Version 1.4 vom 15. Oktober 2025

Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU-Datenschutz-Grundverordnung (AV-Vertrag)

Zwischen dem/der

.....

- Verantwortlicher - nachstehend Auftraggeber genannt -

und

1undbesser Inh. Patrick Dürr

Bachstr. 15

75053 Gondelsheim

.....

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

Inhalt

Präambel ... 3
§ 1 Gegenstand des Auftrags ... 3
§ 2 Anwendungsbereich ... 3
§ 3 Dauer des Auftrags ... 3
§ 5 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers ... 4
§ 6 Pflichten des Auftragnehmers ... 4
§ 7 Mitteilungspflichten und Unterstützung des Auftragnehmers bei Datenschutzvorfällen und der Einhaltung der Art. 32–36 DSGVO ... 6
§ 8 Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO) ... 7
§ 9 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO) ... 7
§ 10 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags (Art. 28 Abs. 3 Satz 2 lit. g DSGVO) ... 8
§ 11 Haftung ... 8
§ 12 Sonstiges ... 9
Anlage 1 ... 10
Gegenstand des Auftrags ... 10
1. Gegenstand, Art und Zweck der Verarbeitung ... 10
2. Art(en) der personenbezogenen Daten ... 10
3. Kategorien betroffener Personen ... 10
Anlage 2 ... 11
Subunternehmer ... 11
Anlage 3 ... 13
Technische und organisatorische Maßnahmen ... 13
1. Pseudonymisierung und Datenminimierung (Art. 32 Abs. 1 it. a ... 13
DSGVO, Art. 25 Abs. 1 DSGVO) ... 13
2. Vertraulichkeit (Art. 32. Abs. Mit. b DSGVO) ... 13
3. Integrität (Art. 32. Abs. llit. b DSGVO) ... 14
4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO) ... 14

Präambel

Dieser Vertrag über die Auftragsverarbeitung ergänzt und konkretisiert die datenschutzrechtlichen Verpflichtungen, die aus den zwischen den Vertragsparteien geschlossenen Individualverträgen resultieren und gilt für alle zwischen den Parteien über die in Anlage 1 genannten Dienstleistungen bestehenden oder künftig geschlossenen Individualverträge. Der Abschluss mindestens eines solchen Individualvertrags ist zwingende Voraussetzung für das rechtlich bindende Zustandekommen dieses Vertrags.

§ 1 Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in Anlage 1 zu diesem Vertrag festgelegt. Die Dauer der Auftragsverarbeitung richtet sich nach der Laufzeit der jeweiligen Individualverträge.

§ 2 Anwendungsbereich

1. Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 DSGVO und Art. 28 DSGVO auf Grundlage dieses Vertrages.
2. Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht.
3. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 3 Dauer des Auftrags

1. Der Vertrag über die Auftragsverarbeitung beginnt mit Abschluss dieses Vertrages und dauert an, solange mindestens ein Individualvertrag mit dem Auftraggeber besteht und endet sodann 14 Tage nach der wirksamen Beendigung dieses letzten Individualvertrags.
2. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 5 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Der Auftragnehmer wird den Auftraggeber nach Maßgabe des § 6 Nr. 5 dieses Vertrags unterstützen.
2. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
3. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
4. Der Auftraggeber kann die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen sowie der vertraglichen Pflichten auf Basis der vom Auftragnehmer bereitgestellten Dokumentation in angemessenem Umfang prüfen.
5. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
6. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Die Verpflichtung dazu bleibt auch nach Beendigung dieses Vertrages bestehen.

§ 6 Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen zur Durchführung des Vertrags und nach dokumentierten Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragnehmer 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 Satz 2 lit. a DSGVO). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.
2. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.
3. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
4. Der Auftragnehmer stellt sicher, dass die vereinbarten Maßnahmen umgesetzt werden und dokumentiert dies in geeigneter Form.
5. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach

gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

6. Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt.
7. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.
8. Der Auftragnehmer dokumentiert alle getroffenen technischen und organisatorischen Maßnahmen (TOMs) gemäß Art. 28 DSGVO und stellt diese Dokumentation dem Auftraggeber auf Anfrage zur Verfügung.
   Kontrollen oder Prüfungen durch den Auftraggeber oder Dritte werden ausgeschlossen. Der Auftragnehmer erfüllt die Nachweispflicht ausschließlich durch Bereitstellung der entsprechenden Dokumentation.
9. Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind.
10. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.
11. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit
    ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

§ 7 Mitteilungspflichten und Unterstützung des Auftragnehmers bei Datenschutzvorfällen und der Einhaltung der Art. 32–36 DSGVO

