

Vertrag über Auftragsverarbeitung gemäß Art. 28 DSGVO

Stand: 25.07.2026 Anbieter: HostingUndDomains.de / kalro digiTal Evolution GmbH

1. Parteien

zwischen

dem jeweiligen Kunden, der Leistungen von HostingUndDomains.de beauftragt und dabei personenbezogene Daten im Auftrag verarbeiten lässt,

im Folgenden "Auftraggeber" oder "Kunde"

und

kalro digiTal Evolution GmbH Gartenweg 2 21521 Dassendorf Deutschland

handelnd unter der Marke HostingUndDomains.de

vertreten durch Kai Plückhahn

im Folgenden "Auftragnehmer"

gemeinsam die "Parteien".

2. Gegenstand und Geltungsbereich

2.1 Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers gemäß Art. 28 DSGVO.

2.2 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der mit dem Auftraggeber vereinbarten Leistungen. Grundlage ist der zwischen den Parteien geschlossene Vertrag über Hosting-, Domain-, Administrations-, Wartungs-, Support-, Beratungs- oder sonstige IT-Dienstleistungen einschließlich aller Anlagen, Leistungsbeschreibungen, Angebote und Servicevereinbarungen (im Folgenden "Hauptvertrag").

2.3 Dieser Vertrag gilt für alle Tätigkeiten, bei denen der Auftragnehmer oder von ihm eingesetzte Unterauftragnehmer personenbezogene Daten des Auftraggebers verarbeiten oder Zugriff auf solche Daten erhalten können.

2.4 Dieser Vertrag begründet keine Verpflichtung zur Erbringung bestimmter IT-Leistungen. Inhalt, Umfang und Vergütung der Leistungen ergeben sich ausschließlich aus dem Hauptvertrag.

3. Art, Zweck und Dauer der Verarbeitung

3.1 Die Verarbeitung erfolgt zum Zweck der Erbringung der im Hauptvertrag vereinbarten Leistungen. Dies kann insbesondere folgende Tätigkeiten umfassen:

- Bereitstellung, Betrieb und Wartung von Hosting-, Web-, E-Mail-, DNS-, Datenbank- oder Serverdiensten
- Einrichtung, Administration, Überwachung und Absicherung von IT-Systemen
- Fehleranalyse, Support, Incident Response und Wiederherstellung von Diensten
- Durchführung von Updates, Backups, Migrationen und Konfigurationsänderungen
- technische Beratung, Systemintegration, Automatisierung und Dokumentation
- sonstige Tätigkeiten, die zur Erfüllung des Hauptvertrags erforderlich sind

3.2 Art der Verarbeitung kann insbesondere sein:

- Erheben, Erfassen und Speichern
- Ordnen, Strukturieren und Auslesen
- Abfragen, Verwenden und Offenlegen durch Übermittlung
- Abgleich, Einschränkung, Löschung und Vernichtung
- Sicherung, Wiederherstellung, Protokollierung und Fehleranalyse

3.3 Die Verarbeitung beginnt mit Wirksamwerden des Hauptvertrags oder mit erstmaligem Zugriff des Auftragnehmers auf personenbezogene Daten des Auftraggebers und endet mit Beendigung des Hauptvertrags oder dieses Vertrags, soweit keine gesetzlichen Aufbewahrungspflichten oder berechnete Dokumentationspflichten entgehen.

4. Kategorien personenbezogener Daten

4.1 Je nach beauftragter Leistung können insbesondere folgende Kategorien personenbezogener Daten verarbeitet werden:

- Stammdaten, z. B. Name, Firma, Kundennummer, Benutzerkennung
- Kontaktdaten, z. B. Anschrift, E-Mail-Adresse, Telefonnummer
- Vertrags- und Abrechnungsdaten
- Inhaltsdaten, z. B. Website-Inhalte, E-Mail-Inhalte, hochgeladene Dateien, Datenbankinhalte
- Nutzungs-, Verbindungs- und Protokolldaten, z. B. IP-Adressen, Zeitstempel, Logfiles, Login-Ereignisse
- technische Metadaten, z. B. Geräte-, Browser-, Domain-, DNS-, Server- und Applikationsdaten
- Support- und Kommunikationsdaten, z. B. Tickets, Fehlermeldungen, Diagnosedaten
- sonstige Daten, die der Auftraggeber in die vom Auftragnehmer betriebenen oder betreuten Systeme einbringt

