Vereinbarung über Auftragsverarbeitung zum Vertrag über die Ticketshop-Software pretix

zwischen

pretix GmbH
Berthold-Mogel-Str. 1, 69126 Heidelberg
Deutschland
– Auftragsverarbeiter / Auftragnehmer / Provider –

und

DEMO MUSTER SAMPLE
– Verantwortlicher / Auftraggeber / Kunde –

Dieses Dokument ist ein Muster unserer Vereinbarung über Auftragsverarbeitung. Bitte senden Sie uns dieses Muster nicht unterschrieben zu! Laden Sie bitte stattdessen die von uns vorbereitete und personalisierte Version aus Ihrem pretix Veranstalterkonto herunter. Diese befindet sich im Bereich "Datenschutz".

§ 1 Gegenstand des Auftrags

(1) Der Auftragnehmer verarbeitet für den Auftraggeber personenbezogene Daten, indem er die technische Infrastruktur zur Abwicklung von Online-Kaufverträgen zur Verfügung stellt.

(2) Dazu stellt der Auftragnehmer (auch: Provider) dem Auftraggeber (auch: Kunden) auf Grundlage der Allgemeinen Geschäftsbedingungen für Verträge über die Ticketshop-Software (Version 1.13 vom 04.07.2025), der darin enthaltenen Service Level Agreements und technischen Spezifikation, sowie ggf. kundenspezifischen Vertragsergänzungen (zusammen im Folgenden: Hauptvertrag) ein Softwareprodukt zur Nutzung über das Internet zur Verfügung. Die Software wird vom Auftragnehmer in einem Rechenzentrum betrieben und dem Auftraggeber zur Nutzung über das Internet zur Verfügung gestellt (auch als „Software as a Service“ bezeichnet).

(3) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO entsprechend der Vereinbarungen aus dem Hauptvertrag mit AGB, SLA und Technischer Spezifikation, auf die hier verwiesen wird.

(4) Diese Zusatzvereinbarung zur Auftragsverarbeitung konkretisiert die Verpflichtungen der Parteien zum Umgang mit personenbezogenen Daten, die sich aus dem Hauptvertrag ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag im Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen.

§ 2 Dauer des Auftrags

(1) Die Dauer des Auftrags richtet sich nach der Laufzeit des Hauptvertrags gemäß § 1 dieser Vereinbarung.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 3 Konkretisierung des Auftragsinhalts

(1) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(2) Art und Zweck der vorgesehenen Verarbeitung von Daten ergeben sich primär aus dem Hauptvertrag.

(3) Die Verarbeitung der Daten besteht dabei insbesondere in der Erhebung, Erfassung, Speicherung und Auswertung der vom Auftraggeber und dessen Kunden eingegebenen Daten sowie Übermittlung dieser Daten an den Auftraggeber.

(4) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten bzw. Datenkategorien:
   a) Personenstammdaten
   b) Kommunikationsdaten (z.B. Telefon, E-Mail)
   c) Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
   d) Kundenhistorie
   e) Vertragsabrechnungs- und Zahlungsdaten
   f) Planungs- und Steuerungsdaten
   g) Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

(5) Konkret geht es um folgende personenbezogene Daten:
   a) Bestelldaten, insbesondere bestellte Produkte sowie E-Mail-Adressen und Namen. Je nach getroffenen Einstellungen des Auftraggebers werden ebenfalls Rechnungsadressen, Lieferadressen oder Eingaben in vom Auftraggeber beliebig definierbare Formularfelder verarbeitet.
   b) Besucherdaten des Online-Shops, insbesondere Anzahl der Besucher und Herkunft der Besucher über bestimmte Verlinkungen sowie freiwillig erfasste E-Mail-Adressen von Kaufinteressenten für Produkte, die zu dem Zeitpunkt nicht verfügbar sind.
   c) Zahlungsdaten je nach gewählter Zahlungsart des Käufers, z.B. Bankverbindungsdaten. Bei Online-Zahlungsarten wie PayPal oder Kreditkarte muss der Auftraggeber einen externen Dienstleister mit der Zahlungsabwicklung beauftragen und auf Seiten des Auftragnehmers fallen höchstens jene Daten an, die die Schnittstelle des externen Dienstleisters bereitstellt. Dies umfasst i.d.R. Namen und Account-Namen, aber keine vollständigen Kreditkartennummern.
   d) Technische Daten, die beim Betrieb einer öffentlichen Website anfallen (z.B. Server-Logs). Hierbei können IP-Adressen enthalten sein, auch wenn diese nur aus konkretem Anlass (z.B. Verdacht auf einen Angriff, Absturz der Software) gespeichert werden. Die Speicherdauer beträgt höchstens 90 Tage.

