

Vertrag über Auftragsverarbeitung im Sinne von Art. 28 Abs. 3 DSGVO

Inhalt

Vertrag über Auftragsverarbeitung im Sinne von Art. 28 Abs. 3 DSGVO	1
1. Allgemeine Bestimmungen und Vertragsgegenstand	2
2. Vertragslaufzeit und Kündigung	2
3. Weisungen des Auftraggebers	2
4. Kontrollbefugnisse des Auftraggebers	3
5. Allgemeine Pflichten von BoothPilot	3
6. Technische und organisatorische Maßnahmen	3
7. Unterstützungspflichten von BoothPilot	4
8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)	4
9. Mitteilungspflichten von BoothPilot	5
10. Vertragsbeendigung, Löschung und Rückgabe der Daten	5
11. Datengeheimnis und Vertraulichkeit	5
12. Haftung	6
13. Schlussbestimmungen	6
Anlage 1 – Auftragsdetails	7
Anlage 2 – Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO	9
Anlage 3 – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses	13

Vertrag über Auftragsverarbeitung im Sinne von Art. 28 Abs. 3 DSGVO

Version 2026-11 · Stand: Oktober 2026

zwischen

dem Operator gemäß dem im Registrierungsprozess geschlossenen Nutzungsvertrag (Stammdaten laut Operator-Account)

nachfolgend „Auftraggeber“

und

Bastian Egelseer – BoothPilot

Altmannshof 15

92284 Poppenricht

nachfolgend „BoothPilot“



1. Allgemeine Bestimmungen und Vertragsgegenstand

1.1 Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch BoothPilot (Art. 28 DSGVO). Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist der Auftraggeber.

1.2 Soweit BoothPilot im Rahmen der Plattform für den Auftraggeber Betreiber-Websites, Buchungsstrecken, Online-Galerien oder vergleichbare Onlineangebote bereitstellt oder hostet, erfolgt die Verarbeitung personenbezogener Daten im Verhältnis zu den Besuchern und Nutzern dieser Angebote ausschließlich im Auftrag des Auftraggebers. Der Auftraggeber bleibt insoweit allein Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. BoothPilot verarbeitet die personenbezogenen Daten ausschließlich nach Maßgabe dieses Vertrags, der dokumentierten Weisungen des Auftraggebers sowie der gesetzlichen Vorgaben. Eigene datenschutzrechtliche Verantwortlichkeiten von BoothPilot bleiben hiervon unberührt, soweit BoothPilot personenbezogene Daten zu eigenen Zwecken verarbeitet.

1.3 Inhalt des Auftrags, Kategorien betroffener Personen und Datenarten sowie Zweck der Vereinbarung sind **Anlage 1** zu entnehmen.

1.4 Die Verarbeitung der Daten durch BoothPilot findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR-Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung oder nach vorheriger Weisung des Auftraggebers.

2. Vertragslaufzeit und Kündigung

Dieser Vertrag tritt mit Abschluss des Nutzungsvertrags zwischen BoothPilot und dem Auftraggeber in Kraft. Laufzeit und Beendigung dieses Vertrags richten sich nach der Laufzeit und Beendigung des Nutzungsvertrags; eine isolierte ordentliche Kündigung dieses Vertrags ist ausgeschlossen. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Sofern und soweit nach Beendigung des Nutzungsvertrags oder dieses Vertrags die in Anlage 1 beschriebenen Daten weiterhin verarbeitet werden, gilt dieser Vertrag für diese Verarbeitungen bis zur Beendigung der Verarbeitung fort.

3. Weisungen des Auftraggebers

3.1 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. BoothPilot zu. BoothPilot informiert den Auftraggeber unverzüglich, falls BoothPilot der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit BoothPilot aus objektiv nachvollziehbaren Gründen anzweifelt, ist BoothPilot berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert. Besteht die Möglichkeit, dass BoothPilot durch das Befolgen der Weisung einem Haftungsrisiko ausgesetzt wird oder ihm sonstige Schäden drohen, kann die Durchführung der Weisung bis zur Klärung der Haftung im Innenverhältnis – oder bis zu einer Einräumung sonstiger angemessener Sicherheiten durch den Auftraggeber zur Abwendung von Schäden von BoothPilot – ausgesetzt werden.

