EDIS Providing the Best

Vereinbarung

über eine

Auftragsverarbeitung nach Art. 28 EU – DSGVO

Der Verantwortliche:		Der Auftragsverarbeiter:
Firmenwortlaut:	Firmenwortlaut	**EDIS GmbH**
Verantwortlicher:	Verantwortlicher	Hauptplatz 3 / 3
Anschrift:	Anschrift	A – 8010 Graz
PLZ, Ort:	PLZ, Ort	
Land:	Österreich	
*(im Folgenden: **Auftraggeber**)*		*(im Folgenden: **Auftragnehmer**)*

PRÄAMBEL

EDIS GmbH erbringt für seine Kunden verschiedene Leistungen im Bereich IT-Infrastruktur.

Kerntätigkeit ist die **Zurverfügungstellung von Serverinfrastruktur und Dienstleistungen (Services) an seine Kunden.** Dazu werden Leistungen in folgenden Bereichen erbracht:

- **Domain** Registrierung
- **Webhosting** (Webserver, FTP-Server, Datenbank-Server)
- **eMail-Services** (Transport und Zustellung von eMails, Antivirus, Spamfilterung)
- Zurverfügungstellung einer **dedizierter Server Infrastruktur**
- Zurverfügungstellung von **virtuellen Server-Resourcen** (OpenVZ, KVM, VRS)

Um o.g. Leistungen für seine Kunden erbringen zu können, werden personenbezogene Daten (gem. Art. 4 Z1 DSGVO) dieser, verarbeitet.

Die Verarbeitung (gem. Art. 4 Z2 DSGVO) ist für die Erfüllung der **vertraglichen Vereinbarung** zwischen Auftraggeber und Auftragnehmer (EDIS) notwendig und ist aufgrund **einer zusätzlichen vorherigen Zustimmung** des Auftraggebers erfolgt (gem. Art. 6 Abs. 1 lit. a) und b)).

1. GEGENSTAND DER VEREINBARUNG

Diese Vereinbarung ist als **Ergänzung zum Leistungsvertrag** mit dem Auftragnehmer (EDIS) zu verstehen.

Ein Vertrag zwischen dem Auftragnehmer (EDIS) und dem Auftraggeber kommt in folgenden Fällen rechtlich zustande:

- wenn der Auftraggeber einen schriftlichen Vertrag mit dem Auftragnehmer (EDIS) abschließt, oder

- wenn der Auftraggeber zahlungswirksam über die Webseite des Auftragnehmers (EDIS) Leistungen bestellt.

Im ***ersten*** Punkt enthält der Auftraggeber neben dem Vertrag zur Leistungsvereinbarung auch diese Vereinbarung über eine Auftragsverarbeitung nach Art. 28 DSGVO.

Im ***zweiten*** Punkt wird der Auftraggeber bei der Online-Bestellung mittels ausdrücklichem Hinweis (AGBs, Nutzungsbedingungen) darauf hingewiesen, dass für die Bereitstellung der Leistungen durch den Auftragnehmer (EDIS) und somit der vertraglichen Erfüllung des Auftrags auch diese Vereinbarung über eine Auftragsverarbeitung nach Art. 28 DSGVO abgeschlossen wird.

(1) Gegenstand dieses Auftrages ist die Durchführung folgender vertraglich vereinbarten Leistungen:

- Zurverfügungstellung einer Serverinfrastruktur und ggf. Services;
- der Auftragnehmer verarbeitet zum Zweck der vorstehenden Leistungserbringung die Daten des Auftraggebers („Kundendaten“), um seine Leistungen abrechnen zu können bzw. die vom Kunden bestellten Leistungen erbringen zu können (z.B. eine Domain-Registrierung vornehmen zu können);
- für sämtliche anderweitigen Daten des Auftraggebers (Uploads von Daten auf die bereitgestellte Infrastruktur und die Nutzung der Services durch den Auftraggeber) ist dieser selbst verantwortlich. Der Auftragnehmer (EDIS) hat keinen unmittelbaren Zugriff, Berechtigung und/oder Beauftragung zur Verarbeitung anderer Daten als der Daten des Auftraggebers – es wird lediglich die Infrastruktur zur Verfügung gestellt.

(2) Folgende Datenkategorien werden verarbeitet: [*Datenkategorien*:].

- Geschlecht, Firmenname / Familienname, Vorname (bei natürlichen Personen), Titel, Adresse, Telefonnummer, E-Mail-Adresse (werden gem. DSGVO als **personenbezogene** Daten behandelt)
- Kreditkartendaten, Geburtsdaten (bei natürlichen Personen), Kontodaten (IBAN), Abbuchungsaufträge (werden gem. DSGVO als **sensible** Daten behandelt)

(3) Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:

- Kunden, Ansprechpartner

2. DAUER DER VEREINBARUNG

Die Vereinbarung wird auf **unbestimmte Zeit** abgeschlossen und ist unmittelbar mit dem Erwerb der Leistungen vom Auftragnehmer (EDIS) durch den Auftraggeber begründet.