e) E-Mails und Metadaten zu Supportfällen bzw. Kontaktaufnahmen des Auftraggebers oder seiner Kunden mit dem Kundendienst des Auftragnehmers.
f) Authentifizierungsdaten der Mitarbeiter des Auftraggebers, die zur Nutzung der Software berechtigt sind.
g) Protokolle über die Nutzung der Software durch den Auftraggeber und seine Mitarbeiter zur Sicherstellung der Nachvollziehbarkeit von Buchungen.

(6) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
a) Mitarbeiter des Auftraggebers
b) Kunden des Online-Shops des Auftraggebers
c) Besucher und Interessenten des Online-Shops des Auftraggebers

§ 4 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel durch entsprechende Konfiguration, Einrichtung und Benutzung der Software. Darüber hinausgehende Weisungen, Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder per E-Mail festzulegen. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise nach vorheriger Terminvereinbarung und ohne Störung des Betriebsablaufes von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Die Prüfung kann durch einen beauftragten Dritten erfolgen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Bei der Prüfung muss mindestens ein Mitarbeiter des Auftragnehmers anwesend sein. Der Auftragnehmer kann für hierdurch direkt entstehenden Aufwand eine Vergütung gemäß des Stundensatzes der aktuell gültigen Preisliste verlangen, sofern die Kontrolle anlasslos und nicht aufgrund eines Datenschutzvorfalls oder einer Weisung einer Aufsichtsbehörde erfolgt.

(5) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

§ 5 Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

(1) Weisungsberechtigte Personen des Auftraggebers sind alle Mitarbeiter des Auftraggebers, denen der Auftraggeber eigene persönliche Zugänge zur bereitgestellten Software selbst einrichtet.

(2) Weisungsempfänger beim Auftragnehmer sind alle Mitarbeiter des Auftragnehmers, die im schriftlichen oder elektronischen Kundendienst tätig sind. Als Datenschutzbeauftragte bestellt ist derzeit Frau Susanne Kasper (E-Mail: datenschutz@pretix.eu, Tel. 06221 3217713).

(3) Weisungen sind durch entsprechende Konfiguration der Software, per E-Mail an support@pretix.eu oder per Post an pretix GmbH, Berthold-Mogel-Str. 1, 69126 Heidelberg, zu erteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

§ 6 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

(2) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu.

(4) Die Daten des Auftraggebers werden mit den Daten anderer Auftraggeber auf gemeinsamen physischen Systemen verarbeitet. Eine Aushändigung oder Vernichtung spezifischer Datenträger ist daher nicht möglich. Möglich ist aber die Löschung bestimmter Daten des Auftraggebers auf den jeweiligen Datenträgern. Der Auftragnehmer stellt durch ein Rechtekonzept sicher, dass jeder Auftraggeber nur auf die jeweils eigenen Daten Zugriff erhält.

(5) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO). Der Auftragnehmer unterstützt den Auftraggeber darüber hinaus im Rahmen seiner Konsultationspflicht gegenüber der Aufsichtsbehörde gemäß Art. 36 DSGVO.

(6) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

(7) Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

(8) Auskünfte über personenbezogene Daten an Dritte darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen. Eine solche Weisung zur Datenweitergabe an Dritte gilt dann als ausdrücklich erteilt, wenn der Auftraggeber die Funktionen der Software zur Kommunikation mit externen Dienstleistern wie z.B. Zahlungsdienstleistern oder Newsletterdienstleistern aktiviert und konfiguriert.

(9) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber – grundsätzlich nach Terminvereinbarung und ohne Störung des Betriebsablaufes – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im

angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte, die nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen, zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO).