4.2 Besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO werden durch den Auftragnehmer nur verarbeitet, wenn und soweit der Auftraggeber solche Daten in die beauftragten Systeme einbringt oder deren Verarbeitung ausdrücklich beauftragt. Der Auftraggeber ist für die Zulässigkeit dieser Verarbeitung verantwortlich.

5. Kategorien betroffener Personen

Je nach beauftragter Leistung können insbesondere folgende Personengruppen betroffen sein:

- Kunden, Interessenten und Geschäftspartner des Auftraggebers
- Beschäftigte, freie Mitarbeiter und Erfüllungsgehilfen des Auftraggebers
- Nutzer von Websites, Shops, Portalen, E-Mail-Systemen oder sonstigen IT-Diensten des Auftraggebers
- Kommunikationspartner des Auftraggebers
- sonstige Personen, deren Daten der Auftraggeber in die beauftragten Systeme einbringt

6. Verantwortlichkeit und Weisungen

6.1 Der Auftraggeber ist Verantwortlicher im Sinne der DSGVO. Er ist für die Rechtmäßigkeit der Verarbeitung, die Wahrung der Rechte betroffener Personen, die Auswahl der zu verarbeitenden Daten und die Erteilung zulässiger Weisungen verantwortlich.

6.2 Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, sofern er nicht gesetzlich zu einer anderen Verarbeitung verpflichtet ist. In diesem Fall informiert der Auftragnehmer den Auftraggeber vor der Verarbeitung über die gesetzliche Pflicht, soweit eine solche Information rechtlich zulässig ist.

6.3 Weisungen können sich aus dem Hauptvertrag, diesem Vertrag, Leistungsbeschreibungen, Tickets, schriftlicher Kommunikation oder sonstiger dokumentierter Abstimmung ergeben. Mündliche Weisungen sind durch den Auftraggeber unverzüglich in Textform zu bestätigen.

6.4 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht oder sonstige gesetzliche Vorgaben verstößt. Der Auftragnehmer ist berechtigt, die Ausführung einer solchen Weisung bis zur Bestätigung oder Änderung durch den Auftraggeber auszusetzen.

6.5 Zur Erteilung und Entgegennahme von Weisungen berechnete Personen werden in Anlage 3 benannt.

7. Pflichten des Auftragnehmers

7.1 Der Auftragnehmer verpflichtet sich, personenbezogene Daten vertraulich zu behandeln und ausschließlich im Rahmen dieses Vertrags, des Hauptvertrags und der Weisungen des Auftraggebers zu verarbeiten.

7.2 Der Auftragnehmer stellt sicher, dass Personen, die mit der Verarbeitung personenbezogener Daten befasst sind, zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.3 Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Die bei Vertragsschluss vereinbarten Maßnahmen sind in Anlage 1 beschrieben.

7.4 Der Auftragnehmer unterstützt den Auftraggeber im erforderlichen und zumutbaren Umfang bei:

- der Beantwortung von Anfragen betroffener Personen
- der Berichtigung, Löschung oder Einschränkung der Verarbeitung
- der Erfüllung von Melde- und Benachrichtigungspflichten gemäß Art. 33 und 34 DSGVO
- Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO
- Anfragen und Prüfungen von Aufsichtsbehörden

7.5 Soweit Unterstützungsleistungen über den vertraglich geschuldeten Leistungsumfang hinausgehen, können diese nach Aufwand gemäß Hauptvertrag oder gesonderter Vereinbarung vergütet werden, sofern der Aufwand nicht durch ein schuldhaftes Verhalten des Auftragnehmers verursacht wurde.

