phexnet
UG (haftungsbeschränkt)

PHEXNET UG · AVV · MUSTER

Vertrag zur Auftragsverarbeitung

Vertrag nach Art. 28 DSGVO

01 VERTRAGSPARTEIEN

Dieser Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO wird geschlossen zwischen

Muster GmbH, Musterstraße 1, 20095 Hamburg, Amtsgericht Hamburg, HRB 000000, vertreten durch die Geschäftsführerin Erika Mustermann (nachfolgend „Verantwortlicher“)

und

phexnet UG (haftungsbeschränkt), Am Pfeilshof 9A, 22393 Hamburg, Amtsgericht Hamburg, HRB 114863, vertreten durch den Geschäftsführer Dr. Felix Reher (nachfolgend „Auftragsverarbeiter“)

– gemeinsam „Parteien“ –

02 GEGENSTAND DER VERARBEITUNG

Leistungsgrundlage	die zwischen den Parteien bestehende Vereinbarung über die in diesem Vertrag genannten Leistungen
Leistungen	Webhosting (Webserver, Laufzeitumgebung, Datenbank); Mailhosting (Postfächer, Annahme, Filterung und Versand von E-Mails); Dateiaustausch (fileshare.phexnet.de)
Art der Verarbeitung	Erheben, Erfassen, Speichern, Auslesen, Abfragen, Übermitteln an den Verantwortlichen und an die von ihm bestimmten Empfänger, Sichern, Wiederherstellen, Einschränken und Löschen (Art. 4 Nr. 2 DSGVO), jeweils soweit für die vereinbarten Leistungen erforderlich.
Webhosting – Gegenstand	Betrieb des Webservers, der Laufzeitumgebung und der Datenbank für die Websites des Verantwortlichen (www.example.org).
Webhosting – Zweck	Bereitstellung und Absicherung der Websites, Entgegennahme von Formulareingaben und ihre Weitergabe an den Verantwortlichen, Fehleranalyse und Abwehr von Angriffen.
Webhosting – Daten	Inhalte der Websites und ihrer Datenbanken, Formulareingaben, Konten der Nutzer der Websites, Zugriffs- und Fehlerprotokolle des Webservers mit IP-Adresse, Zeitpunkt, angeforderter Adresse, Statuscode, übertragener Datenmenge, Referrer und User-Agent.
Webhosting – Betroffene	Besucher der Websites, Absender von Formularen, Nutzer mit Konto, in den Inhalten genannte Personen.
Mailhosting – Gegenstand	Betrieb des Mailservers für die Domains des Verantwortlichen (example.org): Annahme, Prüfung auf Spam und Schadsoftware, Zustellung, Speicherung in Postfächern und Versand.
Mailhosting – Zweck	Bereitstellung der Postfächer und Absicherung des E-Mail-Verkehrs des Verantwortlichen.
Mailhosting – Daten	Inhalte und Anhänge der E-Mails, Kopf- und Verbindungsdaten, Zugangsdaten der Postfächer (Kennwörter nur als Argon2id-Hashwert), Zustell- und Filterprotokolle, als Spam oder Schadsoftware zurückgehaltene Nachrichten (Quarantäne).
Mailhosting – Betroffene	Inhaber der Postfächer, Absender und Empfänger von E-Mails, in E-Mails genannte Personen.
Dateiaustausch – Gegenstand	Bereitstellung der Dateifreigabe fileshare.phexnet.de für den Austausch von Dateien zwischen dem Verantwortlichen und den von ihm bestimmten Personen.
Dateiaustausch – Zweck	Übermittlung und befristete Bereitstellung von Dateien an die vom Verantwortlichen bestimmten Personen und Entgegennahme von Dateien über Upload-Links, einschließlich Prüfung auf Schadsoftware beim Eingang.
Dateiaustausch – Daten	hochgeladene Dateien und ihre Namen, Angaben zu Freigaben (Empfänger, Zeitpunkte, Gültigkeit) und zu Abrufen.
Dateiaustausch – Betroffene	Absender und Empfänger der Dateien, in den Dateien genannte Personen.
Sicherung	Kopien der genannten Daten in den täglichen, verschlüsselten Sicherungen der Server auf Speicherplatz des Rechenzentrumsbetreibers in Falkenstein (Deutschland) (Anlage 1).