3.2 Eine von den Weisungen oder ohne Weisungen des Auftraggebers abweichende Verarbeitung ist nur zulässig, wenn BoothPilot nach dem Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur Datenverarbeitung verpflichtet ist. Im Falle einer solchen Verarbeitung, informiert BoothPilot den Auftraggeber unverzüglich über beabsichtigte oder bereits eingeleitete Verarbeitung, es sei denn, dass das betreffende Recht der Europäischen Union oder des Mitgliedstaates eine solche Mitteilung aufgrund eines wichtigen öffentlichen Interesses verbietet; in diesem Fall erfolgt die Mitteilung unverzüglich, sobald die rechtlichen Hindernisse nicht mehr bestehen.

3.3 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisungen sind in begründeten Einzelfällen zulässig und werden vom Auftraggeber unverzüglich schriftlich oder in einem



elektronischen Format bestätigt. In der Bestätigung ist ausdrücklich zu begründen, warum keine Weisung in Textform erfolgen konnte. Der Auftraggeber hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu dokumentieren.

3.4 Der Auftraggeber benennt auf Verlangen von BoothPilot eine oder mehrere weisungsberechtigte Personen. Personelle Änderungen sind BoothPilot unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

4.1 Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig, im erforderlichen Umfang, zu kontrollieren. BoothPilot hat diese Überprüfungen – einschließlich Inspektionen – die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen und zu diesen beizutragen.

4.2 Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und nicht zu einer übermäßigen Beeinträchtigung des Geschäftsbetriebs führen. In der Regel soll eine Prüfung nur nach vorheriger Anmeldung erfolgen, es sei denn, die vorherige Anmeldung würde den Kontrollzweck gefährden. Wenn der Auftraggeber einen Prüfer bestellt, darf dieser nicht im unmittelbaren Wettbewerbsverhältnis zu BoothPilot stehen.

4.3 Die Ergebnisse der Kontrollen sind vom Auftraggeber in geeigneter Weise zu protokollieren.

4.4 BoothPilot verpflichtet sich, dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Verpflichtungen zur Verfügung zu stellen.

5. Allgemeine Pflichten von BoothPilot

5.1 Die Verarbeitung der vertragsgegenständlichen Daten durch BoothPilot erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur zulässig, wenn BoothPilot nach dem Recht der Europäischen Union oder der Mitgliedstaaten zur Datenverarbeitung verpflichtet ist. Im Falle einer solchen Verarbeitung, informiert BoothPilot den Auftraggeber unverzüglich über beabsichtigte oder bereits eingeleitete Verarbeitung, es sei denn, dass das betreffende Recht der Europäischen Union oder des Mitgliedstaates eine solche Mitteilung aufgrund eines wichtigen öffentlichen Interesses verbietet; in diesem Fall erfolgt die Mitteilung unverzüglich, sobald die rechtlichen Hindernisse nicht mehr bestehen.

5.2 BoothPilot hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

6. Technische und organisatorische Maßnahmen

BoothPilot hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in **Anlage 2** dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt. BoothPilot wird die technischen und organisatorischen Maßnahmen regelmäßig und anlassbezogen überprüfen und anpassen.



7. Unterstützungspflichten von BoothPilot

7.1 BoothPilot verpflichtet sich gem. Art. 28 Abs. 3 lit. e DSGVO, den Auftraggeber unter Berücksichtigung der Art der Vereinbarung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III, Art. 12 – 22 DSGVO genannten Rechte der betroffenen Personen, nachzukommen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten.

7.2 BoothPilot wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32-36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflichten bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der Informationen, die BoothPilot zur Verfügung stehen.

8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

8.1 BoothPilot ist zum Einsatz von Unterauftragsverarbeitern (Subunternehmern) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden Subunternehmerverhältnisse von BoothPilot sind diesem Vertrag abschließend in **Anlage 3** beigelegt. Für die in **Anlage 3** aufgezählten Subunternehmer gilt die Zustimmung mit Abschluss dieses Vertrags als erteilt.

