**Vertrag**

Vereinbarung über eine Auftragsverarbeitung gemäß Art. 28 DSGVO

|  |  |
| --- | --- |
| Der Verantwortliche:<Firma XYZ>(im Folgenden Auftraggeber) | Der Auftragsverarbeiter:tethis IT e.U.Lindengasse 56/18-191070 Wien(im Folgenden Auftragnehmer) |

1. **Gegenstand der Vereinbarung**

**(1) Gegenstand**

Der Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

* Betreuung der IT Systeme des Auftraggebers in Hinsicht auf Hardware, Software oder Bedienungsfragen
* Betreut werden Geräte an allen Standorten des Auftraggebers inkl. Home-Office statt.
* Die Betreuung findet wahlweise vor Ort oder per Fernwartung mittels TeamViewer oder VPN statt
* Unterstützung in Bezug auf Microsoft Office 365
* Betreuung der Webseite https://www.daunenspiel.at und des dort integrierten Webshops
* Sicherung der Daten des Auftraggebers über das Internet auf den Systemen des Auftragnehmers
* Hosting einer Webseite

Der Gegenstand des Auftrags ergibt sich aus dem IT Betreuungsvertrag vom 28.2.2018, der Bestellung eines Webhosting-Pakets vom 25.1.2018 sowie des angenommenen Angebots für Datensicherung vom 29.6.2017 auf die hier verwiesen wird. Diese Vereinbarung ist als Ergänzung zu verstehen.

**(2) Art und Zweck der Verarbeitung von Daten**

Nähere Beschreibung des Auftrages in Hinblick auf Art und Zweck der vorgesehenen Verarbeitung durch den Auftragnehmer:

* IT Betreuung
Der Auftragnehmer führt im Auftrag des Auftraggebers Wartungs- und/oder Pflegearbeiten an IT-Systemen des Auftraggebers durch. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogene Daten bekommt bzw. Kenntnis erlangt oder personenbezogene Daten verarbeitet, um die Wartung und Pflege von IT-Systemen durchzuführen oder durchführen zu können.
* Datensicherung
Der Auftragnehmer sichert im Auftrag des Auftraggebers Daten. Die Daten werden in der Infrastruktur des Auftragnehmers gespeichert.
Die Daten werden vor der Übertragung verschlüsselt und keinesfalls im Klartext über das Internet übertragen oder auf den Systemen des Auftragnehmers gespeichert.
Bei den zu sichernden Daten kann es sich auch um personenbezogene Daten handeln, allerdings kann der Auftragnehmer die Daten weder lesbar machen noch einer Person zuordnen
* Webhosting
Der Auftragnehmer stellt die Infrastruktur für die Webseite daunenspiel.at bereit, betreut und wartet das installierte Content Management System Wordpress sowie den integrierten Webshop. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogene Daten bekommt bzw. Kenntnis erlangt oder personenbezogene Daten verarbeitet, um die Wartung und Pflege der Webseite und des Webshops durchzuführen oder durchführen zu können.

**(3) Art der Daten**

Im Rahmen der Ausführung des Auftrags ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf folgende Datenkategorien hat:

* Zugangsdaten (Username, Passwörter, asymmetrische Schlüssel-Paare) für die vom Auftragnehmer verwendeten IT Systeme und Lösungen
* Name, Anschrift, Bankverbindungen, UIDs, Umsätze von Kunden und Lieferanten
* Geburtsdatum, Personenstand, Staatsbürgerschaft, Bankverbindung von Mitarbeitern
* E-Mail Adressen und E-Mails
* IP-Adressen von Besuchern der Webseite

**(3) Kategorien betroffener Personen**

Folgende Kategorien betroffener Personen unterliegen der Verarbeitung

* Kunden
* Lieferanten
* Interessenten
* Mitarbeiter
* Auftraggeber
1. **Dauer der Vereinbarung**

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von 4 Wochen zum Ende eines Kalendermonats gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

1. **Pflichten des Auftragnehmers**
2. Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
3. 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 schriftlichen Auftrages.
4. Wahrung der Vertraulichkeit und Verschwiegenheit: 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.
5. Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32ff DSGVO ergriffen hat. Konkret handelt es sich hierbei um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Einzelheiten hierzu finden sich im Anhang (Technisch-organisatorische Maßnahmen).
6. Mitwirkungspflicht bei Betroffenenrechten: Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Betroffenenrechte 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.
Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.
7. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenübertragung und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer durchzuführen (sicherzustellen).
8. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten. Dazu gehören 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.
9. Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu erstellen hat.
10. 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.
11. Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, sämtliche in seinem Besitz gelangten Unterlagen, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber zu übergeben oder 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.
Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.
12. 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.
13. **Technisch-organisatorische Maßnahmen**

Die technischen und organisatorischen Maßnahmen (TOMs) unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

Einzelheiten sind dem Anhang zu entnehmen.

1. **Ort der Durchführung der Datenverarbeitung**

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.