Kommunikation – Zweck	Bearbeitung von Supportanfragen, Entgegennahme von Weisungen und Abgabe von Meldungen per E-Mail; personenbezogene Daten, die der Verantwortliche dabei mitteilt, gelangen in die Postfächer des Auftragsverarbeiters (Anlage 2).
Kommunikation – Betroffene	Ansprechpartner und Beschäftigte des Verantwortlichen sowie Personen, die in Anfragen, Weisungen oder Meldungen genannt sind.
Besondere Kategorien	Nicht vorgesehen. Solche Daten werden nur verarbeitet, soweit der Verantwortliche, seine Nutzer oder Dritte sie in Inhalte, Nachrichten oder Dateien einbringen.
Garantien für besondere Kategorien	Werden besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO) oder Daten über Straftaten (Art. 10 DSGVO) verarbeitet, greifen nur Administratoren des Auftragsverarbeiters im Rahmen dokumentierter Weisungen darauf zu, die Inhalte werden nicht ausgewertet und nur in den Systemen der vereinbarten Leistungen verarbeitet; weitergehende Beschränkungen oder Garantien vereinbaren die Parteien in Textform (Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/915, Klausel 7.5).
Ort der Verarbeitung	Server des Auftragsverarbeiters in den Rechenzentren Falkenstein (Deutschland) und Helsinki (Finnland) des in Anlage 2 genannten Rechenzentrumsbetreibers; eine Verarbeitung außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums findet nur nach § 5 Abs. 5 statt.

03 VEREINBARUNGEN

§ 1 Dauer und Kündigung

(1) Dieser Vertrag gilt ab der Unterzeichnung durch beide Parteien und für die Dauer der Leistungsgrundlage.

(2) Er endet mit der Leistungsgrundlage, ohne dass es einer gesonderten Kündigung bedarf. Das Recht beider Parteien zur Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt für den Verantwortlichen insbesondere vor, wenn der Auftragsverarbeiter schwerwiegend gegen diesen Vertrag oder gegen die DSGVO verstößt, eine rechtmäßige Weisung nicht ausführt oder Kontrollen nach § 9 verweigert.

(3) Verstößt der Auftragsverarbeiter gegen diesen Vertrag oder die DSGVO, kann der Verantwortliche ihn anweisen, die Verarbeitung bis zur Abhilfe auszusetzen. Wird die Abhilfe nicht innerhalb angemessener Frist geschaffen, kann der Verantwortliche den Vertrag und die betroffenen Leistungen fristlos kündigen.

(4) Die Pflichten aus diesem Vertrag gelten fort, bis alle Daten nach § 8 gelöscht oder zurückgegeben sind.

§ 2 Weisungen

(1) Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf die Übermittlung in ein Drittland oder an eine internationale Organisation, sofern er nicht durch das Recht der Union oder eines Mitgliedstaats, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist; in diesem Fall teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO).

(2) Dieser Vertrag mit seinen Anlagen, die Leistungsgrundlage und die vom Verantwortlichen veranlasste Konfiguration der Leistungen enthalten die Weisungen. Die in Anlage 1 genannten Löschfristen sind Weisungen. Weitere Weisungen erteilt der Verantwortliche in Textform; mündliche Weisungen bestätigt er unverzüglich in Textform. Der Auftragsverarbeiter bewahrt Weisungen für die Dauer dieses Vertrags auf.

(3) Weisungsberechtigt beim Verantwortlichen: Erika Mustermann, Geschäftsführerin, erika.mustermann@example.org

(4) Weisungen nimmt beim Auftragsverarbeiter entgegen: Dr. Felix Reher, Geschäftsführer, info@phexnet.de

(5) Der Auftragsverarbeiter verarbeitet die Daten nicht für eigene Zwecke und nicht für andere Auftraggeber.

(6) Verlangt eine Behörde oder ein Gericht die Herausgabe von Daten des Verantwortlichen, unterrichtet der Auftragsverarbeiter den Verantwortlichen unverzüglich, soweit das rechtlich zulässig ist, prüft die Rechtmäßigkeit des Verlangens und gibt Daten nur heraus, soweit er rechtlich dazu verpflichtet ist; Ersuchen aus Drittländern erfüllt er nur nach Art. 48 DSGVO.

(7) Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt, teilt er das dem Verantwortlichen unverzüglich mit (Art. 28 Abs. 3 Satz 3 DSGVO). Er darf die Ausführung aussetzen, bis der Verantwortliche die Weisung bestätigt oder ändert.