8.2 Beabsichtigt BoothPilot den Einsatz weiterer Subunternehmer, wird BoothPilot dies dem Auftraggeber rechtzeitig - spätestens jedoch zwei Wochen - vor deren Einsatz in schriftlicher oder elektronischer Form anzeigen. Der Auftraggeber hat nach dieser Mitteilung zwei Wochen Zeit, der Hinzuziehung des/der Subunternehmer zu widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Hinzuziehung des/der Subunternehmer(s) als genehmigt. In dringenden Fällen (z.B. bei kurzfristig benötigten Fehleranalysen oder Mängelbeseitigungen), kann BoothPilot die Anzeige- und Widerspruchsfrist für Subunternehmer angemessen verkürzen. Erfolgt ein fristgerechter Widerspruch, dürfen die betroffenen Subunternehmer nicht eingesetzt werden. Widersprüche sind nur bei Vorliegen eines sachlichen Grundes zulässig, der der Widerspruchsbenachrichtigung beizulegen ist.

8.3 Subunternehmer werden von BoothPilot unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Sämtliche Verträge zwischen Auftragsverarbeiter (BoothPilot) und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Nebenleistungen, welche BoothPilot zur Ausübung von geschäftlichen Tätigkeiten in Anspruch nimmt, stellen keine Unterauftragsverhältnisse im Sinne des Art. 28 DSGVO dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen sowie sonstige Maßnahmen, welche die Vertraulichkeit und/oder Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. BoothPilot wird jedoch auch bei diesen Dritleistungen die Einhaltung der gesetzlichen Datenschutzstandards (insbesondere durch entsprechende Vertraulichkeitsvereinbarungen) sicherstellen.

8.4 Sämtliche Verträge zwischen BoothPilot und dem Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen.

8.5 Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.



9. Mitteilungspflichten von BoothPilot

9.1 Verstöße gegen diesen Vertrag, gegen Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß von BoothPilot selbst, einer bei BoothPilot angestellten Person, einem Subunternehmer oder einer sonstigen Person, die BoothPilot zur Erfüllung vertraglicher Pflichten eingesetzt hat, begangen wurde.

9.2 Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter BoothPilot um Auskunft, Berichtigung, Einschränkung der Verarbeitung oder Löschung, wird BoothPilot die Anfrage unverzüglich an den Auftraggeber weiterleiten und das weitere Vorgehen mit ihm abstimmen.

9.3 BoothPilot wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von denen auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat BoothPilot den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch welche die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

BoothPilot verpflichtet sich, nach Abschluss der Erbringung der Verarbeitungsleistungen alle vertragsgegenständlichen personenbezogenen Daten nach Wahl des Auftraggebers entweder zurückzugeben oder zu löschen und vorhandene Kopien zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Die Löschung der produktiv gespeicherten personenbezogenen Daten erfolgt spätestens innerhalb von 30 Tagen nach Vertragsende, soweit keine gesetzlichen Aufbewahrungsfristen oder sonstigen zulässigen Gründe für eine weitere Speicherung bestehen.

Personenbezogene Daten, die ausschließlich in Backups enthalten sind, werden nicht gesondert wiederhergestellt oder aktiv genutzt. Die Löschung erfolgt in zwei Stufen:

(1) Datenbank-Backups: Personenbezogene Daten, die in den täglichen Sicherungen des Datenbank-Anbieters enthalten sind, werden innerhalb der regulären Aufbewahrungsfrist von 7 Tagen nach Vertragsende automatisch überschrieben oder gelöscht.

(2) Eigene Sicherungen: Personenbezogene Daten, die in den von BoothPilot stündlich bei einem zweiten Anbieter abgelegten Sicherungen enthalten sind, werden innerhalb einer Aufbewahrungsfrist von 90 Tagen nach Vertragsende automatisch überschrieben oder gelöscht. Von dieser Frist sind Fotodateien nicht erfasst; diese werden durch die Spiegelung der Storage-Buckets mit dem nächsten Lauf nach erfolgter Löschung der produktiven Daten automatisch entfernt.

Soweit nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht, bleiben die Daten für die Dauer der gesetzlichen Aufbewahrungsfrist gespeichert.

11. Datengeheimnis und Vertraulichkeit

BoothPilot ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln. BoothPilot hat hierbei insbesondere durch geeignete Maßnahmen dafür zu sorgen, dass die ihm überlassenen auftragsgegenständlichen Daten nicht gegenüber unbefugten Dritten offengelegt werden; innerhalb seines Betriebs hat er durch geeignete Maßnahmen dafür zu sorgen, dass die vertragsgegenständlichen Daten nur denjenigen Personen gegenüber offengelegt werden, die die Daten zur Erfüllung



ihrer Aufgaben benötigen (Need-to-Know-Prinzip). BoothPilot verpflichtet sich, Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit bei BoothPilot aufnehmen.

