

**Vertrag zur Auftragsdatenverarbeitung
i.S.d. Artikel 28, Absatz 3 Datenschutz-Grundverordnung (DS-GVO)**

Vertragsparteien

Auftragsverarbeiter vulgo „Auftragnehmer“

echonet communication GmbH

1010 Wien, Rosenbursenstraße 2, Top 24

Österreich

Telefon: +43 1 512 26 95

E-Mail: office@echonet.at

Internet: <https://www.echonet.at>

Firmenbuchnummer: FN 241662K, Handelsgericht Wien

UID-Nummer: AT U57632823

Verantwortlicher vulgo „Auftraggeber“

Firma, Anschrift, Firmenbuchnummer, UID-Nummer, Verantwortliche Person mit Kontaktangaben.

[1] Präambel / Gegenstand der Vereinbarung

1. Gegenstand dieses Auftrages ist die Durchführung von Datenverarbeitungen im Auftrag des Auftraggebers durch den Auftragnehmer, insbesondere der technische Betrieb von Web-Services und Webseiten sowie die Verarbeitung von Daten für vom Auftraggeber beauftragte Leistungen. Diese Vereinbarung gilt als Ergänzung zu bestehenden Verträgen zwischen Auftraggeber und Auftragnehmer.
2. Dieser Vertrag konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus den aufgelisteten und in ihren Einzelheiten beschriebenen Auftragsverarbeitungen ergeben. Er findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer beauftragte Unternehmen und Personen personenbezogene Daten des Auftraggebers verarbeiten.
3. Folgende Datenkategorien werden verarbeitet: Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bonitätsdaten, Bestelldaten, Entgeltkosten, Content in Text, Bild, Ton, Video und sonstiger Multimediaanwendungen für Webseiten und Webservices.

4. Folgende Kategorien betroffener Personen unterliegen der Verarbeitung: Kunden, Interessenten, Lieferanten, Ansprechpartner, Beschäftigte.

[2] Dauer der Vereinbarung

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von einem Monat zum Kalendervierteljahr gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt davon unberührt.

[3] Pflichten des Auftragnehmers

1. Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen 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 von personenbezogenen Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages durch den Auftraggeber.
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. Auch bleibt die Verschwiegenheitsverpflichtung gegenüber allen Subunternehmen nach Beendigung der Zusammenarbeit entsprechend aufrecht.
3. Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Artikel 32 DS-GVO ergriffen hat. Einzelheiten sind der „Anlage A“ (Serverinfrastruktur) und „Anlage B“ (Lokale Infrastruktur auf den Arbeitsplätzen des Auftragnehmers) zu entnehmen.
4. Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Personen nach Kapitel III der DS-GVO (Information, Auskunft, Berichtigung und Löschung, 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 betriebenen Datenanwendung 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 Artikeln 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzung 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 hat ein für die vorliegende Auftragsverarbeitung geltendes Verarbeitungsverzeichnis nach Artikel 30 DS-GVO zu errichten.
7. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. 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 bzw. in dessen Auftrag zu vernichten. 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 Mitgliedsstaaten.

[4] Ort der Durchführung der Datenverarbeitung

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraumes (EWR) durchgeführt.

[5] Subauftragnehmer

Der Auftragnehmer kann Sub-Auftragsverarbeiter für den technischen Betrieb (z.B. Hosting, Servermanagement, Betrieb der Serverinfrastruktur oder technische Arbeiten am Datenverarbeitungspunkt des Auftraggebers) hinzuziehen. Er 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 einght, 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.

[6] Verpflichtungen des Auftraggebers

1. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Artikel 4, Absatz 7, DS-GVO).
2. Die Verpflichtungen des Auftraggebers („Verantwortlicher“) sind in der Datenschutz-Grundverordnung geregelt. Die folgende Aufzählung soll nur spezifischer erklärend dienen.
3. Für die Wahrung der Rechte von betroffenen Dritten ist allein der Auftraggeber verantwortlich.
4. Die Weisungen des Auftraggebers werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. In Eilfällen können Weisungen auch mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen bzw. rückbestätigen, wenn vorab eine schriftliche Bestätigung des Auftragnehmers an den Auftraggeber über die Weisung und Durchführung der Weisung ergeht.
5. Der Auftraggeber nennt dem Auftragnehmer einen Ansprechpartner samt Kontaktmöglichkeiten (Telefonnummer, E-Mail-Adresse) für im Rahmen des Vertrages anfallende Datenschutzfragen. Der vom Auftraggeber genannte Ansprechpartner ist am Ende dieses Vertrages ersichtlich. Der Auftraggeber ist dafür verantwortlich, einen Wechsel dieses Ansprechpartners unverzüglich dem Auftragnehmer bekanntzugeben.
6. Betrieb von Webseiten / Services auf der Infrastruktur des Auftragnehmers
Insbesondere hinsichtlich des Betriebes von Internetauftritten durch den Auftragnehmer oder seine Subunternehmer durch Weisung des Auftraggebers gilt:
 - a. Die Einbindung von externen Services in Websysteme wie beispielsweise aber nicht ausschließlich externe Statistik-Systeme oder von externen Quellen bezogene Schriftarten sowie Social Plugins, Embedded Video-Player etc erfolgt durch Beauftragung des Auftraggebers. Die dadurch übermittelten Daten, die teilweise auch außerhalb der Europäischen Union oder des EWR landen können, liegen damit auch im alleinigen Verantwortungsbereich des Auftraggebers.
 - b. Für alle eingetragenen Daten, egal ob über Schnittstellenfunktionen oder über Zugang zu Datenbank oder Content-Management-System oder andere Eintragungsmöglichkeiten durch den Auftraggeber, die der Auftraggeber vornimmt, ist der Auftraggeber alleine verantwortlich.