§ 3

Vertraulichkeit

(1) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Die Pflicht besteht nach Ende der Tätigkeit und nach Ende dieses Vertrags fort.

(2) Er stellt sicher, dass ihm unterstellte Personen, die Zugang zu den Daten haben, diese nur auf Weisung des Verantwortlichen verarbeiten (Art. 29, Art. 32 Abs. 4 DSGVO). Zugang zu den Daten haben nur Personen, die mit Betrieb und Verwaltung der Server und Dienste betraut sind; der Auftragsverarbeiter nennt sie dem Verantwortlichen auf Verlangen.

(3) Die beim Mailhosting eingesetzten Personen sind auf das Fernmeldegeheimnis verpflichtet (§ 3 TDDDG); Inhalte und nähere Umstände der Kommunikation nehmen sie nur zur Kenntnis, soweit es für den Betrieb und die Absicherung des Dienstes erforderlich ist (§ 206 StGB).

§ 4

Sicherheit der Verarbeitung

(1) Der Auftragsverarbeiter trifft die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen (Art. 28 Abs. 3 lit. c, Art. 32 DSGVO).

(2) Er darf die Maßnahmen dem Stand der Technik anpassen, wenn das Schutzniveau nicht sinkt. Wesentliche Änderungen dokumentiert er und teilt sie dem Verantwortlichen in Textform mit.

§ 5

Weitere Auftragsverarbeiter

(1) Weitere Auftragsverarbeiter setzt der Auftragsverarbeiter nur nach Maßgabe von Art. 28 Abs. 2 und 4 DSGVO ein (Art. 28 Abs. 3 lit. d DSGVO).

(2) Der Verantwortliche genehmigt den Einsatz der in Anlage 2 genannten weiteren Auftragsverarbeiter.

(3) Im Übrigen erteilt der Verantwortliche eine allgemeine Genehmigung. Der Auftragsverarbeiter unterrichtet ihn mindestens 30 Tage vor dem Einsatz eines neuen oder dem Wechsel eines weiteren Auftragsverarbeiters und vor einem Wechsel des Rechenzentrums per E-Mail an die Adresse nach § 10 Abs. 4 mit Name, Sitz, Leistung und Ort der Verarbeitung. Die jeweils aktuelle Liste mit Stand veröffentlicht er unter https://vertrag.phexnet.de/unterauftragnehmer. Der Verantwortliche kann in dieser Frist Einspruch erheben (Art. 28 Abs. 2 Satz 2 DSGVO). Nach einem Einspruch unterbleibt die Änderung; ist die Leistung ohne sie nicht möglich, kann jede Partei die betroffene Leistung und diesen Vertrag mit einer Frist von 30 Tagen kündigen.

(4) Der Auftragsverarbeiter erlegt jedem weiteren Auftragsverarbeiter durch Vertrag dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen. Kommt der weitere Auftragsverarbeiter seinen Pflichten nicht nach, haftet der Auftragsverarbeiter dem Verantwortlichen dafür (Art. 28 Abs. 4 DSGVO). Die Verträge mit den weiteren Auftragsverarbeitern legt er dem Verantwortlichen auf Verlangen vor.

(5) Eine Verarbeitung außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums findet nur statt, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind; die für die genannten weiteren Auftragsverarbeiter geltenden Garantien nennt Anlage 2. Jede weitere Übermittlung in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen in Textform.

§ 6

Unterstützung des Verantwortlichen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen nach Art. 12 bis 22 DSGVO zu beantworten (Art. 28 Abs. 3 lit. e DSGVO). Dazu gehören Auskünfte aus Daten und Protokollen und deren Berichtigung, Löschung oder Einschränkung, soweit sich die Daten einer Person zuordnen lassen.

(2) Anträge betroffener Personen, die beim Auftragsverarbeiter eingehen, leitet er unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst.

(3) Er unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Art. 28 Abs. 3 lit. f DSGVO), insbesondere bei der Sicherheit der Verarbeitung, bei Meldungen und Benachrichtigungen nach Art. 33 und 34 DSGVO, bei einer Datenschutz-Folgenabschätzung und bei einer vorherigen Konsultation der Aufsichtsbehörde.

(4) Er führt ein Verzeichnis aller Kategorien von Verarbeitungen, die er im Auftrag durchführt (Art. 30 Abs. 2 DSGVO), und legt es dem Verantwortlichen auf Verlangen für diesen Auftrag vor.

