Vereinbarung zum Datenschutz

Auftragsverarbeitung

Die Auftragnehmerin

OE Service GmbH, FN 496886 s
Dr.-Franz-Palla-Gasse 21, 920 Klagenfurt,

(in weiterer Folge "OE Service")

verarbeitet für die Auftraggeberin

der Einzelunternehmung bzw Gesellschaft lt. Registrierungsformular

(in weiterer Folge "Werkstatt")
(gemeinsam als „die Parteien)

aufgrund des nachstehend aufgeführten Vertrages personenbezogene Daten im Rahmen einer Auftragsverarbeitung gemäß § 48 DSG iVm Art 28 DSGVO:

Servicevertrag zwischen der OE Service GmbH und der Einzelunternehmung bzw Gesellschaft und zum Datum lt. Registrierungsformular ("Servicevertrag")

Hierzu wird folgende Zusatzvereinbarung geschlossen:

I. Gegenstand der Vereinbarung und Verantwortlichkeit

(1) OE Service verarbeitet personenbezogene Daten im Auftrag der Werkstatt. Dies umfasst die in Punkt II des Servicevertrags genannten Serviceleistungen und inkludiert auch die Weiterleitung der Daten an die jeweiligen Hersteller. Der Hersteller tritt in ein eigenes Verhältnis zur Werkstatt. Diese Vereinbarung ist als Ergänzung zu dem Servicevertrag zu verstehen.

(2) Betroffen von der Datenverarbeitung sind: (End-) Kunden der Werkstatt.

(3) Die Verarbeitung der Daten (inklusive der Weiterleitung an den jeweiligen Hersteller) ist zur Erbringung der Serviceleistungen aus dem Servicevertrag und somit zur Vertragserfüllung erforderlich und gerechtfertigt.

(4) Damit verbunden sind Zugriffe auf folgende Daten, bei denen es sich nicht um besondere Kategorien personenbezogener Daten gemäß § 39 DSG iVm Art 9 DSGVO handelt: Fahrgestellnummer, Name des Fahrzeughalters und / oder Zulassungsbesitzers oä und allgemeine Fahrzeugdaten (Kennzeichen, BJ, etc).

(5) Änderungen des Verarbeitungsgegenstandes, Verarbeitungsumfanges sowie Verfahrensänderungen sind schriftlich zu vereinbaren.

(6) Die Werkstatt ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze verantwortlich (Art 4 Z 7 DSGVO). OE Service sichert in ihrem Verantwortungsbereich die Umsetzung und Einhaltung der datenschutzrechtlichen Verpflichtungen zu.

(7) Die Parteien verpflichten sich, die ihnen während der Durchführung dieses Vertrages zur Kenntnis gelangten Informationen und Unterlagen, insbesondere Geschäfts- und Betriebsgeheimnisse des Vertragspartners streng vertraulich zu behandeln. Ebenso vertraulich zu behandeln sind der Gegenstand und Inhalt des Vertrages. OE Service ist verpflichtet, die zur Verfügung gestellten oder im Rahmen des Auftrages zur Kenntnis genommenen Daten und Informationen der Werkstatt ausschließlich im Rahmen des Vertragszwecks zu verarbeiten und zu nutzen. Eine Verarbeitung oder Nutzung für eigene Zwecke sowie eine Weitergabe an Dritte – ausgenommen der zur Vertragserfüllung notwendigen Weitergabe an Hersteller durch OE Service– ist nur nach schriftlicher Zustimmung der Werkstatt zulässig.

(8) Die Verarbeitung und Nutzung der Daten findet überwiegend in Österreich, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Zum Teil werden Datenverarbeitungstätigkeiten auch außerhalb der EU bzw des EWR durchgeführt, und zwar über Google Drive in den USA. Das angemessene Datenschutzniveau ergibt sich aus (i) einem Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO und (ii) zwischen dem europäischen Unternehmen und dem Übermittlungsempfänger im Drittland abgeschlossenen Standardvertragsklauseln gem. Art 46 DSGVO.

