Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 DSGVO

Verantwortliche/r i.S.d. DSGVO:
Nils Tester
Teststr. 1, 1111 Teststadt
Österreich
(im Folgenden Auftraggeber)

Auftragsverarbeiter i.S.d. DSGVO:
RSVP GmbH
Herklotzgasse 32/3/8, 1150 Wien
Österreich
(im Folgenden Auftragnehmer)

1. Gegenstand der Vereinbarung

1.1.) Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben: elektronisches Sammeln von Zu- und (eventuell) Absagen mittels der webbasierenden Lösung stage1.uawg.online für die Veranstaltung

- Name der Veranstaltung:
  Test DPA
- mit der URL:
  https://stage1.e-list.at/test-nils/test-dpa

1.2.) Folgende Datenkategorien werden verarbeitet:

- Kontaktdaten wie z.B. Name, E-Mail- bzw. Postadresse oder Telefonnummer bzw. Daten, die für die Organisation und Durchführung der Veranstaltung unbedingt nötig sind. Der Auftraggeber hat folgende weiter Felder konfiguriert:
  Nationalität
- Felder zur Abfrage der Daten gestaltet bzw. formuliert der Auftraggeber selbst oder gibt der Auftraggeber – bei Durchführung der Programmierung durch den Auftragnehmer – frei. Der Auftraggeber hat keine Felder definiert.

Vom Abfragen sensibler Daten im Sinne der DSGVO wird aus Datenschutzgründen ausdrücklich abgeraten. Im Missbrauchsfall hält sich der Auftragnehmer beim Auftraggeber schad- und klaglos.

1.3.) Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:

a. bei geschlossenem Einladungskreis:
   Einladungskreis lt. Liste des Auftraggebers
b. bei offener Einladung mit Passwort:
   alle Interessenten, denen Link und Passwort zugänglich gemacht wird
c. bei offener Einladung:
   alle Interessenten, denen der Link zugänglich gemacht wird

2. Dauer der Vereinbarung

2.1.) Die Vereinbarung kommt durch aktive, explizite, elektronische Zustimmung des Auftraggebers über das Online-System des Auftragnehmers zustande. Das Online-System des Auftragnehmers speichert

dabei den Zeitpunkt der Zustimmung, einen kryptographischen Hashwert zur Integritätsprüfung des vom Auftraggeber heruntergeladenen PDF-Dokuments, sowie die IP-Adresse der Gegenstelle des Auftraggebers.

2.2.) Die Vereinbarung endet mit einmaliger Durchführung der Arbeiten, ist befristet abgeschlossen und endet 30 Tage nach dem Veranstaltungsdatum. Zu diesem Zeitpunkt werden die personenbezogenen Daten (alle Rückmeldungen von betroffenen Personen lt. Punkt 1.3.) von den Servern des Auftragnehmers gelöscht.

2.3.) Die Vereinbarung kann vom Auftraggeber jederzeit vor Ablauf der Frist – durch Löschung der Veranstaltung im admin-Bereich auf uawg.online gekündigt werden.

3. Pflichten des Auftragnehmers

3.1.) 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.

3.2.) 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.

3.3.) 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).

3.4.) 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.

3.5.) 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).

3.6.) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

3.7.) 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.

3.8.) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, zu löschen. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten bis zum Ende dieser Vereinbarung dem Auftraggeber im csv.Format zum Download bereitzustellen.

3.9.) 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

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

5. Sub-Auftragsverarbeiter

5.1.) Als fixer Sub-Auftragsverarbeiter gilt die Firma voll.werbung GmbH, Hauptstraße 32, 2371 Hinterbrühl, die das Hosting von uawg.online übernimmt, sowie den Versand der Bestätigungsmails.

5.2.) Der Auftragnehmer kann Sub-Auftragsverarbeiter (Einladungsdruck, Druck von Namenskärtchen, Newsletter-Versand oder Ähnliches) hinzuziehen. Er hat den Auftraggeber von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann.

5.3.) Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. 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.

Anlage 1: Technisch-organisatorische Maßnahmen

Anlage zur Vereinbarung nach Artikel 28 DSGVO – Beschreibung technische und organisatorische Maßnahmen

Zutrittskontrolle

Der körperliche Zutritt von Personen in Räumlichkeiten des Auftragnehmers ist ohne entsprechende Schlüssel nicht möglich. Zum Einsatz kommen per Schnappschloss gesicherte Türen bzw. elektrische Türöffner. Besucher werden an der Eingangstüre abgeholt.