§ 7

Verletzungen des Schutzes personenbezogener Daten

(1) Eine Verletzung des Schutzes personenbezogener Daten meldet der Auftragsverarbeiter dem Verantwortlichen unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis (Art. 33 Abs. 2 DSGVO). Das gilt auch für Verletzungen bei einem weiteren Auftragsverarbeiter.

(2) Die Meldung enthält die dem Auftragsverarbeiter bekannten Angaben nach Art. 33 Abs. 3 DSGVO; fehlende Angaben reicht er nach.

(3) Er trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung nachteiliger Folgen und dokumentiert die Verletzung, ihre Auswirkungen und die Abhilfemaßnahmen.

(4) Protokolldaten, die zur Aufklärung erforderlich sind, bewahrt er abweichend von den Löschfristen der Anlage 1 bis zur abschließenden Aufklärung auf und teilt das dem Verantwortlichen mit.

(5) Meldungen an die Aufsichtsbehörde und Benachrichtigungen betroffener Personen nimmt allein der Verantwortliche vor.

§ 8

Löschung und Rückgabe

(1) Während der Laufzeit löscht der Auftragsverarbeiter die Daten nach den Fristen der Anlage 1 und auf Weisung des Verantwortlichen.

(2) Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten oder gibt sie zurück und löscht die vorhandenen Kopien, sofern nicht nach dem Recht der Union oder eines Mitgliedstaats eine Pflicht zur Speicherung besteht (Art. 28 Abs. 3 lit. g DSGVO). Die Rückgabe erfolgt als Export in einem gängigen Format (zum Beispiel Dateien der Websites, Auszug der Datenbanken, Postfächer, Dateien) innerhalb von 30 Tagen nach Vertragsende; danach oder wenn der Verantwortliche keine Wahl trifft, löscht der Auftragsverarbeiter.

(3) Kopien in den Sicherungen lassen sich aus den verschlüsselten Gesamtsicherungen nicht einzeln löschen. Die Sicherungsstände werden nach dieser Rotation überschrieben: tägliche Stände 14 Tage, wöchentliche 8 Wochen, monatliche 12 Monate, jährliche 3 Jahre. Der Verantwortliche weist den Auftragsverarbeiter daher an, die Kopien nach Vertragsende nicht gezielt zu löschen, sondern mit der Rotation auslaufen zu lassen; sie sind gelöscht, sobald der letzte Stand abläuft, der sie enthält, spätestens 3 Jahre nach Vertragsende.

(4) Bis dahin sind die Kopien gesperrt: Der Auftragsverarbeiter verwendet sie für keinen Zweck und stellt sie nur auf Weisung des Verantwortlichen wieder her. Muss er einen Stand wiederherstellen, der auch Daten des Verantwortlichen enthält, löscht er diese Daten nach der Wiederherstellung unverzüglich. Die Pflichten aus diesem Vertrag gelten für die Kopien fort.

(5) Die Löschung bestätigt der Auftragsverarbeiter in Textform. Er sorgt dafür, dass auch die weiteren Auftragsverarbeiter löschen.

§ 9

Nachweise und Kontrollen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO und aus diesem Vertrag zur Verfügung, ermöglicht Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer und trägt dazu bei (Art. 28 Abs. 3 lit. h DSGVO).

(2) Überprüfungen werden mit einer Frist von mindestens 14 Tagen angekündigt, bei begründetem Verdacht auf einen Verstoß auch kurzfristig. Soweit eine Prüfung der Unterlagen, der Konfiguration oder eine Prüfung per Fernzugriff ausreicht, findet keine Prüfung vor Ort statt.

(3) Für die Rechenzentren kann der Auftragsverarbeiter den Nachweis durch aktuelle Bescheinigungen, Zertifikate oder Prüfberichte des Rechenzentrumsbetreibers führen. Das Recht des Verantwortlichen auf eigene Überprüfungen bleibt unberührt.

§ 10

Pflichten des Verantwortlichen und Ansprechpartner

(1) Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung, für die Rechtsgrundlagen, für die Information der betroffenen Personen und für die Wahrung ihrer Rechte verantwortlich (Art. 24 DSGVO).

(2) Er teilt dem Auftragsverarbeiter Änderungen, die Art, Umfang oder Zweck der Verarbeitung ändern, vorab in Textform mit; die Parteien passen diesen Vertrag und seine Anlagen an.