II. Pflichten von OE Service

(1) OE Service verarbeitet die von der Werkstatt übermittelten personenbezogenen Daten ausschließlich im Rahmen der getroffenen Vereinbarung und nach dokumentierten Weisungen der Werkstatt – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – sofern OE Service nicht durch das Recht der Union oder der Mitgliedstaaten, dem OE Service unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt OE Service der Werkstatt diese rechtliche Anforderung vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Eine abweichende Verarbeitung oder Nutzung ohne Kenntnis der Werkstatt oder zu eigenen Zwecken der OE Service ist nicht erlaubt.

(2) OE Service sichert in ihrem Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten allgemeinen und technischen und organisatorischen Maßnahmen zu und erklärt,

dass sie alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach § 54 DSG iVm Art 32 DSGVO ergreift. Die konkreten Vorgaben sind durch Anlage 1 geregelt.

(3) OE Service gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und in die Schutzbestimmungen des anwendbaren Datenschutzrechts eingewiesen worden sind.

(4) Soweit dies möglich ist, unterstützt OE Service die Werkstatt durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Pflichten als Verantwortlicher bei Anträgen auf Wahrnehmung der Betroffenenrechte gemäß der §§ 42ff DSG iVm Kapitel III der DSGVO. Irrtümlich an OE Service gestellte Anträge leitet diese an die Werkstatt unverzüglich weiter. Darüber hinaus unterstützt OE Service die Werkstatt bei der Einhaltung ihrer Pflichten gemäß den §§ 52 bis 56 DSG iVm den Art 32 bis 36 DSGVO.

(5) OE Service unterrichtet die Werkstatt umgehend bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der von der Werkstatt übermittelten personenbezogenen Daten. Weiters informiert OE Service die Werkstatt unverzüglich, falls OE Service der Ansicht ist, eine Weisung der Werkstatt verstößt gegen die DSGVO oder nationale Datenschutzbestimmungen.

(6) OE Service wird darauf hingewiesen, dass sie für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach § 49 DSG iVm Art 30 DSGVO zu errichten hat.

(7) OE Service stellt der Werkstatt alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen, einschließlich Inspektionen, die von der Werkstatt oder einem anderen von dieser beauftragten Prüfer durchgeführt werden.

(8) Nach Wahl der Werkstatt löscht OE Service nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten oder gibt diese zurück, sofern nicht nach dem unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

III. Pflichten und Rechte der Werkstatt

(1) Die Werkstatt ist für die Einhaltung der jeweils einschlägigen Datenschutzgesetze (insbesondere der Art 5 und 6 DSGVO) sowie die Wahrung der Betroffenenrechte insbesondere der Erfüllung von Informationspflichten nach den §§ 42ff DSG iVm mit Kapitel III der DSGVO gegenüber ihren Betroffenen verantwortlich. Betroffenenrechte sind gegenüber der Werkstatt geltend zu machen.

(2) Die Werkstatt hat OE Service unverzüglich und vollständig zu informieren, wenn sie bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Die Werkstatt hat das Recht Weisungen im Rahmen des Art 18 Abs 3 lit a DSGVO zu erteilen. Für Datenschutzverletzungen, die aus einer rechtswidrigen oder mangelhaften Weisung oder angeordneten Sicherungsmaßnahme entstehen, hat die Werkstatt einzustehen und OE Service klag- und schadlos zu halten. Dasselbe gilt für Ansprüche Dritter die aus solch einer, der Werkstatt zuzurechnenden Verletzung, resultieren.

IV. Sub-Auftragsverarbeitung

(1) OE Service kann Sub-Auftragsverarbeiter hinzuziehen. OE Service bedient sich der in Anlage 2 angeführten Unternehmen zu dem in Anlage 2 genannten Zweck als Sub-Auftragsverarbeiter. Die Auftragsvergabe an Subauftragsverarbeiter erfolgt schriftlich.

(2) OE Service informiert die Werkstatt über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Sub-Auftragnehmern so rechtzeitig schriftlich, dass sie dies allenfalls untersagen kann. OE Service schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragnehmern dieselben Verpflichtungen eingeht, die OE Service auf Grund dieser Vereinbarung obliegen.