7.6 Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten, soweit er hierzu gesetzlich verpflichtet ist, und stellt dem Auftraggeber die zur Erfüllung seiner Nachweispflichten erforderlichen Informationen in angemessenem Umfang zur Verfügung.

8. Technische und organisatorische Maßnahmen

8.1 Die technischen und organisatorischen Maßnahmen des Auftragnehmers werden in Anlage 1 beschrieben und zusätzlich unter <https://www.hostingunddomains.de/agb/tom/> veröffentlicht. Sie dienen insbesondere der Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste.

8.2 Der Auftragnehmer darf die Maßnahmen an technische, organisatorische oder sicherheitsrelevante Entwicklungen anpassen, solange das vereinbarte Sicherheitsniveau nicht unterschritten wird.

8.3 Wesentliche Änderungen, die das Sicherheitsniveau erheblich betreffen, teilt der Auftragnehmer dem Auftraggeber in geeigneter Weise mit.

8.4 Die konkrete Ausgestaltung der Maßnahmen kann je nach beauftragter Leistung, Systemumgebung und Verantwortungsbereich variieren. Soweit der Auftraggeber eigene Systeme, Zugangsdaten, Anwendungen oder Konfigurationen bereitstellt, bleibt er für deren datenschutzkonformen und sicheren Betrieb verantwortlich, soweit nichts anderes vereinbart ist.

9. Unterauftragnehmer

9.1 Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zum Einsatz von Unterauftragnehmern gemäß Art. 28 Abs. 2 DSGVO.

9.2 Zum Zeitpunkt des Vertragsschlusses eingesetzte Unterauftragnehmer sind in Anlage 2 aufgeführt.

9.3 Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragnehmern. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Tagen widersprechen.

9.4 Der Auftragnehmer verpflichtet Unterauftragnehmer vertraglich auf Datenschutzpflichten, die den Pflichten dieses Vertrags im Wesentlichen entsprechen. Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Einhaltung der Pflichten durch Unterauftragnehmer verantwortlich.

9.5 Kein Unterauftrag im Sinne dieses Vertrags sind rein begleitende Nebenleistungen ohne unmittelbaren Bezug zur Verarbeitung personenbezogener Daten im Auftrag, z. B. Telekommunikationsleistungen, Post- und Transportdienste, Zahlungsdienstleistungen, Wartung von Standardinfrastruktur ohne Zugriff auf personenbezogene Daten oder sonstige Hilfsleistungen. Der Auftragnehmer stellt auch bei solchen Nebenleistungen ein angemessenes Datenschutzniveau sicher.

9.6 Eine Verarbeitung außerhalb der EU, des EWR oder eines Staates mit Angemessenheitsbeschluss der EU-Kommission erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere durch Angemessenheitsbeschluss, Standardvertragsklauseln oder andere geeignete Garantien.

10. Kontroll- und Nachweispflichten

10.1 Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die zur Erfüllung seiner Nachweispflichten gemäß Art. 28 DSGVO erforderlichen Informationen in angemessenem Umfang zur Verfügung.

10.2 Der Auftraggeber ist berechtigt, die Einhaltung dieses Vertrags im erforderlichen Umfang zu kontrollieren. Kontrollen erfolgen vorrangig durch Auskünfte, Dokumentationen, geeignete Nachweise oder vorhandene Prüfberichte.

10.3 Vor-Ort-Prüfungen sind nur nach angemessener Vorankündigung, während der üblichen Geschäftszeiten, unter Wahrung von Betriebs- und Geschäftsgeheimnissen sowie ohne unverhältnismäßige Störung des Geschäftsbetriebs des Auftragnehmers zulässig.

10.4 Der Auftraggeber darf Kontrollen grundsätzlich höchstens einmal pro Kalenderjahr durchführen, soweit kein konkreter Anlass besteht. Anlassbezogene Kontrollen bleiben unberührt.