Zugangskontrolle

Um Zugang zu den technischen Systemen und Anwendungen zu erhalten, muss der für diese Systeme/Anwendungen befugte Mitarbeiter des Auftragnehmers ein Kennwort, einen kryptographischen Schlüssel und ggf. Zwei-Faktor-Authentifizierung benutzen. Ohne Benutzung des personalisierten Benutzerkontos ist eine Authentifizierung gegenüber dem System oder der Anwendung nicht möglich.

Datenverarbeitungs-Arbeitsplätze des Auftragnehmers haben automatische Sperrmechanismen.

Das Benutzerkonto muss über die Geschäftsführung des Auftragnehmers genehmigt werden.

Zugriffskontrolle

Zugriffsberechtigungen werden nach den Prinzipien „need-to-know" und „need-to-do" erteilt. Daher liegen den Zugriffsberechtigungen bedarfsorientierte Berechtigungskonzepte, Benutzerprofile und Funktionsrollen zugrunde.

Zugriffe werden technisch überwacht. Die Ausführung administrativer Zugriffe wird protokolliert und kontrolliert. Auf die Anwendung bezogene Zugriffe werden mit den Mitteln und Möglichkeiten der Anwendung protokolliert und überwacht.

Pseudonymisierung

Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.

Weitergabekontrolle

Der Auftragnehmer stellt die Integrität der (personenbezogenen) Daten bei der Speicherung und Weitergabe innerhalb der DV-Systeme und DV-Anwendungen durch Plausibilitätsprüfung und Verifizierungsverfahren sicher. Die Vertraulichkeit und Weitergabe von (personenbezogenen) Daten, die außerhalb des Verfügungsbereichs des Auftragnehmers gelangen, werden einerseits durch Plausibilitätsprüfung und/oder Verifizierungsverfahren, andererseits durch Verwendung von an die Erfordernisse angepasste und abgestufte Sicherheits- und/oder Verschlüsselungsverfahren sichergestellt.

Eine SSL-Verschlüsselung und das Nutzen von anderweitig verschlüsselten Kommunikationskanälen - insbesondere in der internen Kommunikation – sichert den Transfer der Daten. Es werden möglichst nur geschlossene Datennetze verwendet.

Eingabekontrolle

Eingaben in die Systeme sowie deren Ausgabe werden protokolliert. Die Protokolle werden nach den Inhalten und/oder gesetzlichen Vorschriften archiviert oder nach Zweckverrichtung gelöscht bzw. für die weitere Verarbeitung gesperrt. Abstimmungs- und Kontrollverfahren, die überwiegend automatisiert sind, gewährleisten die Ordnungsmäßigkeit der Verarbeitung.

Auftragskontrolle

Der Auftragnehmer verarbeitet die überlassenen (personenbezogenen) Daten aufgrund und anhand von vertraglich vereinbarten Weisungen des Auftraggebers. Kompetenzen und Kontrollmaßnahmen werden in Abstimmung mit dem Auftraggeber technisch oder organisatorisch in die Betriebsabläufe eingebunden.

Verfügbarkeitskontrolle

Die datentechnischen Systeme des Auftragnehmers sind gegen „Angriffe" von außen unter Verwendung aktueller Sicherheitstechnik geschützt. Dazu gehören technische Systeme wie Firewalls und Intrusion Detection Systeme.

Die benutzten Serversysteme haben eine unterbrechungsfreie Stromversorgung.

Die Daten werden regelmäßig in verschlüsselter Form auf vom Hauptspeicherort unabhängige Systeme gesichert.

Die rasche Wiederherstellbarkeit von gesicherten Daten wird nach Möglichkeit der jeweiligen Anwendung gewährleistet.

(Personenbezogene) Daten werden jeweils nur so lange gespeichert, wie vertraglich mit dem Auftraggeber vereinbart.

Trennungsgebot

Systeme und Anwendungen sind auf eine zweckgebundene und mandantengetrennte Verarbeitung ausgerichtet. Test- und Produktionssysteme sind physikalisch getrennt.

Regelmäßige Evaluierung

Der Auftragnehmer achtet auf regelmäßige Mitarbeiter-Schulungen zum Thema Datenschutz sowie auf datenschutzfreundliche Voreinstellungen in allen entsprechenden Anwendungen.