(3) Er unterrichtet den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

(4) Weiterleitungen nach § 6 Abs. 2 und Meldungen nach § 7 gehen an: datenschutz@example.org

(5) Datenschutzbeauftragter des Verantwortlichen: _____

(6) Der Auftragsverarbeiter hat keinen Datenschutzbeauftragten benannt. Ansprechpartner für den Datenschutz: info@phexnet.de. Zuständige Aufsichtsbehörde des Auftragsverarbeiters: Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit.

§ 11

Haftung und Vergütung

(1) Gegenüber betroffenen Personen haften die Parteien nach Art. 82 DSGVO. Der Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Verantwortlichen oder gegen diese Anweisungen gehandelt hat (Art. 82 Abs. 2 Satz 2 DSGVO). Dieser Vertrag beschränkt die Haftung gegenüber betroffenen Personen nicht.

(2) Hat eine Partei vollständigen Schadenersatz geleistet, kann sie von der anderen Partei den Teil zurückfordern, der deren Anteil an der Verantwortung für den Schaden entspricht (Art. 82 Abs. 5 DSGVO).

(3) Im Übrigen haften die Parteien einander nach der Leistungsgrundlage und den gesetzlichen Vorschriften.

(4) Unterstützungsleistungen nach §§ 6 und 9, die über die Leistungsgrundlage hinausgehen und nicht durch einen Verstoß des Auftragsverarbeiters veranlasst sind, kann der Auftragsverarbeiter nach vorheriger Ankündigung nach Aufwand berechnen. Meldungen und Unterstützung nach § 7 sind nicht gesondert zu vergüten.

§ 12

Schlussbestimmungen

(1) Dieser Vertrag wird schriftlich abgefasst; das kann in einem elektronischen Format erfolgen (Art. 28 Abs. 9 DSGVO). Eine elektronische Signatur genügt. Änderungen und Ergänzungen bedürfen der Textform.

(2) Dieser Vertrag liegt in der Fassung 2026-11-21.1 vor; die Anlagen 1 und 2 sind Bestandteil dieses Vertrags. Bei Widersprüchen geht dieser Vertrag der Leistungsgrundlage in Fragen des Datenschutzes vor.

(3) Beide Parteien bewahren diesen Vertrag bis zum Ende des dritten Kalenderjahres nach seiner Beendigung auf (Nachweis nach Art. 5 Abs. 2, Art. 28 DSGVO).

(4) Ist eine Bestimmung dieses Vertrags unwirksam, bleibt der Vertrag im Übrigen wirksam. An die Stelle der unwirksamen Bestimmung tritt das Gesetz.

(5) Es gilt deutsches Recht. Gerichtsstand ist Hamburg, soweit eine Gerichtsstandsvereinbarung zulässig ist (§ 38 ZPO).

04 UNTERSCHRIFTEN

Verantwortlicher	Muster GmbH
Unterzeichnet von	Erika Mustermann, Geschäftsführerin
Ort, Datum	
Auftragsverarbeiter	phexnet UG (haftungsbeschränkt)
Unterzeichnet von	Dr. Felix Reher, Geschäftsführer
Ort, Datum	