10.5 Der Auftraggeber trägt die durch eine Kontrolle entstehenden eigenen Kosten. Zusätzlicher Aufwand des Auftragnehmers kann nach Aufwand berechnet werden, soweit die Kontrolle nicht durch einen vom Auftragnehmer zu vertretenden Datenschutzverstoß veranlasst wurde.

11. Meldung von Datenschutzverletzungen

11.1 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die im Zusammenhang mit der Auftragsverarbeitung steht.

11.2 Die Mitteilung erfolgt an die vom Auftraggeber benannte Kontaktstelle. Sie enthält, soweit dem Auftragnehmer bekannt und ohne unverhältnismäßigen Aufwand verfügbar:

- Beschreibung der Art der Verletzung
- betroffene Kategorien personenbezogener Daten
- betroffene Personengruppen und ungefähre Anzahl
- mögliche Folgen der Verletzung
- ergriffene oder vorgeschlagene Gegenmaßnahmen
- Kontaktstelle für Rückfragen

11.3 Soweit nicht alle Informationen sofort verfügbar sind, kann der Auftragnehmer diese schrittweise nachreichen.

11.4 Die Entscheidung über Meldungen an Aufsichtsbehörden oder betroffene Personen obliegt dem Auftraggeber, soweit nicht der Auftragnehmer selbst gesetzlich zur Meldung verpflichtet ist.

12. Rechte betroffener Personen

12.1 Macht eine betroffene Person Rechte unmittelbar gegenüber dem Auftragnehmer geltend, leitet der Auftragnehmer die Anfrage unverzüglich an den Auftraggeber weiter, sofern eine Zuordnung möglich ist.

12.2 Der Auftragnehmer beantwortet Anfragen betroffener Personen nur nach Weisung des Auftraggebers, soweit keine gesetzliche Pflicht zur eigenen Beantwortung besteht.

12.3 Der Auftragnehmer unterstützt den Auftraggeber im erforderlichen und zumutbaren Umfang bei der technischen Umsetzung von Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch.

13. Löschung und Rückgabe nach Auftragsende

13.1 Nach Beendigung der Auftragsverarbeitung gibt der Auftragnehmer personenbezogene Daten nach Wahl und Weisung des Auftraggebers zurück oder löscht sie, soweit keine gesetzlichen Aufbewahrungspflichten, Nachweispflichten oder berechtigten Sicherheitsinteressen entgegenstehen.

13.2 Sicherungskopien und Backups werden im Rahmen regulärer Backup-Zyklen überschrieben oder gelöscht, sofern keine frühere Löschung technisch möglich und zumutbar ist. Bis zur Löschung unterliegen die Daten weiterhin den Schutzpflichten dieses Vertrags.

13.3 Dokumentationen, die zum Nachweis ordnungsgemäßer Verarbeitung erforderlich sind, dürfen für die Dauer gesetzlicher Aufbewahrungs- und Verjährungsfristen gespeichert werden.

14. Vertraulichkeit und Geschäftsgeheimnisse

14.1 Beide Parteien behandeln vertrauliche Informationen, Geschäftsgeheimnisse und sicherheitsrelevante Informationen der jeweils anderen Partei vertraulich.

14.2 Diese Pflicht gilt auch nach Beendigung dieses Vertrags fort.

14.3 Der Auftragnehmer ist berechtigt, vertrauliche Informationen an Mitarbeiter, Erfüllungsgehilfen, Berater und Unterauftragnehmer weiterzugeben, soweit dies zur Vertragserfüllung erforderlich ist und die Empfänger angemessen zur Vertraulichkeit verpflichtet sind.

15. Vergütung

15.1 Die Vergütung für die im Hauptvertrag vereinbarten Leistungen richtet sich nach dem Hauptvertrag.

15.2 Unterstützungs-, Nachweis-, Prüfungs- oder Sonderleistungen, die nicht bereits vom Hauptvertrag umfasst sind, können nach Aufwand abgerechnet werden, soweit gesetzlich zulässig und nicht durch ein schuldhaftes Verhalten des Auftragnehmers verursacht.

