THEPLUS UG (HAFTUNGSBESCHRÄNKT) · STAND 11.09.2026

Technisch-organisatorische Maßnahmen

Nach Art. 32 DS-GVO, zur Vereinbarung über Auftragsverarbeitung nach Art. 28 DS-GVO. Gegenstand ist das Teilnehmer-, Ticketing- und Badge-Management-System „Quick Event". Die Gliederung folgt den üblichen Vordrucken, damit dieses Dokument ein solches Formular eins zu eins ersetzen kann.

0 · GELTUNGSBEREICH UND VERANTWORTUNGSABGRENZUNG

Wir betreiben kein eigenes Rechenzentrum. Die Anwendung läuft auf angemieteter Infrastruktur der Hetzner Online GmbH: das Produktivsystem im Rechenzentrum **Nürnberg**, die Datensicherungen im Rechenzentrum **Falkenstein**. Beide Standorte liegen in Deutschland. Maßnahmen der physischen Sicherheit (Ziff. 2.1) liegen daher beim Rechenzentrumsbetreiber; alle übrigen Maßnahmen verantworten wir.

Wir sind ein Kleinstunternehmen mit zwei Beschäftigten. Der Kreis der Personen mit Zugang zu personenbezogenen Daten ist damit abschließend bestimmt und namentlich bekannt. Die Maßnahmen sind darauf ausgelegt: Wo größere Organisationen Freigabeprozesse zwischen Abteilungen brauchen, ersetzt hier die vollständige Personenidentität von Entwicklung und Betrieb den Prozess. Das ist ausdrücklich so benannt und nicht als Verfahren beschrieben, das es nicht gibt.

1 · PSEUDONYMISIERUNG UND VERSCHLÜSSELUNG (ART. 32 ABS. 1 LIT. A)

Verschlüsselung bei der Übertragung

- Sämtlicher Datenverkehr zwischen Endgeräten und Anwendung ausschließlich über TLS (HTTPS); unverschlüsselte Verbindungen werden nicht angenommen.
- Verbindungen zwischen Anwendung und Datenbank sowie zu allen Auftragsverarbeitern (Zahlungsabwicklung, E-Mail-Versand, Fehler-Überwachung) ausschließlich TLS-verschlüsselt.
- E-Mail-Versand über TLS-gesicherte Übergabe an den Versanddienstleister.

Verschlüsselung bei der Speicherung

- Verschlüsselung der Datenträger auf Ebene der Rechenzentrumsinfrastruktur.
- Passwörter ausschließlich als Hash mit Zufallssalz; ein Rückschluss auf das Klartextpasswort ist ausgeschlossen. Zugang ist alternativ ohne Passwort über einen Identitätsanbieter möglich.
- Zugangsdaten zu Fremdsystemen liegen ausschließlich in der Geheimnisverwaltung der Betriebsumgebung — nicht im Quelltext und nicht in der Datenbank.

Pseudonymisierung und Datensparsamkeit

- Die Betriebsanalyse arbeitet mit pseudonymen Kennungen. Personenprofile werden nur für angemeldete Nutzer des Veranstalters geführt, nicht für Teilnehmende.
- Ein automatisches Mitschneiden von Klicks und Eingaben ist projektweit abgeschaltet.
- Sitzungsaufzeichnung ist grundsätzlich deaktiviert und technisch auf die Oberflächen des Veranstalters begrenzt; die Anmeldestrecke der Teilnehmenden wird nicht aufgezeichnet. Eingabefelder sind dort ausnahmslos maskiert (Verbot mit Ausnahmeliste, nicht umgekehrt).

- Anwendungsprotokolle enthalten keine Klarnamen, E-Mail-Adressen oder Zugangsdaten, sondern Kennungen und Wahrheitswerte („E-Mail vorhanden: ja"). Das ist als verbindliche Entwicklungsvorgabe dokumentiert.

2 · VERTRAULICHKEIT (ART. 32 ABS. 1 LIT. B)

2.1 Zutrittskontrolle (physisch)

Verantwortet durch die Hetzner Online GmbH für die Rechenzentren Nürnberg (Produktivsystem) und Falkenstein (Sicherungen): umzäuntes Gelände, Videoüberwachung, Vereinzelungsanlagen, elektronische Zutrittskontrolle mit Protokollierung, Zutritt nur für namentlich berechtigtes Personal.