(10) Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt, indem er die nötigen Einsichtnahmen ermöglicht. Der Auftragnehmer kann für hierdurch direkt entstehenden Aufwand eine Vergütung gemäß des Stundensatzes der aktuell gültigen Preisliste verlangen, sofern die Kontrolle anlasslos und nicht aufgrund eines Datenschutzvorfalls oder einer Weisung einer Aufsichtsbehörde erfolgt.

(11) Der Auftraggeber erklärt sich damit einverstanden, dass die Mitarbeiter des Auftragnehmers ihre Beschäftigung auch von Privatwohnungen aus ausüben (Tele- bzw. Heimarbeit) und auch von dort aus zu Zwecken der Fehleranalyse Zugriff auf Datenbestände haben. Daten des Auftraggebers werden nicht über einzelne Vorgänge der Fehleranalyse hinaus in Privatwohnungen gespeichert. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall sicherzustellen.

(12) Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind.

(13) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese Verpflichtung besteht auch nach Beendigung des Vertrages fort.

(14) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

(15) Ein betrieblicher Datenschutzbeauftragter ist vom Auftragnehmer ohne Anerkennung einer gesetzlichen Notwendigkeit freiwillig bestellt. Als Datenschutzbeauftragte bestellt ist derzeit Frau Susanne Kasper (E-Mail: datenschutz@pretix.eu, Tel. 06221 3217713).

§ 7 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33-36 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

(2) Der Auftragnehmer informiert den Auftraggeber hierzu per E-Mail an die vom Auftraggeber in der Software hinterlegte primäre Kontaktadresse und die ggf. dort hinterlegte Datenschutz-Kontaktadresse.

§ 8 Unterauftragsverhältnisse mit Subunternehmern

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen ohne konkreten Bezug zur Leistung. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Erlaubnis gemäß Art. 28 Abs. 2 DSGVO, dass der Auftragnehmer zur Erfüllung seiner vertraglichen Aufgaben Unterauftragnehmer einsetzen darf.

(3) Der Auftragnehmer muss dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

(4) Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(5) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern.

(6) Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

(7) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(8) Der Auftragnehmer hat die in der Anlage A mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beauftragt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

(9) Der Auftragnehmer informiert den Auftraggeber immer im Voraus über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (Art. 28 Abs. 2 Satz 2 DSGVO). Dabei wird eine Einspruchsfrist von 14 Tagen vereinbart.

(10) Im Falle eines Einspruchs kann der Auftragnehmer den Vertrag entsprechend der regulären Kündigungsfristen des Hauptvertrages kündigen, falls die Fortführung der Dienstleistung ohne die beabsichtigte Änderung nicht zumutbar ist. Der Auftragnehmer muss in diesem Fall sicherstellen, dass

an den neuen Unterauftragnehmer keine Daten des Auftraggebers übertragen werden.

§ 9 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

(1) Für die konkrete Auftragsverarbeitung wird ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

(2) Die vom Auftragnehmer hierbei konkret getroffenen technischen und organisatorischen Maßnahmen werden in Anlage B beschrieben.

(3) Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DSGVO). Das Ergebnis wird dem Auftraggeber auf Anfrage mitgeteilt.

(4) Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

(5) Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

(6) Über wesentliche Änderungen muss der Auftragnehmer den Auftraggeber in dokumentierter Form elektronisch mit einer angemessenen Vorlaufzeit informieren.

§ 10 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

(1) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber wie folgt zu löschen bzw vernichten zu lassen: Alle personenbezogenen Daten auf den Systemen des Auftragnehmers werden nach Abschluss der vertraglichen Arbeiten umgehend gelöscht oder so anonymisiert, dass eine Zuordnung zu Personen unmöglich ist, soweit keine rechtlichen Gründe wie beispielsweise Aufbewahrungspflichten nach HGB entgegenstehen. Die Daten können für einen Zeitraum von bis zu drei Monaten noch in Sicherheitskopien enthalten sein, die zur Sicherung der Integrität der Sicherheitskopien nicht bearbeitet werden können. Die Sicherungskopien werden verschlüsselt in einem getrennten Rechenzentrum gespeichert und nach spätestens drei Monaten automatisch gelöscht.

(2) Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe in einem elektronischen Format dokumentiert zu bestätigen.

§ 11 Haftung

(1) Auf Art. 82 DSGVO wird verwiesen.