16. Haftung

16.1 Die Haftung der Parteien richtet sich nach den gesetzlichen Vorschriften, insbesondere Art. 82 DSGVO, sowie den Haftungsregelungen des Hauptvertrags, soweit diese wirksam vereinbart sind.

16.2 Der Auftraggeber ist für die Rechtmäßigkeit der beauftragten Verarbeitung, die Zulässigkeit der Weisungen und die Erfüllung der Informationspflichten gegenüber betroffenen Personen verantwortlich.

16.3 Der Auftragnehmer haftet für Schäden, die durch eine Verarbeitung verursacht wurden, bei der er seinen speziell auferlegten Pflichten als Auftragsverarbeiter nicht nachgekommen ist oder rechtmäßig erteilte Weisungen des Auftraggebers nicht beachtet oder gegen diese gehandelt hat.

16.4 Soweit der Auftragnehmer aufgrund einer rechtswidrigen Weisung des Auftraggebers in Anspruch genommen wird, stellt der Auftraggeber den Auftragnehmer von daraus entstehenden Ansprüchen und Kosten frei, soweit der Auftragnehmer den Auftraggeber zuvor auf die Rechtswidrigkeit hingewiesen hat oder die Rechtswidrigkeit für den Auftragnehmer nicht erkennbar war.

17. Laufzeit und Kündigung

17.1 Dieser Vertrag tritt mit Unterzeichnung oder mit Beginn der Auftragsverarbeitung in Kraft.

17.2 Der Vertrag endet automatisch mit Beendigung des Hauptvertrags, soweit keine Auftragsverarbeitung mehr stattfindet.

17.3 Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor, wenn eine Partei schwerwiegend gegen datenschutzrechtliche Pflichten verstößt und den Verstoß trotz angemessener Fristsetzung nicht abstellt.

18. Schlussbestimmungen

18.1 Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform, soweit nicht gesetzlich eine strengere Form vorgeschrieben ist.

18.2 Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

18.3 Es gilt das Recht der Bundesrepublik Deutschland.

18.4 Gerichtsstand ist, soweit zulässig, der Sitz des Auftragnehmers.

19. Einbeziehung und Abschluss

19.1 Für Verträge, die ab dem 27.07.2026 abgeschlossen werden, wird diese Vereinbarung zur Auftragsverarbeitung automatisch in den Vertrag einbezogen, soweit die beauftragte Leistung eine Auftragsverarbeitung personenbezogener Daten im Sinne von Art. 28 DSGVO umfasst.

19.2 Für vor dem 27.07.2026 abgeschlossene Verträge kann diese Vereinbarung nachträglich in Textform, insbesondere per E-Mail, einbezogen werden.

19.3 Einer eigenhändigen Unterschrift bedarf es nicht, soweit diese Vereinbarung im Bestellprozess, in der Bestellbestätigung, durch Bezugnahme in den AGB oder durch sonstige Vereinbarung in Textform wirksam einbezogen wird.

Anlage 1 - Technische und organisatorische Maßnahmen

Die folgenden technischen und organisatorischen Maßnahmen beschreiben ein allgemeines Sicherheitsniveau für Hosting-, Administrations- und IT-Dienstleistungen. Die konkrete Ausprägung richtet sich nach den beauftragten Leistungen, eingesetzten Systemen und Verantwortungsbereichen.

1. Vertraulichkeit

1.1 Zutrittskontrolle

- Schutz von Geschäftsräumen, Arbeitsbereichen und technischen Systemen vor unbefugtem Zutritt
- angemessene Schlüssel-, Schließ- und Zugangskonzepte
- Beaufsichtigung von Besuchern in Bereichen mit Zugriffsmöglichkeit auf personenbezogene Daten
- keine unbeaufsichtigte Offenlegung von Kundendaten gegenüber Dritten