12. Haftung

12.1 BoothPilot haftet ggü. dem Auftraggeber im Innenverhältnis nicht, wenn die haftungsauslösende Datenverarbeitung/Maßnahme in Folge einer Weisung des Auftraggebers durchgeführt wurde. Das gleiche gilt für Maßnahmen, die mit dem Auftraggeber abgestimmt wurden (z.B. TOMs nach Art. 32 DSGVO). Als Abstimmung gilt es auch, wenn eine Regelung in diesem Vertrag auf Verlangen des Auftraggebers eingefügt wurde.

12.2 Der Auftraggeber hat dafür zu sorgen, dass die originäre Erhebung der im Auftrag verarbeiteten Daten rechtmäßig erfolgt. Insbesondere hat er die ggf. erforderlichen Einwilligungen vollständig und korrekt einzuholen. Sofern BoothPilot im Außenverhältnis wegen eines Verstoßes gegen diese Pflicht in Anspruch genommen wird, haftet der Auftraggeber BoothPilot gegenüber im Innenverhältnis und stellt BoothPilot vom ggf. entstandenen Schaden frei.

12.3 Im Übrigen bleiben die gesetzlichen Haftungsregelungen (insb. Art. 82 DSGVO) unberührt.

13. Schlussbestimmungen

13.1 Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

13.2 Sind die Vertragsparteien Kaufleute, juristische Personen des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, ist der Sitz von BoothPilot Gerichtsstand für alle Streitigkeiten aus diesem Vertrag; ausschließliche Gerichtsstände bleiben hiervon unberührt.

13.3 Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

13.4 Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

13.5 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

13.6 Dieser Vertrag wird als Anlage zu den Allgemeinen Geschäftsbedingungen von BoothPilot im Rahmen des elektronischen Registrierungs- bzw. Bestellprozesses abgeschlossen. Die Annahme erfolgt durch aktive Bestätigung des Auftraggebers, insbesondere mittels Checkbox oder vergleichbarer Bestätigungsfunktion. BoothPilot protokolliert die angenommene Vertragsversion sowie Datum und Uhrzeit der Annahme. Eine handschriftliche Unterzeichnung ist nicht erforderlich; das elektronische Format genügt den Anforderungen des Art. 28 Abs. 9 DSGVO.



Anlage 1 – Auftragsdetails

Leistungen

Leistungen, bei denen Daten im Auftrag verarbeitet werden	Verarbeitete Datenarten	Betroffene Personenkategorien
Bereitstellung und Betrieb der Plattform (Operator-Dashboard, Cloud-Synchronisation, Kiosk-Software)	Stammdaten Kontaktdaten Zugangsdaten Nutzungsdaten	Auftraggeber Mitarbeiter des Auftraggebers
Speicherung und Bereitstellung von Eventfotos, GIFs und Online-Galerien (Laufzeit 30 Tage ab Versand des Galerie-Links, ohne Versand ab dem siebten Tag nach dem letzten Veranstaltungstag; automatische Löschung 7 Tage nach Ablauf)	Fotoaufnahmen mit Personenabbildungen Galerie-Metadaten (Zugangs-PIN, Ablaufdatum, Einwilligungs-Status)	Veranstaltungsgäste des Auftraggebers
KI-Bildbearbeitung von Gastfotos (Funktion „KI-Stile“; nur nach Einwilligung der Gäste an der Fotobox): Übermittlung des Fotos an den KI-Dienst, Rückgabe der bearbeiteten Fassung, Auftragsprotokoll ohne Bild	Fotoaufnahmen mit Personenabbildungen Auftragsprotokoll (Zeitpunkt, Stil, Modell, Version des Einwilligungstexts, Verweis auf Original- und Ergebnisfoto)	Veranstaltungsgäste des Auftraggebers
Eigene KI-Stile des Auftraggebers: Speicherung von Stil-Beschreibungen und bis zu drei Referenzbildern je Stil, automatische Prüfung, Übermittlung an den KI-Dienst mit jedem Auftrag	Texte und Bilder des Auftraggebers, gegebenenfalls mit Personenabbildungen	Auftraggeber auf Referenzbildern abgebildete Personen
Buchungsabwicklung für Endkunden (Buchungsstrecke/Widget, Magic-Link-Portal)	Name E-Mail-Adresse Telefonnummer Veranstaltungsdatum und -adresse Rechnungsanschrift (Firmenkunden)	Endkunden des Auftraggebers
Zahlungsanbindung für Endkunden-Buchungen (PayPal-Order-Erstellung, Rechnungs-PDF für Banküberweisung; Zahlung fließt direkt an den Auftraggeber)	Zahlungs-Metadaten (Order-IDs, Zahlungsstatus, Rechnungsnummern)	Endkunden des Auftraggebers
Hosting der Operator-Website inkl. Benachrichtigungsversand (E-Mail/SMS)	IP-Adressen und technische Zugriffsdaten E-Mail-Adressen Mobilfunknummern	Besucher der Website des Auftraggebers Auftraggeber