(2) Es gilt die im Hauptvertrag vereinbarte Haftungsregelung.

§ 12 Sonstiges

(1) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

(2) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

(3) Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen

(4) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Dieses Dokument ist ein Muster unserer Vereinbarung über Auftragsverarbeitung. Bitte senden Sie uns dieses Muster nicht unterschrieben zu! Laden Sie bitte stattdessen die von uns vorbereitete und personalisierte Version aus Ihrem pretix Veranstalterkonto herunter. Diese befindet sich im Bereich "Datenschutz".

Anlage A: Auflistung der beauftragten Unterauftragnehmer

(1) netcup GmbH, Daimlerstr. 25, 76185 Karlsruhe
Beauftragt mit Server- und Rechenzentrumsdienstleistungen zur Datenverarbeitung und Speicherung
Rechenzentrumsstandorte: Nürnberg (Deutschland)

(2) Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen
Beauftragt mit Server- und Rechenzentrumsdienstleistungen zur Datenverarbeitung und Speicherung
Rechenzentrumsstandorte: Nürnberg (Deutschland) und Falkenstein (Deutschland)

(3) rapidmail GmbH, Augustinerplatz 2, 79098 Freiburg i.Br.
Beauftragt mit E-Mail-Zustellungsleistungen
Rechenzentrumsstandorte: Deutschland

(4) IONOS SE und deren Tochterunternehmen IONOS Cloud GmbH, Elgendorfer Str. 57, 56410 Montabaur
Beauftragt mit Server- und Rechenzentrumsdienstleistungen zur Datenverarbeitung und Speicherung
Rechenzentrumsstandorte: Deutschland

(5) AhaSend B.V., Willem Fenengastraat 16, Amsterdam, Niederlande
Beauftragt mit E-Mail-Zustellungsleistungen
Rechenzentrumsstandorte: Deutschland, Finnland, Bulgarien, Norwegen

(6) Resilient Data GmbH, Fraunhoferstraße 22, 82152 Planegg-Martinsried
Beauftragt mit der Speicherung verschlüsselter Datensicherungen
Rechenzentrumsstandorte: Deutschland

(7) Invopop S.L., Calle de Pradillo 42, 28002 Madrid, Spanien
Beauftragt mit der Übermittlung von Rechnungen über länderspezifische Übermittlungswege. Invopop kommt nur als Unterauftragnehmer nur zum Einsatz, wenn ein entsprechend gekennzeichnetes Erweiterungsmodul in der Software aktiviert wird. Die Erweiterungsmodule heißen beispielsweise "E-Rechnung für Italien (über Invopop)". Andernfalls findet keine Übertragung an Invopop statt.
Die Verwendung von Invopop kann die Verarbeitung von Daten in Drittländern beinhalten. Die von Invopop eingesetzten weiteren Unterauftragnehmer finden Sie auf dieser Website: https://www.invopop.com/legal-documents#sub-processors

Anlage B: Allgemeine technisch-organisatorische Maßnahmen nach Art. 32 DSGVO

(1) Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO)
   a) Alle Daten werden bei der Übertragung über öffentliche oder private Datennetzwerke immer nach modernen Standards verschlüsselt.
   b) Datensicherungen werden verschlüsselt auf Systemen abgelegt, die sowohl vom Produktivsystem als auch vom Aufbewahrungsort der Schlüssel physisch und logisch getrennt sind.
   c) Dem Auftragnehmer werden Funktionen in der Software zur Verfügung gestellt, um gespeicherte Daten zu anonymisieren oder pseudonymisieren, sodass der Personenbezug mit den bei uns gespeicherten Daten alleine nicht mehr möglich ist.
   d) Daten auf den Produktivsystemen selbst werden nicht verschlüsselt, da zur Sicherstellung der ständigen Abrufbarkeit die Schlüssel auf dem gleichen System gespeichert werden müssen und sich hieraus kein realer Sicherheitsvorteil ergäbe.