1.2 Zugangskontrolle

- personenbezogene Benutzerkonten, soweit technisch möglich und sinnvoll
- Authentifizierung durch starke Passwörter und, wo angemessen, Mehr-Faktor-Authentifizierung
- verschlüsselte Administrationszugänge, z. B. SSH, VPN oder TLS-gesicherte Weboberflächen
- Sperrung oder Entfernung nicht mehr benötigter Zugänge
- Schutz administrativer Konten durch besondere Sorgfalt

1.3 Zugriffskontrolle

- Rechtevergabe nach dem Need-to-know- und Least-Privilege-Prinzip
- rollen- oder gruppenbasierte Berechtigungen, soweit technisch möglich
- Trennung von Kundenumgebungen, Projekten, Mandanten oder Datenbeständen nach technischer Möglichkeit und beauftragter Leistung
- regelmäßige Überprüfung administrativer Berechtigungen in angemessenem Umfang
- sichere Aufbewahrung und Verwaltung von Zugangsdaten, Schlüsseln und Secrets

1.4 Trennungskontrolle

- logische oder physische Trennung von Daten unterschiedlicher Auftraggeber, soweit für die beauftragte Leistung erforderlich
- getrennte Kundenkonten, Verzeichnisse, Datenbanken, Instanzen, Namespaces oder Projekte, soweit technisch und wirtschaftlich angemessen
- getrennte Verarbeitung von Test-, Entwicklungs- und Produktivdaten, soweit vereinbart oder erforderlich

2. Integrität

2.1 Weitergabe- und Transportkontrolle

- Transportverschlüsselung bei administrativen Zugriffen und Datenübertragungen, soweit technisch möglich
- verschlüsselte Übertragung über HTTPS, SSH, SFTP, VPN oder vergleichbare Verfahren
- keine bewusste unverschlüsselte Übermittlung sensibler Zugangsdaten
- dokumentierte oder nachvollziehbare Weitergabe von Zugangsdaten und administrativen Informationen

2.2 Eingabekontrolle und Protokollierung

- Protokollierung administrativer Zugriffe und sicherheitsrelevanter Ereignisse, soweit technisch möglich und verhältnismäßig
- Nutzung von System-, Anwendungs-, Webserver-, Mailserver- oder Sicherheitslogs zur Fehleranalyse und Missbrauchserkennung
- angemessene Begrenzung von Log-Aufbewahrungsfristen unter Berücksichtigung technischer, rechtlicher und sicherheitsrelevanter Anforderungen

2.3 Änderungskontrolle

- nachvollziehbare Durchführung wesentlicher Konfigurationsänderungen
- Einsatz von Versionsverwaltung, Ticketsystemen, Dokumentation oder vergleichbaren Verfahren, soweit angemessen
- Prüfung sicherheitsrelevanter Änderungen vor produktivem Einsatz, soweit möglich und verhältnismäßig

3. Verfügbarkeit und Belastbarkeit

3.1 Backup und Wiederherstellung

- Erstellung von Sicherungskopien nach Maßgabe des Hauptvertrags oder der jeweiligen Leistungsbeschreibung
- regelmäßige oder anlassbezogene Prüfung der Wiederherstellbarkeit, soweit vereinbart oder technisch vorgesehen
- Schutz von Backups vor unbefugtem Zugriff
- angemessene Trennung von Produktivdaten und Sicherungskopien

3.2 Betriebssicherheit

- Einsatz geeigneter Sicherheitsupdates und Patches nach Risiko, Systemkritikalität und Kompatibilität
- Überwachung relevanter Systeme, Dienste oder Ressourcen, soweit Bestandteil der beauftragten Leistung
- Schutz vor Schadsoftware, Missbrauch und unberechtigten Zugriffen durch geeignete technische und organisatorische Maßnahmen
- Nutzung von Firewalls, Zugriffsbeschränkungen, Netzwerksegmentierung oder vergleichbaren Schutzmechanismen, soweit technisch sinnvoll

3.3 Wiederanlauf und Incident Response

- Verfahren zur Analyse und Behebung von Störungen
- Eskalations- und Kommunikationswege für sicherheitsrelevante Vorfälle
- Priorisierung von Vorfällen nach Kritikalität und Auswirkung
- Dokumentation wesentlicher Sicherheitsvorfälle in angemessenem Umfang