Leistungen, bei denen Daten im**Auftrag verarbeitet werden****Verarbeitete Datenarten****Betroffene Personenkategorien**

Technische Protokollierung,
Systemsicherheit und SupportAudit-Logs (Aktion, Zeitstempel,
IP-Adresse)
Druck-Logs
Box-Telemetrie
Inhalte von SupportanfragenAuftraggeber
Endkunden des Auftraggebers



Anlage 2 – Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

BoothPilot setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

1. Sicherung der Arbeitsstätte des Auftragsverarbeiters (Zutrittskontrolle)

Die Arbeitsstätte des Auftragsverarbeiters wird in folgender Weise gegen Einbruch und sonstige unbefugte Zutritte gesichert:

- Der Auftragsverarbeiter betreibt keine eigene Server-Infrastruktur; sämtliche Verarbeitung erfolgt in ISO-27001-zertifizierten Rechenzentren der in Anlage 3 genannten Cloud-Anbieter, deren Zutrittskontrollen gelten
- Abschließbare Arbeitsstätte; Arbeitsgeräte ausschließlich persönlich zugänglich

2. Sicherung der IT-Systeme des Auftragsverarbeiters (Zugangskontrolle)

Die IT-Systeme des Auftragsverarbeiters werden in folgender Weise gegen unbefugte Zugriffe (z.B. Hackerangriffe) gesichert:

- Zugriff ausschließlich über authentifizierte Verbindungen; individuelle Benutzerkonten, Passwörter ausschließlich als bcrypt-Hash gespeichert. Eine Mindestqualität (12 Zeichen, Stärkeprüfung, Abgleich gegen bekannte Datenlecks) wird technisch erzwungen
- Für Verwaltungszugänge des Auftragsverarbeiters ist eine Zwei-Faktor-Authentifizierung (TOTP) technisch zwingend; ohne zweiten Faktor entsteht keine Sitzung
- Für Betreiber-Konten wird die Einrichtung der Zwei-Faktor-Authentifizierung im Registrierungsablauf verbindlich durchlaufen und kann anschließend nicht selbst abgeschaltet werden. Ein als vertrauenswürdig bestätigtes Endgerät kann die Abfrage beim Anmelden für bis zu sieben Tage überspringen; für sicherheitsrelevante Änderungen (Passwort, E-Mail-Adresse, Bank- und Rechnungsdaten) wird der zweite Faktor unabhängig davon jedes Mal erneut abgefragt
- Verwaltungs- und Betreiberzugänge sind in getrennten Konten-Beständen geführt. Der Verwaltungszugang ist ausschließlich dem Inhaber vorbehalten; weitere Verwaltungskonten bestehen nicht. Ein abgestuftes Rollenmodell innerhalb des Verwaltungszugangs besteht bei einem Einzelunternehmen ohne Mitarbeiter nicht
- Sitzungsüberwachung mit Session-Fingerprinting und zentraler Sperrmöglichkeit (Killswitch); erhöhte Bestätigungsstufe für kritische Aktionen (Sudo-Modus)
- Festplattenverschlüsselung der Arbeitsgeräte; aktuelle Betriebssysteme und zeitnahe Sicherheitsupdates

3. Protokollierung von Datenverarbeitungsprozessen (Eingabekontrolle)

Folgende Maßnahmen stellen sicher, dass der Auftragsverarbeiter jederzeit erkennen kann, welche Datenverarbeitungsprozesse in seinen Datenverarbeitungssystemen stattgefunden haben (z.B. Eingabe, Veränderung, Sperrung oder Löschung):