(2) Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)
   a) Zutrittskontrolle

aa) Auswahl von Rechenzentren von Subunternehmern, die durch geeignete Schließsysteme, Zutrittskontrollsysteme, Besucherregelung, Alarmanlage, Videoüberwachung und weitere geeignete Maßnahmen angemessen vor unberechtigtem Zutritt geschützt sind

b) Zugangskontrolle

aa) Zugang zu Systemen nur mit persönlicher Benutzerkennung und Kennwort. Eine Richtlinie für die Vergabe der Passwörter ist definiert.

bb) Arbeitsplatzrechner und Laptops nur mit verschlüsselter Festplatte und zeitgesteuerter Bildschirmsperre mit Wiederanmeldung bei Inaktivität

cc) Aktivierte und konfigurierte Firewall auf allen eingesetzten Systemen

dd) Der Wartungszugang auf Produktivsystemen ist nur mittels persönlicher, geheimer Schlüssel möglich

ee) Zwei-Faktor- oder Public-Key-Authentifizierung für den Mitarbeiterzugriff auf das Produktivsystem

ff) Protokollierung aller Logins auf Produktivsystemen

gg) Aktivierter und aktueller Virenschutz auf allen Windows-basierten Systemen

c) Zugriffskontrolle

aa) Benutzerrollen-/Gruppenkonzept

bb) Regelmäßige Überprüfung der Benutzerberechtigungen

cc) Wartungszugänge zu Produktivsystemen werden nur an eine minimale Anzahl technischer Mitarbeiter vergeben

dd) Normale Mitarbeiterzugänge zur Software verfügen standardmäßig über keinen Zugriff auf Kundendaten, dieser muss temporär aktiviert werden. Hierbei wird ein Protokoll der Zugriffsvorgänge erfasst.

ee) Papier-Schredder für Dokumentenvernichtung.

ff) Es ist eine Regelung zur Datenträgerentsorgung definiert.

d) Trennungskontrolle

aa) Firmendaten (Buchhaltung, Personalverwaltung, etc.) von Kundendaten getrennt

bb) Logische Trennung von Test- und Produktivsystemen

cc) Physische Trennung von Datensicherungen und Produktivsystemen

(3) Integrität (Art 32 Abs. 1 lit. b DS-GVO)

a) Weitergabekontrolle

aa) Verschlüsselte Übertragung personenbezogener Daten in internen und externen Netzwerken

bb) Identifizierung / Authentifizierung

b) Eingabekontrolle

aa) Mitarbeiter des Auftragnehmers dürfen grundsätzlich nur zur Erfüllung einer Weisung des Auftragnehmers oder zur Diagnose eines technischen Fehlers auf diese Daten zugreifen bzw. Daten eingeben, verändern oder löschen.

bb) Protokollierung bei Eingabe, Änderung und Löschung relevanter Daten

cc) Es werden regelmäßig Schulungen der Mitarbeiter zum Thema Datenschutz durchgeführt.

(4) Verfügbarkeit, Belastbarkeit, Wiederherstellbarkeit (Art 32 Abs. 1 lit. b, c DS-GVO)

a) Verfügbarkeitskontrolle

aa) Alle Server stehen in Rechenzentren in Deutschland

bb) Rechenzentren der Unterauftragnehmer weisen geeignete Schutzmaßnahmen auf (insbesondere redundante Stromversorgung, Überspannungsschutz, Schutz gegen Feuer und Wassereintritt)

cc) Redundante IT-Infrastruktur, die Funktionalität des Kernsystems kann trotz Ausfall eines beliebigen Servers sichergestellt werden

dd) Dauerhafte automatische Überwachung der korrekten Funktionalität

ee) Automatische Datensicherungen gemäß SLA in Anlage zum Hauptvertrag

ff) Prüfung der Rücksicherung/Wiederherstellung

gg) Firewalls im Einsatz

(5) Regelmäßige Überprüfung, Bewertung und Evaluierung (Art 32 Abs. 1 lit. d DSGVO)

a) Auftragskontrolle

aa) Der Auftragnehmer bietet auf Wunsch einen schriftlichen Vertrag, der den Datenverarbeitungszweck regelt und ein Weisungsrecht enthält.

bb) Mitarbeiter des Auftragnehmers kennen den Datenverarbeitungszweck. Sie erhalten schriftliche Weisung zum Umgang mit personenbezogenen Daten.

cc) Zwischen Auftragnehmer und evtl. Unterauftragnehmer wird bei Bedarf ein Auftragsverarbeitungsvertrag geschlossen.