnisse werden nachvollziehbar festgehalten.

Anlage 3

Unterauftragsverarbeiter

Diese Anlage beschreibt die für die jeweiligen Funktionen eingesetzten Anbieter, ihre Rollen und die maßgeblichen Verarbeitungs- und Transferbedingungen. Für Geoapify ist die nachfolgend beschriebene vertragliche Einbindung vor produktivem Einsatz mit personenbezogenen Auftragsdaten sicherzustellen. Änderungen richten sich nach Ziffer 9; die Zulässigkeit der Verarbeitung und etwaiger Drittlandübermittlungen bleibt zu gewährleisten.

1. Hetzner Online GmbH

Industriestr. 25, 91710 Gunzenhausen, Deutschland. Zweck: Cloud-Hosting, Rechenleistung, Netzwerk, Datenbankbetrieb und verschlüsselte Offsite-Sicherungen auf einer Hetzner Storage Box. Produktivserverregion: Nürnberg, Deutschland. Betroffene Daten: Plattformdaten aus Anlage 1 sowie verschlüsselte Sicherungskopien.

Der Vertrag zur Auftragsverarbeitung, die Produktivserverregion und die aktuellen Anbieter-Unterauftragsverarbeiter wurden betrieblich geprüft. Vertragsnachweise werden außerhalb des Repositorys aufbewahrt.

2. Plus Five Five, Inc. (Resend)

2261 Market Street #5039, San Francisco, CA 94114, USA. Zweck: Versand transaktionaler E-Mails. Betroffene Daten: Empfängeradresse, Absender- und Zustellinformationen sowie erforderliche Reservierungs-, Verifizierungs- oder Statusinhalte. Nachrichten und Versanddaten werden in den USA gespeichert; eine europäische Versandregion ändert diesen Speicherort nicht. Für die konkrete Übermittlung gilt Ziffer 10.

DPA, dokumentierte Transfergrundlage und aktuelle Unterauftragnehmer wurden betrieblich geprüft. Der konkrete Vertrags- und Transfernachweis wird außerhalb des Repositorys aufbewahrt. Anbieter-Liste: https://resend.com/legal/subprocessors.

3. Cloudflare, Inc.

101 Townsend Street, San Francisco, CA 94107, USA. Zweck: Cloudflare Turnstile zur Erkennung automatisierter und missbräuchlicher Zugriffe. Betroffene Daten: insbesondere IP-Adresse, Verbindungs- und Browsermerkmale, TLS-Signale, User-Agent, Sitekey, Ursprung und Prüfergebnis. Möglicher Drittlandbezug: globale Infrastruktur und USA.

Soweit Cloudflare Turnstile-Daten im Auftrag verarbeitet, ist Cloudflare Unterauftragsverarbeiter. Soweit Cloudflare Daten nach eigenen Bedingungen für eigene Sicherheits- oder Verbesserungszwecke verarbeitet, handelt Cloudflare dafür eigenständig verantwortlich.

Datenverarbeitungsbedingungen, Turnstile-Einordnung, Rollenabgrenzung, dokumentierte Transfergrundlage und aktuelle Unterauftragnehmer wurden betrieblich geprüft. Die Nachweise werden außerhalb des Repositorys aufbewahrt.

4. KEPTAGO LTD (Geoapify)

N. Nikolaidi & T. Kolokotroni, ONISIFOROU CENTER, 2. Stock, 8011 Paphos, Zypern. Zweck: optionale Geocodierung der Unternehmensadresse und Erstellung eines Standortkartenbildes auf Weisung des Unternehmens. Übermittelte Daten: Straße, Hausnummer, Postleitzahl und Ort beziehungsweise daraus ermittelte Koordinaten sowie die öffentliche Ausgangs-IP und erforderliche technische Anfragedaten des Temivaro-Servers. Keine Übermittlung von Kunden- oder Reservierungsdaten, Besucher-IP-Adressen, Besucher-Cookies oder Browser-Headern.

Das Bild wird bei Temivaro gespeichert; Buchungsseitenbesucher rufen es ausschließlich von Temivaro ab. Geoapify nennt Hetzner-Rechenzentren in Deutschland und Finnland und für die eingesetzten Standardendpunkte Cloudflare als Netzwerkdienstleister. Dadurch sind Verarbeitungen außerhalb des EWR, insbesondere in den USA, möglich; Ziffer 10 gilt. Geoapify ist für diese Funktion nur im Umfang personenbezogener Standort- und Anfragedaten Unterauftragsverarbeiter.

Geoapify veröffentlicht Datenverarbeitungsbedingungen einschließlich der Anbieter-Unterauftragnehmer. Danach werden detaillierte personenbezogene Anfragedaten im Regelfall höchstens 24 Stunden, in Ausnahmefällen wie Betrugsverdacht bis zu zwei Monate gespeichert. Vor dem produktiven Einsatz mit personenbezogenen Auftragsdaten stellt Naluvio die verbindliche Einbeziehung dieser Bedingungen für das verwendete Unternehmenskonto und die Nutzung als Unterauftragsverarbeitung sowie die für die gewählten Endpunkte erforderlichen Transfergarantien sicher und dokumentiert sie. Die Veröffentlichung der Bedingungen und ein funktionierender API-Zugang allein werden nicht als Nachweis dieser Einbeziehung behandelt.

Nicht als Unterauftragsverarbeiter für Reservierungsdaten geführt

Stripe: Stripe wird ausschließlich für das Abonnement und die Abrechnung von Temivaro for Business eingesetzt. Stripe erhält nach dem implementierten Datenfluss keine fachlichen Kunden- oder Reservierungsdaten aus Anlage 1. Stripe verarbeitet Unternehmens-, Kontakt-, Zahlungs- und Rechnungsdaten nach den hierfür geltenden Bedingungen und Datenschutzhinweisen.