Die Dauer dieser Vereinbarung ist mit der Dauer der Nutzung der Leistungen des Auftragnehmers (EDIS) gekoppelt.

Der Auftraggeber stimmt ausdrücklich überein, dass sich die Dauer dieser Vereinbarung auf die Dauer des bestehenden Leistungsvertrages bezieht und bei ausgelaufenen oder gekündigten Verträgen noch auf die vereinbarte Speicherdauer des Auftragnehmers (EDIS) erstreckt (vgl. dazu Anhang./1 – Abschnitt „Löschungsfristen“.

3. PFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse **ausschließlich im Rahmen der vereinbarten Leistungen des Auftraggebers zu verarbeiten**. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er – sofern gesetzlich zulässig bzw. falls keine andere Weisung von Behördenseite vorliegt (z.B. richterliche Verfügung, Befehl, Verordnung, u.ä)– den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen.

(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 (EDIS) **ergreift hinreichende technische und organisatorische 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 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 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 erklärt, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art. 30 DSGVO errichtet hat.

(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Prüfung der Datenverarbeitungseinrichtungen eingeräumt. Diese Prüfung kann durch ihn oder auch durch ihn beauftragte Dritte erfolgen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen in Schriftform zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind. Die Parteien kommen ausdrücklich überein, dass dieser Kontrollmöglichkeit seitens des Auftragnehmers (EDIS) in der Anlage ./1 dieser Vereinbarung vollständig entsprochen wird.

(8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten in dessen Auftrag zu löschen. Ausgenommen von der Löschung und/oder Vernichtung sind jene Daten, für die es anderweitige gesetzliche Aufbewahrungspflichten gibt. 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

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

Die Daten von Kunden und einige Dienstleistungen (Services) werden auf ausdrücklichen Wunsch und Bestellung des Auftraggebers und aufgrund einer vertraglichen Vereinbarung auch außerhalb der EU bzw. des EWR Raumes durchgeführt. Der Auftragnehmer (EDIS) handelt in diesen Fällen immer

und ausschließlich auf ausdrücklichen Wunsch und Bestellung des Auftraggebers. Davon unberührt bleibt die Regelung zur Verarbeitung der Kundendaten, die ausschließlich gem. Punkt 1 – Gegenstand der Vereinbarung aus diesem Vertrag verarbeitet werden.

5. SUB-AUFTRAGSVERARBEITER

Der Auftragnehmer ist nicht berechtigt, einen Sub-Auftragsverarbeiter heranzuziehen.

Beabsichtigte Änderungen hinsichtlich der Beschäftigung von Sub-Auftragsverarbeitern sind dem Auftraggeber rechtzeitig schriftlich bekannt zu geben, dass er diesen allenfalls widersprechen oder diese untersagen kann.

Bei einer Genehmigung durch den Auftraggeber ist der Auftragnehmer verpflichtet, die erforderlichen Vereinbarungen im Sinne des Art. 28 Abs. 4 DSGVO mit jeden einzelnen Sub-Auftragsverarbeiter abzuschließen. 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: Ort

Graz, am Datum: 08.05.2018

,

Datum: Datum

Für den Auftraggeber:

Name: Name
Funktion: Funktion

.....
[*Unterschrift*]

Für den Auftragnehmer:

Gerhard Kleewein
Geschäftsführer
EDIS GmbH

ANLAGE ./1 – TECHNISCH-ORGANISATORISCHE MASSNAHMEN

VERTRAULICHKEIT

- **Zutrittskontrolle:** Physischer Zugriff auf die Infrastruktur des Auftragnehmers (EDIS) erfolgt ausschließlich durch befugte Personen mittels Schlüssel bzw. elektrischem Türöffner und Fingerabdrucks-Sensoren (Zutritt zu den Räumlichkeiten). Zusätzlicher Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen gewährleisten Sicherheitspersonal und Alarmanlagen rund um die Uhr;
- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung bzw. Zugriff auf die Infrastruktur des Auftragnehmers (EDIS) erfolgt ausschließlich durch befugte Personen. Dabei kommen Sicherheitsprotokolle auf dem jeweiligen aktuellsten Stand der Technik zum Einsatz, ebenso wie ein VPN Zugriff und digitale Signaturen (geregelt durch die interne Security Policy);
- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „*need to know-Basis*“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb. von administrativen Benutzerkonten;
- **Pseudonymisierung**: die als sensibel eingestuften Daten (z.B. Kreditkartendaten) werden in der jeweiligen Datenanwendung gesondert, verschlüsselt und pseudonymisiert aufbewahrt.