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- anlassbezogene Überprüfung der getroffenen Sicherheitsmaßnahmen
- Berücksichtigung aktueller Sicherheitsrisiken, Schwachstellen und technischer Entwicklungen
- Pflege von Dokumentationen, Konfigurationen und Sicherheitskonzepten in angemessenem Umfang
- Sensibilisierung und Verpflichtung beteiligter Personen auf Datenschutz und Vertraulichkeit

5. Mobiles Arbeiten und Privatgeräte

- Verarbeitung personenbezogener Daten außerhalb fester Geschäftsräume ist zulässig, soweit geeignete Sicherheitsmaßnahmen bestehen
- administrative Zugriffe erfolgen über gesicherte Geräte, verschlüsselte Verbindungen und angemessene Authentifizierung
- Privatgeräte dürfen nur genutzt werden, wenn sie ein angemessenes Sicherheitsniveau aufweisen und keine unkontrollierte Speicherung personenbezogener Kundendaten erfolgt
- lokale Speicherung personenbezogener Daten wird auf das erforderliche Maß beschränkt

6. Löschung und Datenträger

- Löschung personenbezogener Daten nach Weisung des Auftraggebers oder nach Ablauf vereinbarter Fristen
- sichere Entsorgung oder Löschung von Datenträgern unter Berücksichtigung des Schutzbedarfs
- bei cloud- oder hostingtypischen Speicherumgebungen Löschung nach den technischen Möglichkeiten der eingesetzten Plattform

Anlage 2 - Unterauftragnehmer

Zum Zeitpunkt des Vertragsschlusses setzt der Auftragnehmer folgende Unterauftragnehmer ein:

Hetzner Online GmbH

Anschrift / Sitz: Industriestr. 25, 91710 Gunzenhausen, Deutschland

Leistung: Rechenzentrum, Server, Netzwerk, Storage, Backup-Infrastruktur, Betrieb technischer Hosting-, DNS- und E-Mail-Systeme

Ort der Verarbeitung: Deutschland / EU

Datenschutzgarantien: AVV, technische und organisatorische Maßnahmen, Verarbeitung innerhalb EU/EWR

InterNetX GmbH

Anschrift / Sitz: Johanna-Dachs-Str. 55, 93055 Regensburg, Deutschland

Leistung: Domainregistrierung, Registry-/Registrar-Anbindung, Slave-DNS-Dienste

Ort der Verarbeitung: Deutschland / EU, je nach Registry ggf. weitere Staaten nach Domain-Endung

Datenschutzgarantien: Datenschutzvereinbarungen, Registry-/Registrar-Vorgaben, geeignete Garantien nach Art. 44 ff. DSGVO soweit erforderlich

WHMCS Limited

Anschrift / Sitz: 13th Floor, One Angel Court, London EC2R 7HJ, Vereinigtes Königreich

Leistung: Softwarewartung und Herstellersupport für WHMCS; Zugriff auf Kundendaten nur im Support- oder Fehleranalysefall, soweit erforderlich

Ort der Verarbeitung: Vereinigtes Königreich

Datenschutzgarantien: Datenschutzvereinbarungen, EU-Angemessenheitsbeschluss für das Vereinigte Königreich bzw. geeignete Garantien nach Art. 44 ff. DSGVO soweit erforderlich

WebPros International GmbH / Plesk

Anschrift / Sitz: Vordergasse 59, 8200 Schaffhausen, Schweiz

Leistung: Softwarewartung und Herstellersupport für Plesk; Zugriff auf Kundendaten nur im Support- oder Fehleranalysefall, soweit erforderlich

Ort der Verarbeitung: Schweiz

Datenschutzgarantien: Datenschutzvereinbarungen, EU-Angemessenheitsbeschluss für die Schweiz bzw. geeignete Garantien nach Art. 44 ff. DSGVO soweit erforderlich

E-Mail, DNS, Monitoring, Ticketing, Backup und Listmonk werden derzeit selbst betrieben, soweit nicht in dieser Anlage anders angegeben. Die selbst betriebenen Systeme laufen auf Infrastruktur von Hetzner Online GmbH. Externe Ticket- oder Monitoringdienste werden derzeit nicht eingesetzt.