05 ANLAGE 1 – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

	Die Maßnahmen gelten für alle Leistungen dieses Vertrags (Art. 32 DSGVO). Stand der Angaben: 18.11.2026; die Werte sind auf den Servern des Auftragsverarbeiters gemessen.
Ort der Verarbeitung	Server in den Rechenzentren Falkenstein (Deutschland) und Helsinki (Finnland) des in Anlage 2 genannten Rechenzentrumsbetreibers.
Zutritt	Die Server stehen in den Rechenzentren des Rechenzentrumsbetreibers. Für den Zutritt gelten dessen technische und organisatorische Maßnahmen aus dem Vertrag nach § 5 Abs. 4.
Zugang	Administrativer Zugang zu den Servern besteht von außen nur über einen zentralen Verwaltungszugang mit Anmeldung; Anmeldungen an Servern nur mit SSH-Schlüssel. Verwaltungsanwendungen sind nur nach Anmeldung über den zentralen Anmeldedienst mit Kennwort und zweitem Faktor erreichbar, und nur für Konten mit Freigabe des jeweiligen Dienstes. Anmeldungen der Administratoren werden protokolliert.
Zugriff	Jede Anwendung hat eigene Datenbankkonten mit den für sie erforderlichen Rechten. Zugangsdateien liegen außerhalb der Webverzeichnisse und sind nur für den Systemverwalter und den jeweiligen Dienst lesbar.
Trennung	Websites laufen in eigenen virtuellen Hosts mit eigenen Webverzeichnissen und Datenbanken, Anwendungsinstanzen getrennt je Kunde; Daten verschiedener Auftraggeber werden nicht zusammengeführt.
Weitergabe	Die Dienste werden über TLS ausgeliefert. Die TLS-Verbindung endet auf dem Reverse-Proxy des Auftragsverarbeiters in Falkenstein (Deutschland); von dort werden die Anfragen an die Anwendungsserver in Helsinki (Finnland) weitergeleitet, also zwischen zwei Rechenzentren. Eine zusätzliche Transportverschlüsselung dieser Weiterleitung sagt der Auftragsverarbeiter nicht zu. Sicherungen werden verschlüsselt übertragen.
Pseudonymisierung	Eine Pseudonymisierung durch den Auftragsverarbeiter ist nicht vorgesehen; Inhalt und Form der Daten bestimmt der Verantwortliche mit der Nutzung der Leistungen.
Datenträger	Die Datenträger der Server sind nicht verschlüsselt. Verschlüsselt gespeichert sind die Sicherungen sowie Daten, die eine Anwendung selbst verschlüsselt.
Schlüsselverwaltung	Die Schlüssel der Sicherungen (Repository-Schlüssel und Passphrase) erzeugt und verwahrt der Auftragsverarbeiter selbst auf dem Server, der die Sicherung schreibt, nur für den Systemverwalter lesbar; der Rechenzentrumsbetreiber erhält Sicherungen und Kopien dieser Schlüssel nur verschlüsselt. Schlüssel, mit denen eine Anwendung Daten selbst verschlüsselt, verwahrt der Auftragsverarbeiter getrennt von diesen Daten, je Instanz mit Kennung; ältere Schlüssel bleiben aufbewahrt, solange Sicherungen mit ihnen bestehen.
Verfügbarkeit	Tägliche Sicherung aller Server, verschlüsselt (Borg) auf Speicherplatz des Rechenzentrumsbetreibers (Storage Box) im Rechenzentrum Falkenstein (Deutschland); Aufbewahrung der Stände: tägliche Stände 14 Tage, wöchentliche 8 Wochen, monatliche 12 Monate, jährliche 3 Jahre; nach Vertragsende sind die Kopien des Verantwortlichen bis zum Ablauf gesperrt (§ 8). Verfügbarkeit und Auslastung der Server und Dienste werden überwacht.
Belastbarkeit und Wiederherstellung	Die Leistungen laufen auf einzelnen Servern ohne automatische Umschaltung auf einen zweiten Server; Hochverfügbarkeit ist nicht Bestandteil der Leistungen. Nach einem Ausfall stellt der Auftragsverarbeiter aus der letzten täglichen Sicherung wieder her. Ein dokumentierter Wiederherstellungstest in isolierter Umgebung und eine zugesicherte Wiederherstellungszeit liegen noch nicht vor; der Auftragsverarbeiter führt den Test mindestens jährlich durch und teilt Ergebnis und gemessene Dauer auf Verlangen mit.
Schutz gegen Schadsoftware	Eingehende E-Mails werden auf Spam und Schadsoftware geprüft, Dateien der Dateifreigabe beim Eingang; die Server erhalten automatische Sicherheitsaktualisierungen.
Sicherheitsupdates	Sicherheitsaktualisierungen werden automatisch eingespielt; ein Sicherheitsupdate, das länger als 7 Tage offen ist, löst einen Alarm aus.
E-Mail-Transport	Einlieferung durch Nutzer nur verschlüsselt (Submission mit erzwungenem TLS, SMTPS); Abruf der Postfächer (IMAP, POP3) nur verschlüsselt; zwischen Mailservern wird TLS verwendet, wenn die Gegenstelle es anbietet; MTA-STS und TLS-Berichte sind je Domain einschaltbar.
Eingabekontrolle	Zugriffe und Änderungen sind über die Protokolle der Webserver, des Mailservers, des Systemjournals und das Anmeldeprotokoll der Administratoren nachvollziehbar.
Löschfristen	Zugriffs- und Fehlerprotokolle der Webserver 14 Tage; Sperrprotokolle (fail2ban) 4 Wochen; Protokolle des Mailservers 4 Wochen; Systemjournal der Server 30 Tage; Anmeldeprotokoll der Administratoren 365 Tage; Sicherungen nach der Rotation unter „Verfügbarkeit“, höchstens 3 Jahre. Inhalte der Leistungen (Websites, Postfächer, Dateien, Anwendungsdaten) bleiben bis zur Löschung durch den Verantwortlichen oder auf seine Weisung und nach § 8.

