V e r e i n b a r u n g

über eine

Auftragsverarbeitung nach Art 28 DSGVO

durch

den Auftragsverarbeiter

FONDA LABS Digitalwerkstatt GmbH
Technologiepark 17
4320 Perg

(im Folgenden Auftragnehmer)

im Rahmen der Nutzung des Online-Tools
klickundguat

1. GEGENSTAND DER VEREINBARUNG

(1) Gegenstand dieses Auftrages ist der technische Betrieb des Online-Shops auf klickundguat.at.
(2) Folgende Datenkategorien werden verarbeitet:
    a. IP Adressen
    b. Emailadressen
    c. Vor- und Nachname
    d. Usernamen
    e. Kontaktdaten
(3) Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:
    a. Website-Besucher
    b. Website-Redakteure

2. DAUER DER VEREINBARUNG

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien wie die zugrundeliegende Service- und Wartungsvereinbarung zum Ende eines jeden Kalenderjahres unter Einhaltung einer Kündigungsfrist von einem Monat gekündigt werden

. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. PFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. 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.

(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 ergreift die technischen und organisatorischen 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 wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

(7) 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.

(8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben. 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. PFLICHTEN AUFTRAGGEBER

(1) Der Auftraggeber informiert den Auftragnehmer, wenn Fehler oder Unregelmäßigkeiten bei der Auftragsverarbeitung durch den Auftragnehmer bekannt werden.

(2) Der Auftraggeber unterstützt den Auftragnehmer bei der Einhaltung der Verpflichtungen dieser Vereinbarung und der DSGVO.

5. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.

ANLAGE ./1 – TECHNISCH-ORGANISATORISCHE MASSNAHMEN

Technisch-organisatorische Maßnahmen

Der Auftragsverarbeiter bestätigt folgende Maßnahmen zur Einhaltung der Anforderungen an die Sicherheit der Datenverarbeitung ergriffen zu haben (Art. 32 DSGVO):

1. Vertraulichkeit

1.1. Zutrittskontrolle

- Die Datenspeicheranlagen (Server-Festplatten) sind mehrfach zutrittsgesichert: durch eine Büro-Sicherheitstür, eine weitere versperrte Serverraum-Tür sowie eine Absperrung direkt auf dem Serverschrank. Zutritt haben ausschließlich befugte Personen mittels entsprechender Schlüssel. Die InhaberInnen der Schlüssel sind durch Lichtbildausweis identifiziert.
- Selbstständigen Zutritt zu den Büroräumen haben grundsätzlich nur MitarbeiterInnen und ausgewählte GeschäftspartnerInnen des Auftragverarbeiters mittels drei Schlüsseln.
- Gäste müssen sich am Empfang anmelden und dürfen sich nicht unbegleitet in den Büroräumlichkeiten bewegen.
- Türen, Tore und Fenster sind außerhalb der Betriebszeiten fest verschlossen.

1.2. Zugangskontrolle

- Der elektronische Zugang zu Systemen über Netzwerk ist durch Firewalls und VPNs geschützt.
- Die administrativen Zugangsdaten zu den jeweiligen Serversystemen sind nur den
- System-AdministratorInnen bekannt.
- Jede BenutzerIn erhält einen personalisierten, passwortgeschützten Account.
- Pro BenutzerIn wird eine individuelle Benutzererkennung vergeben.
- Es werden sichere Passwörter entsprechend der internen Sicherheitsrichtlinien des Auftragsverarbeiters verwendet.
- MitarbeiterInnen sind angehalten, ihre Workstation bei Verlassen des Arbeitsplatzes immer zu sperren. Außerdem erfolgt eine automatische Sperre nach wenigen Minuten Inaktivität des Mitarbeiters/der Mitarbeiterin.

1.3. Zugriffskontrolle

- Zu Kundensystemen erhalten nur diejenigen MitarbeiterInnen Zugriff, die die jeweilige Kundschaft betreuen.
- Zugriff auf Systeme mit Daten der Kundschaft haben jeweils nur die MitarbeiterInnen, die einen solchen Zugriff für ihre Tätigkeit benötigen.
- Die vergebenen Berechtigungen von Benutzerkonten werden periodisch überprüft.

2. Integrität

2.1. Weitergabekontrolle

- Die Daten sind durch geeignete technische Maßnahmen (z.B., Firewalls, Virenschutzsysteme, Zugriff via VPN) vor dem unberechtigten Zugriff von außen, sowie vor Manipulationen, geschützt.
- Alle MitarbeiterInnen, SubauftragnehmerInnen, Erfüllungsgehilfen und Kooperationspartner sind zur Verschwiegenheit und zur Einhaltung des Datengeheimnisses verpflichtet. Insbesondere auch nach Beendigung ihrer Tätigkeit beim Auftragsverarbeiter bzw. nach Beendigung der Zusammenarbeit mit dem Auftragsverarbeiter.

2.2. Eingabekontrolle

- Das Nachverfolgen von Dateneingaben/-änderungen wird, wo technisch möglich und organisatorisch vertretbar, mittels etablierter Logging-Verfahren gewährleistet. Somit ist es jederzeit nachvollziehbar, welche BenutzerIn welche Daten eingegeben/verändert hat.
- Beispiel: Zur Kontrolle der Dateneingabe oder Datenveränderung in den Content Management Systemen (z.B. Wordpress, TYPO3, Drupal, Magnolia, Kentico, Liferay, eZ Platform) verfügen diese im Normalfall über entsprechende Log-Mechanismen. Anhand dieser lässt sich im Anlassfall nachvollziehen, welche BenutzerIn zu welchem Zeitpunkt welche Änderungen durchgeführt hat.

3. Verfügbarkeit und Belastbarkeit

- Alle Systeme, die im Zusammenhang mit der Verarbeitung von personenbezogenen Daten genutzt werden, werden im Rahmen regelmäßiger Backups gegen zufällige Zerstörung oder Verlust geschützt.
- Die Serversysteme sind mit unterbrechungsfreier Stromversorgung durch Batteriebackup ausgestattet.
- Die verwendeten Backupsysteme erlauben eine rasche Wiederherstellbarkeit der Daten.
- Löschungsfristen sind in den internen Sicherheitsrichtlinien des Auftragsverarbeiters definiert.

4. Verfahren zur Überprüfung, Bewertung und Evaluierung

- Es wird keine Auftragsdatenverarbeitung im Sinne des Art 28 DSGVO ohne entsprechende Weisung des Verantwortlichen durchgeführt.
- Alle MitarbeiterInnen, SubauftragnehmerInnen, Erfüllungsgehilfen und Kooperationspartner werden zur Verschwiegenheit und zur Einhaltung des Datengeheimnisses verpflichtet.
- Alle MitarbeiterInnen werden regelmäßig und nachweislich zu den Vorgaben der DSGVO geschult.
- Die angewandten Prozesse und Systeme werden regelmäßig überprüft und ggf. adaptiert.