1. **Sub-Auftragsverarbeiter**

Der Auftragnehmer kann Sub-Auftragsverarbeiter zur unmittelbaren Erbringung der Hauptdienstleistung hinzuziehen

Die Auslagerung auf folgende Unterauftragnehmer ist gestattet:

* Cyberwebhosting, Hamburg, Deutschland (Infrastruktur für Webhosting)
* IPAX, Wien, Österreich (Infrastruktur für Datensicherung)
* IP-Interactive, Frankfurt, Deutschland (Redundante Infrastruktur für Datensicherung)
* LogMeIn Ireland Ltd., Dublin, Irland (verschlüsselter Speicher für Zugangsdaten)
* Microsoft Europe Ltd., Dublin, Irland (Infrastruktur Microsoft Office 365, E-Mail, Cloud-Speicher)

Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

* der Auftragnehmer dies dem Auftraggeber eine angemessene Zeit vorab schriftlich anzeigt und
* der Auftraggeber nicht gegenüber dem Auftragnehmer schriftlich Einspruch gegen die geplante Auslagerung erhebt und
* die erforderlichen Vereinbarungen zwischen dem Auftragnehmer und dem Sub-Auftragsverarbeiter gemäß des Art. 28 Abs. 4 DSGVO abgeschlossen werden.

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], am [Datum]Für den Auftraggeber:....................................................[Name samt Funktion] | [Ort], am [Datum]Für den Auftragnehmer:....................................................[Name samt Funktion] |

**Anhang – Technisch-organisatorische Maßnahmen (TOMs) [[1]](#footnote-1)**

**Vertraulichkeit**

* Zutrittskontrolle: Verschlossene Arbeitsräume. Rechenzentren der Sub-Auftragsverarbeiter sind durch Zutrittskontrollsysteme geschützt und nur nach Voranmeldung zugänglich. Nähere Informationen sind vom Sub-Auftragsverarbeiter erhältlich.
* Zugangskontrolle: Schutz aller verwendeten Systeme mit unterschiedlichen Passwörtern mit mindestens 12 Stellen und Ziffern, Buchstaben und Sonderzeichen, asymmetrischen Schlüssel-Paaren oder Zwei-Faktor-Authentifizierung.
Alle mobilen oder stationären Geräte die nicht ausschließlich privat verwendet werden und nicht in einem Rechenzentrum untergebracht sind, verfügen über verschlüsselte Datenträger. Mobile Datenträger (USB Sticks) werden nur im Notfall und verschlüsselt verwendet.
* Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, Vergabe für Berechtigungen für Mitarbeiter auf „need to know-Basis“, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten;
* Trennungskontrolle: Daten der Webseiten und der Datensicherungen des Auftraggebers sind durch entsprechende Berechtigungen für andere Kunden nicht zugänglich.
* Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
* Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich). Alle Daten der Kunden, Mitarbeiter oder Lieferanten des Auftraggebers werden grundsätzlich als geheim eingestuft.

**Integrität**

* Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung (Verwendung der https oder ssl Protokolle), Virtual Private Networks (VPN), elektronische Signatur;

**Verfügbarkeit und Belastbarkeit**

* Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch tägliche Sicherungen der auf den Systemen des Auftragnehmers gespeicherten Daten des Auftraggebers, mit Ausnahme der Datensicherungen des Auftraggebers, die durch einen redundanten Sicherungs-Server geschützt werden. Die Datensicherungen des Auftragnehmers werden unter Nutzung von tethis CDS off-site, also in einem Rechenzentrum in Wien gespeichert. Die Geräte des Auftraggebers sind durch Virenscanner, eine Firewall und automatische Updates geschützt.
* Die Daten der Datensicherungen sind durch Redundanz bei Ausfall eines Servers weiterhin verfügbar. Die Daten des Webhostings können innerhalb von 6 Stunden wiederhergestellt werden. Die auf den lokalen Systemen gespeicherten Daten sind in sicheren Cloud-Lösungen gespeichert und sind von lokalen Hardware-Ausfällen nicht betroffen.
* Löschungsfristen: Alle Daten des Auftragnehmers werden sofort nach Ende des Vertrages gelöscht oder auf Wunsch an den Auftraggeber übergeben, sofern keine gesetzlichen Vorschriften oder laufende juristische Verfahren existieren, die eine Aufbewahrung nötig machen. Anfallende Meta-Daten (Logfiles) des Webhostings werden nach 3 Monaten gelöscht. Logfiles der Datensicherung werden je nach konfigurierten Aufbewahrungsfrist für gelöschte Dateien aufbewahrt und anschließend gelöscht, jedoch spätestens nach einem Jahr.

**Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

* Die Maßnahmen zum Datenschutz werden kontinuierlich überprüft und jährlich evaluiert.
* Der Auftragnehmer verpflichtet sich zur Teilnahme an regelmäßigen Schulungen zum Thema Datenschutz und zur Beobachtung relevanter Mitteilungen der Presse oder der Datenschutzbehörde
* Die Konfiguration der benutzten Software sowie die Auswahl neuer Lösungen wird unter Beachtung des bestmöglichen Datenschutzes vorgenommen.
* Es findet keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers statt. Dies wird durch eindeutige Vertragsgestaltung und vorab genehmigte Auswahl von Sub-Auftragsverarbeitern erreicht.
1. [↑](#footnote-ref-1)