(3) Sofern der Sub-Auftragnehmer außerhalb eines in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum stammt oder die Datenverarbeitung dort stattfindet, ist durch OE Service darüber hinaus sicherzustellen, dass die Voraussetzungen der Art 45ff DSGVO erfüllt sind. Dies ist der Werkstatt gegenüber schriftlich vor Aufnahme der Tätigkeiten des Subunternehmers nachzuweisen (Nachweis durch Vorlegen des Safe-Harbor-Zertifikats bei Sub-Auftragnehmer aus den USA, der unterzeichneten einschlägigen "Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Sub-Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates" und/oder der durch eine Aufsichtsbehörde genehmigten Binding Corporate Rules). Der Nachweis für die Einhaltung der Voraussetzungen der Art 45ff DSGVO findet sich ebenfalls in Anlage 2.

V. Vertragsdauer

(1) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Servicevertrages.

(2) Die Verpflichtungen zur Einhaltung des Datengeheimnisses und der Vertraulichkeit bestehen auch nach Beendigung dieser Vereinbarung fort.

VI. Sonstiges, Allgemeines

(1) Der Abschluss dieser Vereinbarung erfolgt im elektronischen Weg (§ 48 Abs 5 DSG iVm At 28 Abs 9 DSGVO). Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen der OE Service – bedürfen einer schrift-

lichen oder elektronischen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt.

(2) Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden oder der Vertrag eine Lücke enthalten, so bleibt die Rechtswirksamkeit der übrigen Bestimmungen hiervon unberührt. Anstelle der unwirksamen oder fehlenden Bestimmung gilt eine wirksame Bestimmung als vereinbart, die dem von den Parteien Gewollten wirtschaftlich am nächsten kommt.

(3) Es gilt österreichisches Recht. Gerichtsstand ist das sachlich zuständige Gericht in Klagenfurt.

Anlage 1: Technische und organisatorische Schutzmaßnahmen

Sofern personenbezogene Daten verarbeitet oder genutzt werden (z. B. zur Kenntnis genommen werden), sind gemäß §§ 37 und 48 DSG iVm den Art 5 und 24f DSGVO die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des/der DSG/DSGVO zu gewährleisten. OE Service erfüllt diese Verpflichtung durch folgende Sicherheitsmaßnahmen:

Vertraulichkeit

Zutrittskontrolle

Unbefugten ist der physische Zutritt zu den Räumlichkeiten mit entsprechenden Datenverarbeitungsanlagen zu verwehren, in denen personenbezogene Daten der Werkstatt verarbeitet oder genutzt werden.

Hierunter fallen neben dem Serverraum auch die weiteren Räume, in denen sich Datenverarbeitungsanlagen befinden, die einen Zugang zu den Systemen/Daten der Werkstatt ermöglichen.

Zur Zutrittskontrolle gehören u. a. folgende Maßnahmen:

- Automatisches Zugangskontrollsystem
- Regulierte Schlüsselausgabe
- Elektrische Türöffner
- Manuelle Verriegelungssysteme
- Sicherheitsschlösser
- Sorgfältige Auswahl des Reinigungspersonals

Zugangskontrolle

Es ist zu verhindern, dass die Datenverarbeitungssysteme von Unbefugten genutzt werden können. Die Zugangsberechtigungen sind auf die für die Aufgabenerfüllung notwendigen Rechte zu beschränken (Minimalprinzip). Nach Erfüllung der Aufgabe sind die Berechtigungen zu löschen oder zu sperren.

Die Zugangsprotokolle umfassen erfolgreiche/erfolglose Logins und vom Benutzer bzw. dem System initiierte Logins. Systemsicherheitsrelevante Aktivitäten (alle Aktivitäten im Administrator-Modus) sind stets zu protokollieren.

Zur Zugangskontrolle gehören ferner u. a. folgende Maßnahmen:

- Vergabe von Benutzerrechten
- Passwortvergabe
- Verwendung von Antivirensoftware

- Authentifizierung mit Benutzername/Passwort
- Passwort-Richtlinien inkl Passwortlänge und regelmäßiger Passwortänderung
- Sicher Verschlüsselung der Festplatte

Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung der Inhalte der Datenverarbeitungssysteme nur Berechtigten und ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Ferner ist sicherzustellen, dass personenbezogene Daten der Werkstatt bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Zur Zugriffskontrolle gehören u. a. folgende Maßnahmen:

- Erstellung eines Berechtigungskonzepts
- Rechteverwaltung durch Systemadministratoren
- Periodische Überprüfung der vergebenen Berechtigungen, insb. Von administrativen Benutzerkonten
- Einsatz von Aktenvernichtern
- Sichere Speicherung von Datenträgern
- Differenzierter Zugriff pro Benutzer entsprechend seiner Aufgaben
- Clear-Desk / Clear-Screen Policy

Trennungsprinzip

Maßnahmen, die sicherstellen, dass die für verschiedene Zwecke erhobene Daten getrennt verarbeitet werden können.