INTEGRITÄT

- **Weitergabekontrolle**: der Auftragnehmer stellt die Infrastruktur zur Verfügung: es findet zu keinem Zeitpunkt ein Zugriff auf die Daten der Kunden auf der für den Auftraggeber bereitgestellten Infrastruktur statt. Dies ist technisch nicht bzw. nur mit erheblichen Aufwand möglich.
- **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: 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, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;
- **Wiederherstellbarkeit und Backup Policies**: um eine optimale Verfügbarkeit der Leistung für seine Kunden zu ermöglichen, nimmt der Auftragnehmer folgende Sicherungs- bzw. Backup Prozedere vor:
    - Laufende Verträge: im Bereich Webhosting und eMail-Services: Backups der letzten 40 Tage (ältere Daten als 40 Tage werden per Grundeinstellung gelöscht und sind nicht wiederherstellbar gem. Art. 25 Abs. 1 – Privacy by Design)

- Ausgelaufene oder gekündigte Verträge: Daten von Webseiten und Inhalte von eMail-Konten werden noch 3 Monate am Server und weitere 40 Tage auf Backups gespeichert. Nach dieser Frist werden Daten per Grundeinstellung gelöscht und sind nicht wiederherstellbar gem. Art. 25 Abs. 1 – Privacy by Design)

Protokolle auf Webservern und Loadbalancern (“Logdateien”) werden 10 Tage aufbewahrt. Die letzten 24 Stunden stehen dem Auftragnehmer im Klartext zur Verfügung. Historischen Logdateien (Stände vom Vortag bis incl. 10 Tage zurück) werden verschlüsselt gespeichert. Logdateien werden im Rahmen von Debugging und zur Fehlersuche herangezogen. Diese fallweise Verarbeitung erfolgt ausschließlich durch Mitarbeiter des Auftragnehmers. Logdateien sind getrennt von anderen Datenbanken und werden auch mit keinen Datenbanken zusammengeführt (“big data”). Logdateien die dem Auftraggeber zur Verfügung gestellt werden, enthalten keine personenbezogenen Daten, da IP-Adressen in der Detailschärfe reduziert sind (Entfernung des 4. Oktetts) und somit seitens des Auftraggebers keine Behandlung im Sinne der DSGVO erforderlich ist.

Protokolle auf Mailservern (“Logdateien”) werden 10 Tage aufbewahrt. Die letzten 24 Stunden stehen dem Auftragnehmer im Klartext zur Verfügung. Historische Logdateien (Stände vom Vortag bis incl. 10 Tage zurück) werden verschlüsselt gespeichert. Diese Logdateien werden mit keinen anderen Datenbanken verknüpft (“big data”) und dienen dazu, den Transport von eMails nachvollziehen zu können und damit verbundene Fehler auf dem Transportweg aufzeigen zu können. Diese fallweise Verarbeitung erfolgt ausschließlich durch Mitarbeiter des Auftragnehmers. Der Auftraggeber hat keinen Zugriff auf Logdateien, weshalb seitens des Auftraggebers keine Behandlung im Sinne der DSGVO erforderlich ist.

- **Löschungsfristen**: wie im vorangegangenen Punkt dargestellt. Die Löschung erfolgt für Backups und Logdateien per Grundeinstellung gem. Art. 25 – Privacy by Design, Privacy by Default.
  - ***Virtuelle Server „KVM“ und „VRS“*** werden nach einer Kündigung durch den Kunden (sofortige Wirkung oder per Stichtag) bzw. nach der ersten unbezahlten Rechnung unmittelbar „Suspendiert“ und nach weiteren 8 Kalendertagen automatisch gelöscht.
  - ***Virtuelle Server „OpenVZ“*** werden nach einer Kündigung durch den Kunden (sofortige Wirkung oder per Stichtag) bzw. nach der ersten unbezahlten Rechnung innerhalb von 24 Stunden nach Kündigung automatisch gelöscht.
  - ***Dedizierte Server*** werden nach einer Kündigung durch den Kunden (sofortige Wirkung oder per Stichtag) bzw. nach der ersten unbezahlten Rechnung innerhalb eines (1) Monats nach der Kündigung händisch vom Auftragnehmer (EDIS) gelöscht.

VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- **Datenschutz-Management**, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- Bereits Durchgeführte und regelmäßige Überprüfung der **Datenschutzfolgeabschätzung**
- **Incident-Response-Management**;
- Datenschutzfreundliche Voreinstellungen;