# **Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO**

zwischen

**[NAME DES KUNDEN]**

[Adresse des Kunden]

im Folgenden <Auftraggeber>

und

ExaMesh GmbH

Reiterweg 2, 86972 Altenstadt

im Folgenden <Auftragnehmer>

**Präambel**

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der Auftragsdatenverarbeitung des Auftragnehmers für den Auftraggeber auf Grundlage des zwischen den Parteien geschlossenen Hostingvertrags (im Folgenden: Hauptvertrag) ergeben. Sie finden Anwendung auf alle Tätigkeiten, die mit der Auftragsdatenverarbeitung in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

**§ 1 Gegenstand des Auftrages und Konkretisierung des Auftragsinhalts durch Weisungen**

(1) Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers. Art und Zweck dieser Datenverarbeitung sowie die Betroffenen dieser Datenverarbeitung einschließlich der betroffenen Datenarten ergeben sich aus Anlage 1 zu diesem Vertrag sowie aus dem Hauptvertrag.

(2) Der Auftraggeber ist berechtigt, dem Auftragnehmer Weisungen hinsichtlich der Datenverarbeitung zu erteilen. Weisungen sind grundsätzlich in Textform zu erteilen. Werden Weisungen ausnahmsweise mündlich erteilt, sind sie unverzüglich nachträglich vom Auftraggeber schriftlich in Textform zu dokumentieren. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen die vertragsgegenständlichen Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften.

**§ 2 Pflichten des Auftragnehmers**

(1) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen.

(2) Der Auftragnehmer wird bei der Durchführung der Arbeiten nur Mitarbeiter einsetzen, die er mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut gemacht hat und in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO, § 53 BDSG).

(3) Der Auftragnehmer hat die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung hinsichtlich der konkreten Auftragsdurchführung in Anlage 2 dokumentiert. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

(4) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(5) Der Auftragnehmer wird den Auftraggeber dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von datenschutzrechtlichen Rechten Betroffener nachzukommen und wird ihn bei der Einhaltung seiner datenschutzrechtlichen Pflichten aus Art. 32-36 der Datenschutzgrundverordnung unterstützen und ihm alle erforderlichen Informationen zur Einhaltung der in Art. 28 Datenschutzgrundverordnung niedergelegten Pflichten zur Verfügung stellen.

(6) Der Auftragnehmer wird dem Auftraggeber jederzeit auf Anfrage über Person und Kontaktdaten des betrieblichen Datenschutzbeauftragten des Auftragnehmers informieren.

**§ 3 Kontrollen des Auftraggebers und von Aufsichtsbehörden**

(1) Sollten im Einzelfall Kontrollen der technischen organisatorischen Maßnahmen hinsichtlich der vertragsgegenständlichen Daten durch den Auftraggeber erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt.

(2) Der Auftragnehmer darf die Durchführung von Kontrollen von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen, wenn nicht der Auftraggeber einen von Gesetzes wegen und/oder berufsrechtlich zur Verschwiegenheit verpflichteten Prüfer mit der Durchführung der Kontrolle beauftragt.

(3) Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(4) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Kontrolle der vertragsgegenständlichen Datenverarbeitung durchführen wollen, wird der Auftragnehmer den Auftraggeber hierbei unterstützen. Die vorstehenden Absätze gelten entsprechend.

**§ 4 Berichtigung, Einschränkung und Löschung von Daten**

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nur löschen oder deren Verarbeitung einschränken, wenn dies im Hauptvertrag oder in diesem Vertrag über die Auftragsdatenverarbeitung vorgesehen ist oder der Auftraggeber eine entsprechende Weisung erteilt. Soweit eine betroffene Person sich mit einem Löschbegehren unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Der Auftragnehmer wird nach Ende dieses Vertrags alle vertragsgsgegenständlichen personenbezogenen Daten nach Wahl des Auftraggebers entweder löschen oder zurückgeben, soweit nicht nach dem Unionsrecht oder dem deutschen Datenschutzrecht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(3) 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.

**§ 5 Unterauftragsverhältnisse**

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) beauftragen, wenn diese Ihren Sitz innerhalb der Europäischen Union haben und der Auftragnehmer mit diesen einen Vertrag über die Auftragsverarbeitung geschlossen hat.

**§ 6 Haftung**

Die Haftung richtet sich nach Art. 82 der DS-GVO.

**§ 7 Vergütung**

Die Vergütung aller Arbeiten des Auftragnehmers ist nicht Bestandteil dieses Vertrages über die Auftragsverarbeitung, sondern richtet sich allein nach dem Hauptvertrag, soweit nicht nachfolgend Abweichendes bestimmt ist.

**§ 8 Laufzeit und Ersetzung etwaiger vorbestehender Verträge über die Auftragsdatenverarbeitung**

Der Auftrag gilt in dieser Form ab Unterzeichnung und endet mit der vollständigen Durchführung der in Anlage 1 beschriebenen Maßnahmen, ohne dass es einer Kündigung durch eine der Parteien bedürfte oder mit der Beendigung des diesem Vertrag zugrundeliegenden Hauptvertrags.

**§ 9 Schlussbestimmungen**

(1) Änderungen und Ergänzungen dieses Vertrags über die Auftragsdatenverarbeitung und aller ihrer Bestandteile bedürfen Vereinbarung in Schriftform oder in Textform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts (CISG) und des deutschen internationalen Privatrechts.

