



Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 DSGVO

Der Verantwortliche:

Der Auftragsverarbeiter:

.....

Firmenwortlaut

.....

Straße, Hausnummer

.....

PLZ, Ort

.....

Firmenbuchnummer · UID

Lukas Krempl IT Services e.U.
Bergviertel 61

8190 Miesenbach bei Birkfeld
FN 667716k · UID ATU83372315

(im Folgenden Auftraggeber)

(im Folgenden Auftragnehmer)

1. GEGENSTAND DER VEREINBARUNG

- (1) Gegenstand dieses Auftrages ist die IT-Betreuung der vom Auftraggeber genutzten Systeme im vereinbarten Umfang, insbesondere Einrichtung, Betreuung und Reparatur von Netzwerk, Endgeräten, Servern und Software, Fernwartung und Überwachung, IT-Sicherheit, Datensicherung, Datenrettung und Datenmigration, Hosting, Administration von Cloud-Diensten sowie Anwender-Support und Schulungen. Zweck der Verarbeitung ist ausschließlich die Erbringung dieser Leistungen; ein Zugriff auf Inhaltsdaten erfolgt nur, soweit dies für Wartung, Fehlerbehebung oder Wiederherstellung technisch erforderlich ist.

Diese Vereinbarung ergänzt die zwischen den Parteien vereinbarten IT-Leistungen (Angebote, Aufträge und Abonnements).

- (2) Folgende Datenkategorien werden verarbeitet: Kontakt- und Stammdaten (Name, Adresse, Telefon, E-Mail), Benutzerkonten und Zugangsdaten, Geräte-, Protokoll- und Systemdaten (Inventar, Log- und Telemetriedaten), E-Mail- und Dokumentinhalte, Vertrags-, Kunden- und Verrechnungsdaten, Beschäftigtendaten wie Einsatz- und Arbeitszeitplanung sowie Inhalte von Datensicherungen – jeweils in dem Umfang, in dem sie sich auf den betreuten Systemen des Auftraggebers befinden.

- (3) Folgende Kategorien betroffener Personen unterliegen der Verarbeitung: Beschäftigte des Auftraggebers, Kunden und Interessenten, Lieferanten und Geschäftspartner sowie sonstige Personen, deren Daten in den betreuten Systemen gespeichert sind. Soweit dabei besondere Kategorien personenbezogener Daten im Sinne des Art 9 DSGVO (insbesondere Gesundheitsdaten) oder Daten, die einer berufsrechtlichen Verschwiegenheitspflicht unterliegen (etwa bei Ärzten, Steuerberatern oder Rechtsanwälten), verarbeitet werden, beschränkt der Auftragnehmer den Zugriff auf das für die Leistungserbringung unbedingt erforderliche Maß und wendet die Maßnahmen der Anlage ./1 mit besonderer Sorgfalt an; Inhaltsdaten werden nur auf ausdrückliche Weisung des Auftraggebers eingesehen.

2. DAUER DER VEREINBARUNG

Die Vereinbarung gilt, solange der Auftragnehmer für den Auftraggeber Leistungen erbringt, bei denen personenbezogene Daten verarbeitet werden, und endet automatisch mit deren Beendigung. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Die Verpflichtungen zur Vertraulichkeit sowie zur Rückgabe und Löschung der Daten gelten über das Ende der Vereinbarung hinaus.

3. PFLICHTEN DES AUFTRAGNEHMERS

- (1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der dokumentierten Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er – sofern gesetzlich zulässig – den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines dokumentierten Auftrages.
- (2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.
- (3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage ./1 zu entnehmen).
- (4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenverarbeitung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.
- (5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).
- (6) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.
- (7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht auf Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen, sei es auch

durch von ihm beauftragte Dritte, nach rechtzeitiger Vorankündigung eingeräumt. Die Kontrolle erfolgt vorrangig durch Vorlage geeigneter Nachweise. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

- (8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag zu vernichten, soweit keine gesetzliche Aufbewahrungspflicht besteht. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.
- (9) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Die Datenverarbeitung erfolgt innerhalb der Europäischen Union bzw. des EWR. Soweit Sub-Auftragsverarbeiter ihren Sitz in einem Drittland haben oder bei eingesetzten Diensten Zugriffe aus Drittländern möglich sind, erfolgt dies nur auf Grundlage eines Angemessenheitsbeschlusses (Art 45 DSGVO, insbesondere EU-US Data Privacy Framework) oder geeigneter Garantien (Art 46 DSGVO, insbesondere EU-Standardvertragsklauseln). Die betroffenen Anbieter und die jeweilige Grundlage sind in Anlage ./2 angeführt.

5. SUB-AUFTRAGSVERARBEITER

Der Auftragnehmer kann Sub-Auftragsverarbeiter für die in Anlage ./2 genannten Tätigkeiten hinzuziehen. Die zum Zeitpunkt des Vertragsabschlusses eingesetzten Sub-Auftragsverarbeiter sind in Anlage ./2 angeführt und gelten als genehmigt.