- Physisch getrennte Speicherung auf bestimmten Systemen oder Datenträgern
- Erstellung eines Berechtigungskonzepts

Integrität

Weitergabekontrolle

Personenbezogene Daten der Werkstatt sind bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger davor zu schützen, dass sie nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Die Übertragung von sensiblen, schutzwürdigen personenbezogenen Daten der Werkstatt ist zur Wahrung der Vertraulichkeit ausschließlich in verschlüsselter Form oder passwortgeschützt zulässig. Dies gilt auch (oder insbesondere) bei einem Versand bei E-Mail; hierbei ist das Verfahren mit der Werkstatt abzusprechen.

Zur Weitergabekontrolle gehören folgende Maßnahmen:

- Erstellung einer Übersicht über die regulären Zugriffs- und Transferprozesse

Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten der Werkstatt in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Rückverfolgbarkeit der Eingabe, Änderung und Löschung von Daten über individuelle Benutzernamen (keine Benutzergruppen)
- Zugriffs- und Änderungshistorie

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Personenbezogene Daten der Kunden der Werkstatt sind gegen zufällige Zerstörung oder Verlust zu schützen. Um das Risiko eines Datenverlusts zu reduzieren, sind regelmäßige Datensicherungen durchzuführen, welche mit der Werkstatt abzusprechen sind. Ferner sind die Datenverarbeitungssysteme entsprechend zu warten und zu aktualisieren.

Ferner gehören zur Verfügbarkeitskontrolle u. a. folgende Maßnahmen:

- Backup-Strategie
- Meldeweg und Notfallpläne
- Virenschutz oder Firewall

Wiederherstellbarkeit

Maßnahmen, die sicherstellen, dass installierte Systeme im Falle iener Unterbrechung sofort wiederhergestellt werden können.

- Einsatz eines mehrstufigen Backup – Verfahrens mit umfangreichem Backup

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Auftragskontrolle

Es ist sicherzustellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Werkstatt verarbeitet werden können. Die Pflicht zur Auftragskon-

trolle liegt bei OE Service wobei OE Service dieser regelmäßig und nach Anforderung die entsprechenden Informationen zukommen lässt.

- Auswahl des Auftragnehmers unter Beachtung der Sorgfaltspflicht (insbesondere im Hinblick auf die Datensicherheit)
- Schriftliche Anweisungen an den Auftragnehmer (zB über einen Auftragsverarbeitungsvertrag gemäß Art. 28 GDPR)
- Formalisiertes Vertragsverhältnis

Incident Response Plan

Regelmäßige Überprüfung, Dokumentation und ggf. Optimierung.

- Dokumentation des durchgeführten Datenschutzes
- Regelmäßige Datenschutzkontrollen
- Jährliche interne Datenschutzüberprüfung
- Datenschutzkonforme Softwarelösung
- Umfassendes Rechte- und Rollenkonzept

Anlage 2: Sub-Auftragsverarbeiter

Dienstleister 1:

Name des Dienstleisters:	Google LLC (früher Google Inc.),
Anschrift: 94043	1600 Amphitheatre Parkway, Mountain View, California
Art der Dienstleistung:	Datenspeicher
Bestellter Datenschutzbeauftragter:	
Kontaktdaten des DSB:	
Übermittlung ins Drittland:	USA auf Basis Privacy Shield Zertifizierung abrufbar unter: https://www.privacyshield.gov/participant?id=a2zt0000000 1L5AAI und Standardvertragsklauseln abrufbar unter: https://gsuite.google.com/intl/de/terms/mcc_terms.html

Dienstleister 2:

Name des Dienstleisters:	Artline Design® e.U.
Anschrift:	Wiesingerstraße 8 Top 21, 1010 Wien
Art der Dienstleistung:	Webdesign
Bestellter Datenschutzbeauftragter:	
Kontaktdaten des DSB:	
Übermittlung ins Drittland:	Nein