\_\_\_\_\_\_\_\_\_\_\_, **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Ort, Datum Name in Blockschrift und Unterschrift Auftraggeber

\_\_\_\_\_\_\_\_\_\_\_, **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Ort, Datum Name in Blockschrift und Unterschrift Auftragnehmer

**Anlage 1:** Auflistung der beauftragten Dienstleistungen (Umfang, Art, Zweck der Erhebung, Verarbeitung, Nutzung von Daten, Art der Daten, Kreis der Betroffenen)

|  |  |  |  |
| --- | --- | --- | --- |
| **Art der Dienstleistung** | **Art der Verarbeitung** | **Datenarten** | **Kreis der Betroffenen** |
| Bereitstellung von Instanzen auf einem Server | Die Verarbeitung durch den Auftragnehmer beschränkt sich auf die Bereitstellung der Instanzen, die ausschließlich vom Kunden verwaltet werden. | (z.B. Name, Email-Adresse Telefonnummer, Beruf, Einkommen, Portraitfotos); vom Kunden zu ergänzen | (z.B. Mitarbeiter des Kunden; Kunden des Kunden usw); vom Kunden zu ergänzen |

# **Anlage 2 – Technisch-organisatorische Maßnahmen**

## 1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

1. Zutritt zum Gebäude nur mit Schlüssel. Besucher müssen klingeln.
2. Bürobereich nicht allgemein zugänglich.

1.2 Zugangskontrolle

1. Ausschließlich persönliche Übergabe aller relevanten Passwörter durch IT-Leitung (Admin) an verantwortliche Mitarbeiter
2. Benutzeridentifikation durch persönlichen Login am Client
3. Automatische Bildschirmsperre nach 5 Minuten
4. Dienstanweisung zur manuellen Sperrung des Clients bei Verlassen des Arbeitsplatzes
5. Je nach Anzahl erfolgloser Anmeldeversuche zeitlich ansteigende Sperrung der Anmeldung mit einem Benutzernamen/Passwort
6. Passwortrichtlinie für alle Passwörter (mindestens 8 Zeichen, mindestens 1 Großbuchstabe; mindestens 1 Zahl)
7. Sicherung der Systeme über eine Firewall
8. Protokollierung aller Anmeldungen der letzten 30 Tage
9. Der Zugriff unserer Administratoren auf das Rechenzentrum ist über SSH (Secure Shell) mit einer private/public key Methode gesichert.
10. Automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware (z. B. Virenscanner)
11. Revisionssicheres, verbindliches Verfahren zur Rücksetzung „vergessener“ Passwörter
12. Eindeutige Zuordnung von Benutzerkonten zu Benutzern
13. Richtlinie zum sicheren, ordnungsgemäßen Umgang mit Passworten

1.3 Zugriffskontrolle

1. Es existiert ein Berechtigungskonzept nach dem need-to-know-Prinzip, dass den Zugriff von Mitarbeitern auf Daten von Auftraggebern regelt.
2. Protokollierung von Änderungen bei Zugriffsberechtigungen
3. Verbot der Verwendung von privaten Speichermedien in der IT-Umgebung des Auftragnehmers
4. Authentifizierung auf Betriebssystemebene erforderlich
5. Separate Authentifizierung und Berechtigungsvergabe auf Anwendungsebene
6. Protokollierung der Zugriffe durch Logfiles
7. Wiederherstellung von Daten aus Backup nur durch Mitarbeiter im IT-Team
8. Alle Netzwerklaufwerke sind verschlüsselt:

1.4 Trennungskontrolle

1. Es existiert ein Berechtigungskonzept, das der getrennten Verarbeitung von Daten des Auftraggebers von Daten anderer Kunden/Mandanten Rechnung trägt.
2. Die in den verwendeten Systemen verfügbaren Berechtigungsmechanismen ermöglichen die exakte Umsetzung der Vorgaben des Berechtigungskonzepts.

1.5 Pseudonymisierung

Um den Prinzipien „privacy by design“ und „Datensparsamkeit“ zu entsprechen kann die Option "Pseudonymisierung" in den Datenschutzeinstellungen aktiviert werden. Dies führt zur Unkenntlichmachung aller personenbezogenen Daten und Informationen, die nicht direkt zur Beantwortung der Nachricht notwendig sind.

## 2. Integrität des Systems

2.1 Weitergabekontrolle

1. Verschlüsselung von Daten auf dem Webportal über https /SSL
2. Protokollierung der Übertragungsvorgänge
3. Protokollierung von Datenübertragungen (30 Tage) durch Logfiles
4. IT-Security-Überprüfungen: regelmäßiger Penetration-Test der exponierten (von außen erreichbaren) Systeme.

2.2 Eingabekontrolle

1. Logfiles (mindestens 30 Tage)
2. Überwachung der Protokollierung: anlassbezogen (Troubleshooting) durch die Systemadministratoren
3. Passwort-Rücksetzung nur manuell durch Systemadministratoren (Archivierung über Ticket-System)

## 3. Verfügbarkeit und Belastbarkeit des Systems

1. Dokumentiertes Backup-Konzept und Recovery-Konzept mit täglicher Sicherung
2. Festplatten-Echtzeitspiegelung auf redundantem Server in einem separaten Rechenzentrum
3. Notstrom über Dieselaggregat für Server verfügbar
4. Sicherheit: Sicherheits-Update für Betriebssystem und für Programme wird regelmäßig aufgespielt
5. Sachkundiger Einsatz von IT-Security (Virenschutz; Verschlüsselung; Spam-Filter; Firewalls etc) und schriftliches Konzept des Einsatzes

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1. Datenschutz-Management

Schulungen durch externen Experten

1. Datenschutzfreundliche Voreinstellungen

Die Software wird standardmäßig so konfiguriert, dass alle personenbezogenen Daten, welche älter sind als 180 Tage automatisch gelöscht werden. Dieser Wert kann vom Auftraggeber in den Einstellungen gemäß den eigenen Wünschen tagesgenau angepasst werden.

1. Auftragskontrolle  
   Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.