Der Rechenzentrumsbetreiber ist nach ISO/IEC 27001:2022 zertifiziert (SOCOTEC Certification Deutschland GmbH, Zertifikat ZN-2025-35, gültig 27.09.2025 bis 26.09.2028). Der Geltungsbereich umfasst „alle Hosting-Dienstleistungen und die Rechenzentren"; die genutzten Standorte Nürnberg und Falkenstein/Vogtland sind im Zertifikatsanhang ausdrücklich aufgeführt. Ergänzend liegt ein BSI-C5-Testat Typ 2 vor. Beide Nachweise legen wir auf Anforderung vor.

Unsere Arbeitsplätze: abschließbare Geschäftsräume, keine Aufbewahrung personenbezogener Daten auf Papier. Vor Ort eingesetzte Geräte (Notebooks, Druckstationen) bleiben während der Veranstaltung unter Aufsicht des eingesetzten Personals.

2.2 Zugangskontrolle (Systemzugang)

- Persönliche, nicht geteilte Benutzerkonten; keine Sammel- oder Funktionskonten.
- Anmeldung mit Passwort und Salt-Hash-Verfahren oder über Identitätsanbieter.
- Serverseitige Begrenzung der Anmeldeversuche über einen gemeinsamen, datenbankgestützten Zähler mit Sonderregeln für sicherheitsrelevante Endpunkte; die Zählung ist instanzübergreifend und lässt sich nicht durch Lastverteilung umgehen.
- Bot-Abwehr auf den Anmelde- und Registrierungsendpunkten, die im Fehlerfall schließt statt durchzulassen.
- Die Erkennung der Client-Adresse liest ausschließlich den vom Betreiber gesetzten Kopfeintrag, nicht den vom Aufrufer beliebig setzbaren — Anfragebegrenzungen sind dadurch nicht durch Kopfzeilen-Manipulation zu umgehen.
- Sitzungen laufen nach spätestens 30 Tagen ab; Einmalcodes für den Gastzugang nach 10 Minuten.
- Zugang zur Betriebsumgebung (Server, Datenbank, Geheimnisverwaltung) nur für die Geschäftsführung, über persönliche Konten mit Zwei-Faktor-Authentifizierung.

2.3 Zugriffskontrolle (Berechtigungen innerhalb des Systems)

- Der Zugriff auf eine Veranstaltung entsteht aus genau zwei dokumentierten Quellen: Eigentümerschaft oder eine ausdrückliche Mitgliedschaft. Die Zugehörigkeit zu einer Organisation begründet **keinen** Zugriff.
- Berechtigungen sind je Produktmodul und Rechteart getrennt vergebbar; der Veranstalter steuert selbst, wer welchen Bereich lesen oder bearbeiten darf.
- Die Rechteprüfung ist als eigener, ohne Datenbank testbarer Vertrag umgesetzt und durch automatisierte Tests abgesichert. Eine Abweichung zwischen Modulliste und Rechteschlüsseln bricht die Übersetzung des Quelltextes, statt an einer Prüfstelle still „kein Recht" zu liefern.
- Serverseitige Prüfung an jedem Endpunkt; die Oberfläche ist keine Zugriffsschranke.

2.4 Trennungskontrolle

- Mandantentrennung auf Datenebene: Jeder Datensatz trägt die Event-Zugehörigkeit, jede Abfrage ist darauf eingeschränkt.
- Die Konten der Teilnehmenden liegen in eigenen Tabellen, getrennt von den Konten der Veranstalter-Nutzer. Dieselbe Person in zwei Veranstaltungen sind zwei getrennte Konten — über das Datenmodell erzwungen, nicht über eine Regel.
- Getrennte Sitzungs-Merkmale je Veranstaltung; die Anmeldung an einer Veranstaltung meldet nicht von einer anderen ab.
- Entwicklung findet in lokalen Umgebungen mit eigenem Datenbestand statt, getrennt von der Produktion. In Entwicklung, Test und Vorführung werden **keine echten Teilnehmerdaten** verwendet.