1. Der Auftragnehmer teilt dem Auftraggeber unverzüglich alle Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt insbesondere im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Meldungen nach Art. 33 oder Art. 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gemäß § 5 dieses Vertrages durchführen.
2. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Einhaltung der in den Art. 32 bis 36 DSGVO geregelten Pflichten. Dies umfasst insbesondere:
   a) die Bereitstellung von Informationen und Nachweisen zur Sicherheit der Verarbeitung gemäß Art. 32 DSGVO,
   b) die Unterstützung bei der Erfüllung von Meldepflichten gegenüber der Aufsichtsbehörde nach Art. 33 DSGVO sowie von Benachrichtigungspflichten gegenüber betroffenen Personen nach Art. 34 DSGVO,
   c) die Mitwirkung bei Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO und
   d) die Unterstützung bei vorherigen Konsultationen mit der Aufsichtsbehörde nach Art. 36 DSGVO.
3. Die Unterstützung erfolgt im erforderlichen und angemessenen Umfang und soweit sie durch den Auftragnehmer mit vertretbarem Aufwand möglich ist. Soweit die Unterstützung über die Erfüllung der in diesem Vertrag geregelten Hauptleistungspflichten hinausgeht, kann der Auftragnehmer hierfür eine Vergütung verlangen.

§ 8 Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

1. Der Auftragnehmer besitzt die allgemeine Genehmigung des Auftraggebers für die Beauftragung von Unterauftragsverarbeitern nach Maßgabe dieses § 8. Der Auftragnehmer muss dafür Sorge tragen, dass er die Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur dann erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
2. Der Auftragnehmer hat dem Subunternehmer vertraglich im Wesentlichen dieselben Datenschutzpflichten aufzuerlegen, die in diesem Vertrag für den Auftragnehmer festgelegt sind. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Der Auftraggeber kann die Einhaltung der Pflichten der Subunternehmer auf Basis von Dokumentationen überprüfen. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).
3. Zurzeit sind für den Auftragnehmer die in Anlage 2 mit Namen, Rechtsform, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und werden vom Auftraggeber genehmigt. Als weitere genehmigte Subunternehmer nach diesem Vertrag gelten alle verbundenen Unternehmen des Auftragnehmers im Sinne des AktG. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden und genehmigt diese. Sie sind in der in Anlage 2 beigefügten Liste aufgeführt.
4. Der Auftragnehmer informiert den Auftraggeber mindestens 14 Tage vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Subunternehmern. Der Auftraggeber kann innerhalb von 7 Tagen nach Zugang der Information aus wichtigem Grund widersprechen. Erfolgt ein solcher Widerspruch, bemühen sich die Parteien um eine einvernehmliche Lösung. Kommt eine solche nicht zustande, steht dem Auftraggeber ein außerordentliches Kündigungsrecht zu.

§ 9 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

1. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.
2. Die angewandten Methoden zur Risikobewertung und Überwachung werden permanent aktualisiert und auf den aktuellen Stand der Technik überprüft

3. Die in Anlage 3 beschriebenen TOM stellen die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.
4. Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DSGVO).
5. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.
6. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren. Wesentliche Änderungen im Sinne dieser Regelung sind solche, die das vereinbarte Schutzniveau beeinträchtigen können.

§ 10 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags (Art. 28 Abs. 3 Satz 2 lit. g DSGVO)

1. Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zurückzugeben oder zu löschen. Eine gleichzeitige Verpflichtung zur Rückgabe und Löschung besteht nicht.
2. Der Auftragnehmer hat alle vorhandenen Kopien der personenbezogenen Daten in Übereinstimmung mit der Entscheidung des Auftraggebers zu löschen.

3. Etwaige gesetzliche Aufbewahrungspflichten nach Unionsrecht oder nationalem Recht bleiben unberührt und gehen den Weisungen des Auftraggebers vor.

§ 11 Haftung

Hinsichtlich der Haftung wird auf Art. 82 DSGVO verwiesen.

§ 12 Sonstiges

1. Alle Änderungen, Nebenabreden, die Kündigung und Aufhebung dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für die Aufhebung dieser Klausel. Nebenabreden wurden nicht getroffen. Streichungen in dieser Vereinbarung müssen von beiden Parteien gezeichnet werden.
2. Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam oder lückenhaft sein, so berührt dies die Gültigkeit der übrigen Bestimmungen nicht. Vielmehr tritt für den Fall, dass ein Verbraucher an dem Vertrag nicht beteiligt ist an die Stelle der unwirksamen Bestimmung eine Regelung, die dem gewollten Zweck am nächsten kommt. Im Fall einer Lücke gilt dann diejenige Bestimmung als vereinbart, die dem entspricht, was nach dem Zweck vereinbart worden wäre, hätten die Parteien die Angelegenheit von vornherein bedacht. Ist hiernach eine Lösung nicht möglich, finden die Parteien eine Regelung im Geist partnerschaftlicher Kooperation.
3. Es gilt deutsches Recht.