- Sicherheitsrelevante Vorgänge – Anmeldungen, Zwei-Faktor-Vorgänge, Eingriffe in Konten, Buchungs- und Belegvorgänge, Löschungen sowie automatisierte Systemläufe – werden in einem Protokoll mit Akteur, Aktion, betroffenem Objekt und Zeitstempel festgehalten. Bei Anmelde-, Authentifizierungs- und Verwaltungsvorgängen werden zusätzlich IP-Adresse und Browserkennung erfasst. Eine Protokollierung sämtlicher Änderungen an Stammdaten der Betreiber (etwa Pakete, Zusatzleistungen, Website-Inhalte) erfolgt nicht durchgängig



- Im Protokoll wird der Akteur primär über eine interne Kennung (UUID) referenziert. E-Mail-Adresse und Objektbezeichnung werden zusätzlich im Klartext geführt, solange das Konto besteht, weil das Protokoll sonst nicht auswertbar wäre. Bei Löschung eines Betreiberkontos werden E-Mail-Adresse, Objektbezeichnung und Zusatzdaten aller zugehörigen Protokolleinträge unwiderruflich entfernt; die Vorgangsspur selbst bleibt erhalten
- Protokolleinträge zu rein betrieblichen Vorgängen – Anmeldungen, automatisierte Systemläufe, Empfangsquittungen – werden nach einem Jahr gelöscht. Alle übrigen Protokolleinträge, insbesondere zu Einwilligungen, Vertragsannahmen, Widerrufen und Belegvorgängen, werden nach drei Jahren gelöscht
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung durch individuelle Benutzerkonten

4. Sichere Löschung von Daten

Folgende Maßnahmen stellen die ordnungsgemäße Löschung der vertragsgegenständlichen Daten sicher:

- Dokumentiertes Löschkonzept: Die Online-Galerie steht dem Endkunden 30 Tage zur Verfügung. Die Frist beginnt mit dem Versand des Galerie-Links; erfolgt kein Versand, beginnt sie sieben Tage nach dem letzten Veranstaltungstag. Der Betreiber kann den Zeitraum im Einzelfall verlängern. Sieben Tage nach Ablauf werden sämtliche Fotodateien – Originale, Vorschaubilder und Archivdateien – sowie die zugehörigen Datenbankeinträge durch einen täglich laufenden automatischen Vorgang unwiderruflich gelöscht. Der Endkunde wird drei Tage vor Ablauf per E-Mail vorgewarnt
- KI-Stile: Für die KI-Bearbeitung wird das Foto an den KI-Dienst übermittelt und nicht zusätzlich gespeichert; das fertige KI-Bild folgt den Fristen der Online-Galerie. Das Auftragsprotokoll (ohne Bild) bleibt als Nachweis der Einwilligung bis zur Löschung des Kontos; die Verweise auf Fotos entfallen mit deren Löschung. Eigene Stile, ihre früheren Fassungen und Referenzbilder werden spätestens mit dem Konto gelöscht
- Löschung aller personenbezogenen Daten binnen 30 Tagen nach Vertragsende, vorbehaltlich gesetzlicher Aufbewahrungspflichten. Die Löschung wird verwaltungsseitig ausgelöst und im Rahmen einer dokumentierten Wiederholung überwacht; sie umfasst Datenbankinhalte, Foto- und Dateispeicher sowie die Anmeldedaten. Konten aus der kostenlosen Testphase werden automatisiert 90 Tage nach Ablauf der Testphase gelöscht, mit Vorwarnung 30 Tage vorher
- Daten, die ausschließlich in Sicherungen enthalten sind, werden nicht gesondert wiederhergestellt oder aktiv genutzt. Sicherungen des Datenbestands werden spätestens nach 90 Tagen überschrieben. Fotodateien folgen der Löschung unmittelbar: Die Spiegelung des Dateispeichers übernimmt Löschungen mit dem nächsten Lauf, so dass gelöschte Aufnahmen auch dort nicht länger als 24 Stunden fortbestehen
- Keine physischen Datenträger mit vertragsgegenständlichen Daten (rein cloudbasierte Verarbeitung)

5. Datenschutz bei den Subunternehmern des Auftragsverarbeiters

Folgende Maßnahmen stellen sicher, dass sich die vom Auftragsverarbeiter ausgewählten Subunternehmer datenschutzkonform verhalten:

- Auswahl der Subunternehmer unter Berücksichtigung ihrer technischen und organisatorischen Maßnahmen; bevorzugt Anbieter mit Datenhaltung in der EU
- Vereinbarungen zur Auftragsverarbeitung nach Art. 28 Abs. 4 DSGVO; bei Anbietern mit Sitz außerhalb der EU zusätzlich Standardvertragsklauseln bzw. Zertifizierung nach dem EU-US Data Privacy Framework
- Überprüfung der Vereinbarungen und Zertifizierungen mindestens einmal jährlich



6. Sicherung von Daten bei Transport und Übermittlung (Weitergabekontrolle)

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) vor unbefugten Dritten geschützt werden:

- Sämtliche externen Verbindungen laufen ausschließlich verschlüsselt über TLS in einer aktuellen Version (mindestens TLS 1.2, üblicherweise TLS 1.3). Ein unverschlüsselter Aufruf wird per HTTP-Strict-Transport-Security (ein Jahr Gültigkeit, einschließlich aller Unterdomänen) unterbunden
- Alle Auslieferungen tragen eine Content-Security-Policy mit ausdrücklicher Positivliste der zulässigen Herkunfte sowie die Schutz-Header X-Frame-Options, X-Content-Type-Options, Referrer-Policy und Permissions-Policy. Ausgenommen ist ausschließlich das zur Einbettung bestimmte Buchungs-Widget
- Kein Transport physischer Datenträger

7. Datensicherung und Backups (Verfügbarkeit und Wiederherstellbarkeit)

Folgende Maßnahmen stellen sicher, dass die vertragsgegenständlichen Daten jederzeit verfügbar sind:

- Zweistufiges Sicherungskonzept. Erste Stufe: Der Datenbank-Anbieter sichert die Datenbank täglich vollständig; die Aufbewahrungsdauer dieser Sicherungen beträgt sieben Tage. Zweite Stufe: Der Auftragsverarbeiter erstellt zusätzlich stündlich einen eigenen, verschlüsselten Abzug des Datenbestands und legt diesen bei einem zweiten, vom Datenbank-Anbieter unabhängigen Anbieter mit Sitz in der Europäischen Union ab; die Aufbewahrungsdauer dieser Abzüge beträgt 90 Tage
- Der Dateispeicher mit den Fotoaufnahmen wird zu demselben zweiten Anbieter gespiegelt. Die Spiegelung übernimmt Löschungen, so dass sie den Löschfristen dieser Anlage nicht entgegensteht
- Der maximale Datenverlust im Wiederherstellungsfall entspricht dem Abstand zwischen zwei Sicherungsläufen und beträgt damit höchstens eine Stunde
- Die Wiederherstellbarkeit aus der Sicherung wird mindestens vierteljährlich geprüft und protokolliert. Geprüft werden Vollständigkeit und Konsistenz der wiederhergestellten Datenbestände
- Live-Monitoring der Systeme: ein Fehler- und Leistungs-Monitoring der Anwendung, eine Verfügbarkeitsprüfung im Minutentakt sowie ein automatischer Statusbericht jeder Fotobox alle zehn Minuten. Bleibt der Statusbericht einer Box aus oder meldet sie einen Drucker- oder Upload-Fehler, wird der zuständige Betreiber nach einer Bestätigungsphase automatisch per E-Mail und auf Wunsch per SMS benachrichtigt
- Die physische Sicherung der Serverräume (USV, Brandschutz, Klimatisierung) obliegt den ISO-27001-zertifizierten Rechenzentren der Cloud-Anbieter

8. Sonstige Datenschutzmaßnahmen

Folgende weitere Datenschutzmaßnahmen wurden implementiert:

- Logische Mandantentrennung in zwei Stufen. Auf Datenbankebene ist auf allen Tabellen Row-Level-Security aktiviert; ein direkter Zugriff über die Daten-Schnittstelle liefert einem Betreiber ausschließlich die eigenen Datensätze. Der Anwendungsserver greift zusätzlich über ein privilegiertes Dienstkonto zu; dort wird die Zuordnung zum Betreiberkonto in jedem einzelnen Endpunkt anhand der angemeldeten Sitzung erzwungen. Beide Ebenen werden regelmäßig geprüft: ein nächtlicher automatisierter Test misst den von außen tatsächlich erreichbaren Zustand, ein Prüfprogramm kontrolliert jede neue Datenbankänderung
- Trennung von Produktiv- und Testsystem
- Sämtliche Übertragungen erfolgen verschlüsselt. Ruhende Daten werden auf Ebene der eingesetzten Cloud-Anbieter verschlüsselt gespeichert. Zusätzlich verschlüsselt der Auftragsverarbeiter besonders schutzbedürftige