3 · INTEGRITÄT (ART. 32 ABS. 1 LIT. B)

3.1 Weitergabekontrolle

- Datenübertragung ausschließlich TLS-verschlüsselt (Ziff. 1).
- Datenexporte (Teilnehmerlisten, Umsätze) nur für berechtigte Nutzer des Veranstalters, ausgelöst über die Anwendung, mit serverseitiger Rechteprüfung.
- Kein Versand personenbezogener Daten über unverschlüsselte Kanäle; keine Weitergabe an Dritte außer den benannten Auftragsverarbeitern (siehe Beilage „Auftragsverarbeiter und Datenhaltung").
- Zahlungsdaten (Kartendaten) werden zu keinem Zeitpunkt von uns erhoben, verarbeitet oder gespeichert; die Eingabe erfolgt unmittelbar beim Zahlungsdienstleister.

3.2 Eingabekontrolle

- Änderungen an Teilnehmer- und Buchungsdaten sind dem auslösenden Konto zuordenbar; Anlage- und Änderungszeitpunkte werden je Datensatz geführt.
- Jeder Check-in- und Check-out-Vorgang wird einzeln mit Zeitpunkt, Richtung und Check-in-Punkt protokolliert.
- Der Versandstatus jeder E-Mail wird je Empfänger protokolliert und ist im Nachgang nachvollziehbar.
- Anwendungsprotokolle in strukturierter, maschinell auswertbarer Form mit Schweregrad. Aufbewahrung 30 Tage, danach automatische Löschung — auf den Zweck zugeschnitten und bewusst kurz gehalten (Art. 5 Abs. 1 lit. e DS-GVO).
- Davon zu unterscheiden sind fachliche Aufzeichnungen (Check-in-Protokoll, Versandstatus, Änderungszeitpunkte). Sie sind kein Betriebsprotokoll, sondern Bestandteil der Auftragsdaten und werden mit diesen nach Ziff. 7 herausgegeben und gelöscht.

4 · VERFÜGBARKEIT UND BELASTBARKEIT (ART. 32 ABS. 1 LIT. B UND C)

4.1 Verfügbarkeitskontrolle

- Betrieb in einem Rechenzentrum mit unterbrechungsfreier Stromversorgung, Netzersatzanlage, redundanter Netzanbindung und Brandfrüherkennung (Leistung des Rechenzentrumsbetreibers).
- Datensicherung der Datenbank als **Point-in-Time-Recovery**: fortlaufende Sicherung der Transaktionsprotokolle, wodurch der Datenbestand auf einen beliebigen Zeitpunkt innerhalb des

Sicherungsfensters zurückgeführt werden kann. Die Sicherungen liegen in einem ausschließlich dafür genutzten Speicher im Rechenzentrum Falkenstein, während das Produktivsystem in Nürnberg läuft — rund 300 km entfernt, in einem anderen Gebäude, Brandabschnitt und Stromnetz, und beides innerhalb Deutschlands. Sicherungen sind verschlüsselt abgelegt. Zugesichertes Sicherungsfenster: mindestens 30 Tage rückwirkend.

- Schutz auf Netzebene durch Paketfilter; nach außen sind ausschließlich die für den Betrieb erforderlichen Dienste erreichbar.
- Fehler- und Ausfallüberwachung der Anwendung mit Benachrichtigung der Geschäftsführung.
- **Besonderheit vor Ort:** Die Druckstation erzeugt Badges lokal auf dem angeschlossenen Rechner. Ein kurzzeitiger Ausfall der Netzverbindung unterbricht den Einlass daher nicht. Ergänzend wird je Veranstaltungsort eine vom Netz der Location unabhängige Mobilfunk-Rückfallebene bereitgestellt.

4.2 Rasche Wiederherstellbarkeit — Wiederanlaufkonzept

Die Werte sind Wiederanlaufziele (RTO/RPO), also **zugesicherte Obergrenzen** — nicht Durchschnittswerte. Anwendung und Datenbank werden getrennt wiederhergestellt; die Gesamtzeit ist deshalb nicht die Summe beider Werte, sondern der längere von beiden zuzüglich des Umschaltvorgangs.