Anlage 1

Gegenstand des Auftrags

1. Gegenstand, Art und Zweck der Verarbeitung

Gegenstand der Verarbeitung sind je nach den geschlossenen Individualverträgen zu erbringende Dienstleistungen für Webhosting, Rechenzentrumsarbeiten, Administration des oder der entsprechenden Server(s) inklusive des Anlegens von Datensicherungen und die damit im Zusammenhang stehende Verarbeitung der Daten auf den Systemen des Auftragnehmers. Zweck der Verarbeitung ist die jeweilige Nutzung dieser vom Auftragnehmer erbrachten Leistungen. Die Arten der Verarbeitung sind die damit im Zusammenhang stehenden Vorgänge oder Vorgangsreihen, insbesondere das Erheben, Ordnen, Speichern, Übermitteln, Löschen, Anonymisieren, oder Pseudonymisieren.

2. Art(en) der personenbezogenen Daten

Die Art(en) der personenbezogenen Daten sind alle sind die Nutzungs- und Contentdaten, die im Rahmen der jeweiligen Dienstleistungen der einzelnen Individualverträge vom Auftraggeber in den für ihn beim Auftraggeber gehosteten Websites, Servern, Datenbanken und E-Mail-Postfächern gespeichert oder verarbeitet werden, die vom Auftraggeber selbst, oder von Nutzern der Websites des Auftraggebers auf dessen Websites eingegeben werden, die per E-Mail an ihn gesendet oder vom Aufraggeber per E-Mail versendet werden.
Insbesondere kann es sich dabei um folgende Daten handeln:

- Daten, die technisch erforderlich sind, um eine Webseite anzuzeigen
- Vertragsdaten von Lieferanten und Kunden des Auftraggebers
- Kontaktdaten von Mitarbeitern, Lieferanten, Kunden und Interessenten des Auftraggebers
- Abrechnungsdaten von Kunden des Auftraggebers
- Bank- und Kontodaten von Kunden des Auftraggebers
- Inhaltsdaten, insbesondere aus E-Mailkommunikation

Soweit rechtlich zulässig, kann der Auftraggeber auch besondere Kategorien personenbezogener Daten gemäß Artikel 9 personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 auf den Systemen des Auftragnehmers verarbeiten lassen.

3. Kategorien betroffener Personen

Es werden die personenbezogenen Daten von Personen verarbeitet, deren Daten im Rahmen der gehosteten Services verarbeitet werden. Dies können sein:

- Kunden
- Nutzer
- Lieferanten und Dienstleister
- Beschäftigte
- Interessenten

Anlage 2

Subunternehmer

1. Hetzner Online GmbH

Adresse:
Industriestr. 25
91710 Gunzenhausen
Leistungen:
Bereitstellung Serverinfrastruktur
Übermittelte Daten:
Keine direkte Übermittlung personenbezogener Daten. Hetzner stellt ausschließlich die technische Infrastruktur bereit.

2. netcup GmbH

Adresse:
Daimlerstraße 25
76185 Karlsruhe
Leistungen:
Bereitstellung Serverinfrastruktur
Übermittelte Daten:
Keine direkte Übermittlung personenbezogener Daten. Netcup stellt ausschließlich die technische Infrastruktur bereit.

3. INWX GmbH

Adresse:
Prinzessinnenstr. 30
10969 Berlin
Leistungen:
Domainregistrierung
Übermittelte Daten:
Personenbezogene Daten der Domaininhaber. Die Daten sind notwendig, um die jeweiligen Domains auf den Kunden zu registrieren
- Name / Firmenname
- Anschrift
- Telefonnummer
- Je nach Land Außerdem noch (z.B. Italien): Steuernummer/Umsatzsteuer-ID, Personalausweis-ID

4. Haufe-Lexware GmbH & Co. KG

Adresse:
Munzinger Straße 9
79111 Freiburg
Leistungen:
Bereitstellung Buchhaltungs- und Rechnungsdienstleistungen / Software
Übermittelte Daten:
- Kundendaten im Rahmen der Rechnungsstellung
- Zahlungsdaten

5. IT-Lösungen Christian Müller

Adresse:
Husarengasse 6
76829 Landau / Pfalz
Leistungen:
3cx Telefonanlagen Partner
Übermittelte Daten:
Die Daten sind notwendig. um eine Lizenz einer 3cx Telefonanlage auf den Kunden zu registrieren:
- Name / Firmenname
- Anschrift
- Telefonnummer
- E-Mail-Adresse

6. Microsoft Corporation

Adresse:
One Microsoft Way
Redmond, WA 98052-6399
USA
Leistungen:
Bereitstellung von Cloud-Diensten für die Interne Nutzung (Microsoft 365/Exchange Online) beim Auftragnehmer selbst.
Übermittelte Daten:
Microsoft Corporation handelt für die in Deutschland gehosteten Microsoft 365 Business-Dienste als Auftragsverarbeiter im Sinne von Art. 28 DSGVO. Eine Übermittlung personenbezogener Daten in Drittländer erfolgt nicht.