Personal	Personen mit Zugang sind vor Aufnahme der Tätigkeit auf Vertraulichkeit verpflichtet (§ 3) und über den Datenschutz unterrichtet; Zugänge erhalten sie nur im erforderlichen Umfang, beim Ausscheiden oder Aufgabenwechsel werden sie unverzüglich entzogen.
Vorfälle	Sicherheitsvorfälle werden über die Überwachung oder Meldungen erkannt, bewertet, behoben und mit Ursache, Auswirkung und Abhilfe dokumentiert; Verletzungen des Schutzes personenbezogener Daten meldet der Auftragsverarbeiter nach § 7.
Datenträgervernichtung	Ausgesonderte Datenträger der Server löscht oder vernichtet der Rechenzentrumsbetreiber nach seinen technischen und organisatorischen Maßnahmen (Vertrag nach § 5 Abs. 4).
Auftragskontrolle	Verarbeitung nur nach dokumentierter Weisung nach § 2; weitere Auftragsverarbeiter nur nach § 5 und mit Vertrag nach Art. 28 Abs. 4 DSGVO.
Überprüfung	Der Auftragsverarbeiter überprüft diese Maßnahmen mindestens jährlich und bei wesentlichen Änderungen, dokumentiert das Ergebnis und legt es auf Verlangen vor (Art. 32 Abs. 1 lit. d DSGVO).

06 ANLAGE 2 – WEITERE AUFTRAGSVERARBEITER

	Der Verantwortliche genehmigt den Einsatz der folgenden weiteren Auftragsverarbeiter (§ 5 Abs. 2). Stand der Liste: 21.11.2026; die jeweils aktuelle Fassung steht unter https://vertrag.phexnet.de/unterauftragnehmer.
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Deutschland; Kontakt: Datenschutzbeauftragter der Hetzner Online GmbH unter der genannten Anschrift. Leistung: Server im Rechenzentrum und Speicherplatz für die Sicherungen (Storage Box). Ort der Verarbeitung: Rechenzentren Falkenstein (Deutschland) und Helsinki (Finnland); Speicherplatz für die Sicherungen (Storage Box) in Falkenstein (Deutschland); nach dem Vertrag mit Hetzner Verarbeitung ausschließlich in der Europäischen Union bzw. im EWR. Vertrag nach Art. 28 Abs. 4 DSGVO vom 19.11.2026.
Nanosystems S.r.l.	Via del Commercio, 76/A, 63100 Ascoli Piceno (AP), Italien; Kontakt: Nanosystems S.r.l. unter der genannten Anschrift. Leistung: Vermittlung der Verbindung bei der Fernwartung über das Support-Tool (Supremo); die Sitzungen werden nicht aufgezeichnet. Ort der Verarbeitung: Server in der Europäischen Union; Sitz und Verarbeitung in der Europäischen Union.
Microsoft Ireland Operations Limited	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland; Kontakt: Datenschutzbeauftragter von Microsoft in der EU über https://aka.ms/privacyresponse. Leistung: E-Mail-Postfächer und Bürokommunikation des Auftragsverarbeiters (Microsoft 365), ausschließlich für die Kommunikation mit dem Verantwortlichen (Supportanfragen, Weisungen, Meldungen). Ort der Verarbeitung: Rechenzentren in der Europäischen Union (EU-Datengrenze); ein Zugriff aus Drittländern, insbesondere durch die Microsoft Corporation (USA), ist im Ausnahmefall möglich und durch die Zertifizierung nach dem EU-US Data Privacy Framework (Art. 45 DSGVO) sowie durch Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) im Datenschutznachtrag von Microsoft abgesichert. Vertrag nach Art. 28 Abs. 4 DSGVO: Microsoft Products and Services Data Protection Addendum, Fassung gemäß Product Terms, Stand bei Vertragsschluss.