Felder anwendungsseitig: Zwei-Faktor-Geheimnisse mit AES-256-GCM, Passwörter und Wiederherstellungscodes als bcrypt-Hash, Geräte-Token als SHA-256-Hash. Fotodateien liegen ausschließlich in nicht-öffentlichen Speicherbereichen und sind nur über zeitlich befristete, signierte Verweise erreichbar

- Verarbeitungsverzeichnis nach Art. 30 DSGVO, getrennt nach eigener Verantwortlichkeit und Auftragsverarbeitung; jährliche Überprüfung
- Dokumentierter Ablauf zur Behandlung von Sicherheitsvorfällen und Verletzungen des Schutzes personenbezogener Daten mit festgelegten Schritten zur Eindämmung, Aufklärung, Benachrichtigung und Nachbereitung. Jeder Vorfall wird dokumentiert, auch wenn keine Meldepflicht besteht

9. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragsverarbeiter wird die in dieser Anlage beschriebenen technischen und organisatorischen Maßnahmen im Abstand von 12 Monaten und anlassbezogen, prüfen, evaluieren und bei Bedarf anpassen.



Anlage 3 – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

(Unternehmens-) Name und Anschrift	Beschreibung der Leistung	Land der Leistungserbringung
Supabase, Inc., 548 Market St, PMB 86778, San Francisco, CA 94104, USA	Datenbank, Dateispeicher, Authentifizierung (Datenhaltung Region Frankfurt)	EU (Deutschland); Konzernsitz USA – DPF/SCC
Vercel Inc., 340 S Lemon Ave #4133, Walnut, CA 91789, USA	Web-Hosting (Dashboard, Operator-Websites, API; Region fra1)	EU (Deutschland); Konzernsitz USA – DPF/SCC
Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA	CDN, Reverse-Proxy/WAF, Bot-Schutz (Turnstile)	EU/weltweit; Konzernsitz USA – DPF/SCC
Plus Five Five, Inc. (Resend), 2261 Market Street #5039, San Francisco, CA 94114, USA	Transaktionaler E-Mail-Versand (EU-Versandregion)	EU; Konzernsitz USA – DPF/SCC
BunnyWay, informacijske storitve d.o.o., Dunajska cesta 165, 1000 Ljubljana, Slowenien	Update-Hosting der Kiosk-Software	EU
Upstash, Inc., San Francisco, USA	Cron-Scheduling, Rate-Limiting (Redis; Datenhaltung Region Frankfurt)	EU (Deutschland); Konzernsitz USA – DPF/SCC
seven communications GmbH & Co. KG, Kiel, Deutschland (seven.io)	SMS-Versand (Benachrichtigungen an den Auftraggeber)	Deutschland
ALL-INKL.COM – Neue Medien Münnich, Inh. René Münnich, Hauptstraße 68, 02742 Friedersdorf, Deutschland	E-Mail-Postfach (hallo@boothpilot.de, u. a. Supportanfragen) und DNS	Deutschland
Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Irland	KI-Bildbearbeitung und automatische Prüfung eigener Stile (Gemini über Google Cloud Vertex AI, Multiregion „eu“; Bildbearbeitung nur nach Einwilligung der betroffenen Person)	EU (Multiregion „eu“); Google-Konzern USA – DPF/SCC
Anthropic, PBC, 548 Market Street, PMB 90375, San Francisco, CA 94104, USA	KI-Chatbot auf Operator-Websites	USA – SCC
Functional Software, Inc. (Sentry), San Francisco, USA	Error-Tracking, Performance-Monitoring	USA – DPF/SCC
Sanity AS, Oslo, Norwegen	Content-Management-System für den Blog	EWK (Norwegen)
Microsoft Ireland Operations Ltd., Dublin, Irland (Azure Trusted Signing)	Code-Signierung der Windows-Installer (administrative Daten)	EU/USA – DPF/SCC
PayPal (Europe) S.à r.l. et Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxemburg	Technische Bereitstellung der PayPal-Schnittstelle zur Zahlungsabwicklung des Auftraggebers; PayPal verarbeitet Zahlungsdaten als eigenständig Verantwortlicher nach seinen eigenen Datenschutzbestimmungen	EU (Luxemburg)