7. Nutzung von Software-Services auf der Infrastruktur des Auftragnehmers

Insbesondere hinsichtlich der Nutzung von „Software as a Service“-Produkten (wie z.B. das Einladungsmanagementsystem „invite.life“, aber nicht ausschließlich) des Auftragnehmers durch den Auftraggeber gilt:

- a. Der Auftragnehmer ist für die Datenübermittlung im Rahmen von Statistik-Systemen, die der Auftragnehmer implementiert hat und die durch den Auftraggeber nicht beeinflusst werden können oder ohne dessen explizite Weisung eingebaut wurden, ist der Auftragnehmer verantwortlich.
- b. Für alle eingetragenen Daten, egal ob über Schnittstellenfunktionen oder über Zugang zu Datenbank oder Systemoberflächen, die der Auftraggeber vornimmt, ist der Auftraggeber alleine verantwortlich.
- c. Für alle eingetragenen Daten, die vom Auftraggeber dem Auftragnehmer mit Weisung der Eintragung der Daten übermittelt werden – wenn also von Seiten des Auftragnehmers auf Weisung des Auftraggebers eine Dateneinspielung vorgenommen wird – ist ebenfalls der Auftraggeber verantwortlich.

8. Nutzung von eigener oder durch den Auftraggeber selbst beauftragter technischer Infrastruktur

Insbesondere hinsichtlich der Auftragsverarbeitung durch en Auftragnehmer allerdings ohne physikalischen Zugriff des Auftragnehmers oder eines seiner Subunternehmer auf die technische Infrastruktur, hat der Auftraggeber selbst mit seinem dafür zuständigen Auftragnehmer eine entsprechende Datenschutzvereinbarung zu treffen. Für diesen Fall entfällt auch die Gültigkeit des „Anlage A“, da es Sache des Auftraggebers ist selbst mit seinem dafür zuständigen Auftragnehmer entsprechende Vereinbarungen zu treffen.

[7] Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die Daten des Auftraggebers beim Auftragnehmer oder einem seiner Subauftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. echonet, der Auftragnehmer, wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der DS-GVO liegen.
2. Änderungen und Ergänzungen dieses Vertrages und seiner Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers bedürfen der Schriftform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung handelt. Ein elektronisches Format (Textform) ist zulässig. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

3. Bei etwaigen Widersprüchen zwischen den Regelungen dieses Auftragsvertrages zum Datenschutz und den Datenschutz-Regelungen des Servicevertrages / Auftrages gehen die Regelungen dieses Auftragsvertrages vor. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht.
4. Es gilt österreichisches Recht.
5. Gerichtsstand für etwaige Streitigkeiten ist das zuständige Gericht am Gerichtsstandort des Auftragnehmers.

[8] Kontaktpersonen

Kontaktperson beim Auftragnehmer

Für datenschutzrechtliche Fragen oder datenschutzrechtliche Nachfragen aus diesem Vertrag wird beim Auftragnehmer genannt:

- Herr Roland Vidmar
- Büroanschrift: Rosenbursenstraße 2, Top 24, 1010 Wien, Österreich
- Kontaktangaben
 - Telefon: +43 1 512 26 95
 - E-Mail-Adresse: vidmar@echonet.at

Kontaktperson beim Auftraggeber

Für datenschutzrechtliche Fragen oder datenschutzrechtliche Nachfragen aus diesem Vertrag wird beim Auftraggeber genannt:

Zu diesem Vertrag gehören die „Anlage A“ und die „Anlage B“ sofern zutreffend, diese sind im Vertragsdokument (PDF) enthalten.