Anlage 3 - Weisungsberechtigte Personen

Auftraggeber

vom Auftraggeber zu benennen; sofern keine gesonderte Benennung erfolgt, gelten die im Kundenkonto hinterlegten Vertrags-, Admin- oder technischen Kontakte als weisungsberechtigt

Funktion: weisungsberechtigte Person

E-Mail: gemäß Kundenkonto oder gesonderter Benennung

Telefon: gemäß Kundenkonto oder gesonderter Benennung

Auftragnehmer

Kai Plückhahn

Funktion: Geschäftsführung / vertretungsberechtigte Person

E-Mail: info@kairo.digital

Telefon: siehe Impressum

Änderungen der weisungsberechtigten Personen sind der jeweils anderen Partei unverzüglich in Textform mitzuteilen.

Anlage 4 - Leistungsbeschreibung und Verarbeitungskategorien

Diese Anlage beschreibt die Auftragsverarbeitung produkt- und leistungsübergreifend. Art und Umfang der konkreten Verarbeitung bestimmen sich durch die vom Auftraggeber beauftragten Leistungen, die Produktwahl, die Konfiguration, die Nutzung der Dienste und die vom Auftraggeber eingebrachten Daten.

Beauftragte Leistung

Die beauftragten Leistungen können insbesondere Hosting, Webhosting, Managed Hosting, Serveradministration, Domainregistrierung, DNS-Betrieb, Mailhosting, Datenbankbetrieb, Website-Betrieb, Wartung, Migration, Monitoring, Security-Hardening, Backup-Betrieb, technischen Support und technische Beratung umfassen.

Systeme und Dienste

- Domains und DNS-Zonen
- Web-, Mail-, Datenbank- und Applikationsserver
- Hosting- und Verwaltungsplattformen, insbesondere WHMCS und Plesk
- Websites, Shops, Portale, Content-Management-Systeme und sonstige Anwendungen
- Datenbanken, Dateiablagen, E-Mail-Postfächer und Backups
- Monitoring-, Logging-, Sicherheits- und Supportsysteme

Verarbeitungskategorien

- Datenarten: Stammdaten, Kontaktdaten, Vertrags- und Abrechnungsdaten, Inhaltsdaten, Nutzungs-, Verbindungs- und Protokolldaten, technische Metadaten, Support- und Kommunikationsdaten sowie sonstige Daten, die der Auftraggeber in die beauftragten Systeme einbringt.
- Betroffenengruppen: Kunden, Interessenten, Beschäftigte, freie Mitarbeiter, Erfüllungsgehilfen, Website-, Shop-, Portal-, E-Mail- und IT-Systemnutzer, Kommunikationspartner sowie sonstige Personen, deren Daten der Auftraggeber in die beauftragten Systeme einbringt.
- Zwecke: Erbringung, Betrieb, Wartung, Absicherung, Fehleranalyse, Support, Migration, Backup, Wiederherstellung, Dokumentation und technische Weiterentwicklung der beauftragten Leistungen.
- Besondere Kategorien nach Art. 9 DSGVO: werden nur verarbeitet, wenn und soweit der Auftraggeber solche Daten in die beauftragten Systeme einbringt oder deren Verarbeitung ausdrücklich beauftragt.
- Drittlandtransfer: erfolgt nur, soweit dies für einzelne Leistungen, Registries, Supportfälle oder Unterauftragnehmer erforderlich ist und die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

Ansprechpartner

- Ansprechpartner Auftraggeber: siehe Anlage 3
- technischer Ansprechpartner Auftragnehmer: Kai Plückhahn, info@kairo.digital
- Datenschutzkontakt: info@kairo.digital