Der Auftragnehmer hat den Auftraggeber von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen.

Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

.....
Ort, Datum

Für den Auftraggeber:

Miesenbach bei Birkfeld, ...
Ort, Datum

Für den Auftragnehmer:

.....
Unterschrift

.....
Lukas Krempl, Inhaber

.....
Name in Blockschrift, Funktion

Anlage ./1 – Technisch-organisatorische Maßnahmen

A. VERTRAULICHKEIT

Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:

☒ Schlüssel	☐ Magnet- oder Chipkarten
☐ Elektrische Türöffner	☐ Portier
☐ Sicherheitspersonal	☐ Alarmanlagen
☐ Videoanlage	☐ Einbruchshemmende Fenster und/oder Sicherheitstüren
☐ Anmeldung beim Empfang mit Personenkontrolle	☐ Begleitung von Besuchern im Unternehmensgebäude
☐ Tragen von Firmen-/Besucherausweisen	☐ Sonstiges:

Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch:

☒ Kennwörter (einschließlich entsprechender Policy)	☒ Verschlüsselung von Datenträgern
☒ Automatische Sperrmechanismen	☐ Sonstiges:
☒ Zwei-Faktor-Authentifizierung	

Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

☒ Standard-Berechtigungsprofile auf „need to know-Basis“	☐ Standardprozess für Berechtigungsvergabe
☒ Protokollierung von Zugriffen	☒ Sichere Aufbewahrung von Speichermedien
☐ Periodische Überprüfung der vergebenen Berechtigungen, insb. von administrativen Benutzerkonten	☒ Datenschutzgerechte Wiederverwendung von Datenträgern
☒ Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger	☒ Clear-Desk/Clear-Screen Policy
☐ Sonstiges:	

Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.

☐ Ja	☒ Nein
-----------------------------	--

Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

☐ Ja	☒ Nein
-----------------------------	--

B. DATENINTEGRITÄT

Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

☒ Verschlüsselung von Datenträgern	☒ Verschlüsselung von Dateien
☒ Virtual Private Networks (VPN)	☐ Elektronische Signatur
☐ Sonstiges:	

Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch:

☒ Protokollierung	☒ Dokumentenmanagement
☐ Sonstiges:	

C. VERFÜGBARKEIT UND BELASTBARKEIT

Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

☒ Backup-Strategie (online/offline; on-site/off-site)	☐ Unterbrechungsfreie Stromversorgung (USV, Dieselaggregat)
☒ Virenschutz	☒ Firewall
☒ Meldewege und Notfallpläne	☐ Security Checks auf Infrastruktur- und Applikationsebene
☐ Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum	☐ Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
☐ Sonstiges:	

Rasche **Wiederherstellbarkeit:**

☐ Ja	☒ Nein
-----------------------------	--

D. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen:

☐ Ja	☒ Nein
-----------------------------	--

Incident-Response-Management:

☐ Ja	☒ Nein
-----------------------------	--

Datenschutzfreundliche Voreinstellungen:

☒ Ja	☐ Nein
--	-------------------------------

Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers durch:

☒ Eindeutige Vertragsgestaltung	☐ Formalisiertes Auftragsmanagement
☒ Strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS)	☒ Vorabüberzeugungspflicht
☐ Nachkontrollen	☐ Sonstiges:

Anlage ./2 – Sub-Auftragsverarbeiter

Stand: September 2026. Die angeführten Sub-Auftragsverarbeiter kommen jeweils nur im Umfang der vom Auftraggeber beauftragten Leistungen zum Einsatz. Alle verarbeiten die Daten innerhalb der EU/des EWR. Für NinjaOne (Sitz USA, Verarbeitung in der EU-Instanz) und Microsoft (Verarbeitung im Rahmen der EU Data Boundary) gelten für allfällige Zugriffe aus Drittländern das EU-US Data Privacy Framework (DPF) sowie ergänzend die EU-Standardvertragsklauseln (SCC).

Unternehmen / Sitz	Tätigkeit
Microsoft Ireland Operations Ltd., Dublin, IE	E-Mail, Dateiablage und Zusammenarbeit des Auftragnehmers (EU)
NinjaOne LLC, Oldsmar, Florida, USA – EU-Instanz	Fernwartung, Monitoring, Patchmanagement (DE; DPF/SCC)
Bitdefender SRL, Bukarest, RO (Bezug über NinjaOne)	Virenschutz und EDR (EU)
IONOS SE, Montabaur, DE	Server-Hosting, Veeam-Backup-Konsole und Cloud-Speicher (DE)
Hornetsecurity GmbH, Hannover, DE	E-Mail-Sicherheit, Archivierung, M365-Backup (DE)
Odoo S.A., Ramillies, BE	Ticket- und Verrechnungssystem (EU)