Unterschriften

Für den Auftraggeber (Verantwortlicher)

Für den Auftragnehmer (Auftragsdatenverarbeiter)

Datum, Ort, Unterschrift

Wien, _____ 2018, Unterschrift

Anlage A

Technische und Organisatorische Maßnahmen zum Datenschutz bei echonet-Serverumgebungen. Zutreffend für alle Vertragspartner, die ein System von echonet nutzen und es auf der Infrastruktur von echonet betreiben (lassen). Technische und organisatorische Maßnahmen gem. Artikel 32, Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30, Abs. 2 lit. d).

Technischer Zulieferer

Technischer Lieferant und Zurverfügungsteller der echonet-Infrastruktur ist:

KAPPER NETWORK-COMMUNICATIONS GmbH, 1090 Wien, Alserbachstraße 11/6

Das Unternehmen hat eine interne Information Security Policy (ISecP) basierend auf der Norm ISO 27000ff eingeführt und auf den von uns für unsere Auftraggeber genutzten Systemen („Managed Services“) auf der Hardware umgesetzt. Außerdem verfügt das Unternehmen über eine Zertifizierung TÜV Qualitätsmanagement nach ISO 9001.

Zutrittskontrollen

- Zugangskontrollsystem
 - Sicherheitsschlüssel mit Schlüsselregelung
 - Elektronische Türöffner
 - Videoüberwachung
 - Festgelegte Sicherheitszonen.

Zugangskontrolle & Zugriffskontrolle

- Kennwörter einschließlich entsprechender Policy
- Automatische Sperrmechanismen
- Verschlüsselung von Datenträgern
- Einsatz von VPN-Technologie
- Standard-Berechtigungsprofile auf „Need to Know-Basis“
- Standardisierter Prozess für Berechtigungsvergabe
- Protokollierung von Zugriffen
- Periodische Überprüfung von vergebenen Berechtigungen insbesondere administrativer Benutzerkonten

Integrität

- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport
- Verschlüsselung, Virtual Private Networks (VPN) und elektronische Signatur

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

Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle und Wiederherstellbarkeit: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.
- Backup-Strategie (On-Site und teilw. Off-Site)
- Unterbrechungsfreie Stromversorgung
- Regelmäßige Updates der Systeme
- Virenschutz
- Firewall
- Medlewege und Notfallpläne
- Security Checks auf Infrastruktur- und Applikationsebene
- Mehrstufiges Sicherungskonzept mit Auslagerung der Sicherungen i ein Auswiesrechenzentrum
- Standardprozesse bei Wechsel / Ausschreiben von Mitarbeitern

Anlage B

Technische und Organisatorische Maßnahmen zum Datenschutz bei echonet. Zutreffend für alle Vertragspartner, die im Datenaustausch mit echonet stehen oder zu Zwecken der Bearbeitung und Wartung eines Softwaresystems an echonet entsprechende Zugangsdaten und/oder Datenmaterial übermitteln.

Technische und organisatorische Maßnahmen gem. Artikel 32, Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30, Abs. 2 lit. d).

Verwehrung des Zugangs zu Verarbeitungsanlagen für Unbefugte

- Zutrittskontrolle mit Sicherheitsschlüssel zu den Büroanlagen von echonet / Verspernte Eingangstür
- Alarmanlage mit Türkontrolle und Bewegungsmelder

Technische Maßnahmen

- Verfahren zur User-Anmeldung und Abmeldung auf allen Geräten (Servern und Client-Geräten)
- Verwaltung von Administrationsrechten nach dem „Need to Know-Prinzip“
- Technische Passwortvergaben
- Speichermedien werden sicher aufbewahrt
- Kopien von Datenmaterial werden dokumentiert und kontrolliert
- Speicherungen erfolgen verschlüsselt
- Entsorgung von Geräten mit Speichermedien erfolgt datenschutzkonform
- Löschung von Speichermedien und Wiederverwenden von Speichermedien erfolgt datenschutzkonform
- Nutzerverhalten im Zusammenhang mit Daten von Auftraggebern wird protokolliert
- Bildschirme und Endgeräte der Nutzer verfügen über eine automatische Passwort-Sperrung („Bildschirmschoner“)
- Administrations-Bereich im Unternehmen ist getrennt vom Produktionsbereich
- Technische Installationen vor Ort:
 - Firewall
 - Virenschutz
 - Passwörter werden gesichert und nicht im Klartext verfügbar gemacht
 - Zugangsberechtigungen zu Daten sind einzeln an Personen vergeben

Organisatorische Maßnahmen

- Besucher werden am Betriebsgelände nicht unbeaufsichtigt gelassen
- Kein Zugang zu Aktenmaterial und Datenmaterial in den Räumen in denen Besucher unbeaufsichtigt sein könnten.

- Protokollierung der Besuche im Zusammenspiel mit Terminvergaben, Identifizierung der Besucher, namentliche Aufzeichnung des Besuchers und des Gesprächspartners bei echonet