stwt.

VEREINBARUNG ÜBER

Cloud Hostservices

Auftragsverarbeitung nach Art 28 DSGVO

Der/die Verantwortliche:

KundIn mit Cloud Hostservices

(im Folgenden AuftraggeberIn)

Die Auftragsverarbeiterin:

Steirische Wirtschaftstreuhand
GmbH & co KG
Leonhardstraße 109
A 8010 Graz

(im Folgenden Auftragnehmerin)

1. GEGENSTAND DER VEREINBARUNG

Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben:

- Cloud Hostservices Ressourcenbereitstellung
- Datensicherung aller Ressourcen

2. DAUER DER VEREINBARUNG

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von 3 Monaten zum 1. September gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. PFLICHTEN DER AUFTRAGNEHMERIN

(1) Die Auftragnehmerin verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers oder der Auftraggeberin zu verarbeiten. Erhält die Auftragnehmerin einen behördlichen Auftrag, Daten des Auftraggebers oder der Auftraggeberin herauszugeben, so hat sie – sofern gesetzlich zulässig – den/die AuftraggeberIn unverzüglich darüber zu informieren und die Behörde an dieseN zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke der Auftragnehmerin eines schriftlichen Auftrages.

(2) Die Auftragnehmerin erklärt rechtsverbindlich, dass sie 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 bei der Auftragnehmerin aufrecht.

(3) Die Auftragnehmerin erklärt rechtsverbindlich, dass sie alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage ./1 zu entnehmen).

(4) Die Auftragnehmerin wird darauf hingewiesen, dass sie für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

(5) Die Auftragnehmerin ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem/der AuftraggeberIn zu übergeben / in dessen/deren Auftrag zu vernichten. Wenn die Auftragnehmerin die Daten in einem speziellen technischen Format verarbeitet, ist sie verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des/der AuftraggeberIn in dem Format, in dem sie die Daten von dem/der AuftraggeberIn erhalten hat oder in einem anderen, gängigen Format herauszugeben.

(6) Die Auftragnehmerin hat den/die AuftraggeberIn unverzüglich zu informieren, falls sie der Ansicht ist, eine Weisung des Auftraggebers oder der Auftraggeberin 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.

5. SUB-AUFTRAGSVERARBEITERINNEN

Die Auftragnehmerin kann Sub-AuftragsverarbeiterInnen hinzuziehen.
Sie hat den/der AuftraggeberIn von der beabsichtigten Heranziehung eines/einer Sub-AuftragsverarbeiterIn so rechtzeitig zu verständigen, dass er/sie dies allenfalls untersagen kann. Die Auftragnehmerin schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem/der Sub-AuftragsverarbeiterIn ab. Dabei ist sicherzustellen, dass der/die Sub-AuftragsverarbeiterIn dieselben Verpflichtungen eingeht, die der Auftragnehmerin auf Grund dieser Vereinbarung obliegen. Kommt der/die Sub-AuftragsverarbeiterIn seinen/ihren Datenschutzpflichten nicht nach, so haftet die Auftragnehmerin gegenüber dem/der AuftraggeberIn für die Einhaltung der Pflichten des/der Sub-AuftragsverarbeiterIn.

Graz, am 10.11.2021

ANLAGE ./1 – TECHNISCH-ORGANISATORISCHE MAßNAHMEN

VERTRAULICHKEIT

- **Zutrittskontrolle**: Schutz vor unbefugtem Zutritt durch ISO 9001/27001 zertifiziertes Datacenter
- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung durch komplexe Kennwörter und SSL/VPN Verschlüsselung
- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insbesonders von administrativen BenutzerInnenkonten;

INTEGRITÄT

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

VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch Backup-Strategie, unterbrechungsfreie Stromversorgung, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastrukturebene, mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein getrenntes Datacenter, Standardprozesse bei Wechsel/Ausscheiden von MitarbeiterInnen;
- Rasche **Wiederherstellbarkeit**;
- **Löschungsfristen**: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.