Hinweiß:
Der Auftragnehmer vertreibt zudem Microsoft-Lizenzen an Dritte. Diese Tätigkeit stellt keine Auftragsverarbeitung durch Microsoft für den Auftragnehmer dar.
Die Datenverarbeitung durch Microsoft erfolgt im Verhältnis zwischen Microsoft und dem jeweiligen Endkunden auf Grundlage eigener Verträge (z. B. Microsoft-Datenschutzbestimmungen und DPA).

Anlage 3

Technische und organisatorische Maßnahmen

1. Pseudonymisierung und Datenminimierung (Art. 32 Abs. 1 it. a DSGVO, Art. 25 Abs. 1 DSGVO)

Maßnahmen zur Verarbeitung personenbezogener Daten in einer Weise, dass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und den entsprechenden technischen und organisatorischen Maßnahmen unterliegen:

1. IP-Adressen werden in Logdateien nur vollständig erfasst, sofern dies zum ordnungsgemäßen Betrieb der Server erforderlich ist (d.h. zur Abwehr von Angriffen, zur Feststellung missbräuchlicher Verwendung von Diensten oder der Herausgabe bei Anfragen durch Strafverfolgungsbehörden, usw.).
2. Logdateien, welche unverfremdete IP-Adressen enthalten, werden auf unseren Systemen automatisch rotiert.
3. Über längere Zeit gespeicherte IP-Adressen (z.B. als Grundlage zur Erstellung von Statistiken für unsere Kunden) sind durch Unkenntlichmachung eines Oktetts (IPv4) bzw. eines Hextetts (IPv6) nicht mehr eindeutig einer bestimmten Person zuzuordnen.
4. Es werden nur solche persönlichen Daten unserer Kunden erhoben, die für die Erbringung unserer Dienstleistung notwendig sind. Mitarbeiter sind zur Datensparsamkeit gehalten.

2. Vertraulichkeit (Art. 32. Abs. Mit. b DSGVO)

1. Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle):
    - Alle DV-Systeme, die Zugang zu personenbezogenen Daten gewähren, erfordern mindestens eine Authentifikation mittels Benutzername und Kennwort.
    - Benutzerzugänge sind personalisiert.
    - Es erfolgt ein Entzug von Berechtigungen, sofern diese nicht mehr benötigt werden.
    - Bei wiederholten Authentifizierungsfehlern erfolgt eine automatische Sperrung von Zugängen.
    - Vorgeschrieben ist für alle Arbeitsplatzrechner das Einrichten einer automatischen Bildschirmsperre mit Kennwortschutz bei Untätigkeit.
2. Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene
   Daten getrennt verarbeitet werden (Trennungskontrolle):
    - Personenbezogene Daten werden ausschließlich zweckgebunden verarbeitet.

3. Integrität (Art. 32. Abs. llit. b DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der Übertragung, Verarbeitung oder Speicherung nicht unbefugt gelesen, verändert, kopiert oder gelöscht werden können:

1. Entfernter Zugriff erfolgt ausschließlich über verschlüsselte Verbindungen (z. B. VPN oder SSH).
2. Daten werden, wo technisch möglich, verschlüsselt gespeichert.
3. Systeme werden regelmäßig auf unbefugte Änderungen, Manipulationen oder Sicherheitslücken überprüft.
4. Sicherheitsupdates und Patches werden zeitnah eingespielt, um die Integrität der Systeme zu gewährleisten.
5. Personenbezogene Daten werden standardmäßig nicht an Dritte übermittelt, außer im Rahmen schriftlicher Weisungen des Auftraggebers oder gesetzlicher Verpflichtungen.

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

Maßnahmen, welche gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und verfügbar bleiben (Verfügbarkeitskontrolle):

1. Es existiert ein vollständiges Backup- und Recovery-Konzept, um Daten im Falle eines Ausfalls wiederherstellen zu können.
2. Tägliche Datensicherungen werden automatisch durchgeführt.
3. Server sind mit RAID-Systemen ausgestattet, um die Ausfallsicherheit zu erhöhen.
4. Auf Wunsch werden Hochverfügbarkeitslösungen umgesetzt.
5. In den Rechenzentren wird Gebrauch von unterbrechungsfreier Stromversorgung gemacht.
6. Es besteht eine mehrfach-redundante Anbindung an Backbone Provider.
7. Serverstandorte befinden sich – soweit nicht anders vereinbart – in Deutschland.