SZENARIO	MASSNAHME	WIEDERANLAUFZIEL
Ausfall der Anwendung	Neustart des Anwendungsprozesses, andernfalls Neuausbringung aus dem versionierten Stand	RTO ≤ 15 Minuten
Fehlerhafte Auslieferung	Rückführung auf den zuletzt lauffähigen Stand	RTO ≤ 15 Minuten
Datenverlust oder -beschädigung in der Datenbank	Point-in-Time-Recovery auf einen Zeitpunkt vor dem Ereignis (Ziff. 4.1)	RPO ≤ 5 Minuten RTO ≤ 1 Stunde
Ausfall des E-Mail-Versands	Erneuter Versand aus der Anwendung; der Versandstatus je Empfänger ist gespeichert, Doppelversand wird dadurch vermieden	laufender Betrieb
Netzausfall am Veranstaltungsort	Mobilfunk-Rückfallebene; Badges werden lokal auf der Druckstation erzeugt	Einlass unterbrechungsfrei

Grundlage der Werte für die Anwendung. Im Rahmen der Betriebsumstellung gemessen: Neustart des Anwendungsprozesses 1,1 Sekunden, Austausch des vorgelagerten Proxys 8 Sekunden, vollständige Neuausbringung rund 5 Minuten, Rückführung auf den vorherigen Stand rund 4,5 Minuten. Der ungünstigste real aufgetretene Fall lag bei 7 Minuten einschließlich Fehlersuche. Das zugesicherte Ziel von 15 Minuten liegt bewusst darüber.

Grundlage der Werte für die Datenbank. In einer Wiederherstellungsübung gemessen: Rückspielen von 1.991 Dateien (67,5 MB) in 35 Sekunden, Datenbank nach weiteren 15 Sekunden betriebsbereit, nachdem die Transaktionsprotokolle nachgefahren waren — zusammen unter einer Minute. Die Vollständigkeit wurde anhand der Datensatzzahlen je Tabelle geprüft. Das zugesicherte Ziel von einer Stunde liegt bewusst weit darüber, weil der Datenbestand zum Veranstaltungszeitpunkt größer sein wird als in der Übung.

Der Wiederanlauf wird vor Beginn eines Leistungszeitraums vollständig erprobt und das Ergebnis mit gemessener Dauer dokumentiert. Die Erprobung umfasst beide Teile getrennt: das Rückspielen einer Datenbanksicherung in eine Nebeninstanz und die Neuausbringung des Anwendungscontainers.

4.3 Risikoanalyse

Bewertet nach Eintrittswahrscheinlichkeit und Schwere für die Rechte und Freiheiten der betroffenen Personen (Art. 32 Abs. 1 DS-GVO):

RISIKO	BEWERTUNG	MASSNAHME
Unbefugter Zugriff auf die Teilnehmerliste (vertrauliche Gästeliste)	mittel / hoch	Rechteprüfung serverseitig je Endpunkt, Mandantentrennung auf Datenebene, persönliche Konten, Begrenzung der Anmeldeversuche
Übernahme eines Veranstalter-Kontos	gering / hoch	Hash-Verfahren, Bot-Abwehr, Anfragebegrenzung, Sitzungsablauf, Zwei-Faktor für Betriebszugänge
Verwechslung von Daten zwischen Veranstaltungen	gering / mittel	Event-Zugehörigkeit als Pflichtfeld, getrennte Konten je Veranstaltung, automatisierte Tests
Datenverlust	gering / hoch	Sicherung mit erprobtem Rückspielen (Ziff. 4.2)
Ausfall am Veranstaltungstag	mittel / mittel	lokale Badge-Erzeugung, Mobilfunk-Rückfallebene, Vor-Ort-Betreuung an allen Veranstaltungstagen
Unbeabsichtigte Offenlegung durch Protokolle	gering / mittel	Protokollvorgabe ohne personenbezogene Inhalte; Maskierung in der Betriebsanalyse

5 · REGELMÄSSIGE ÜBERPRÜFUNG UND EVALUIERUNG (ART. 32 ABS. 1 LIT. D; ART. 25)

- **Datenschutz-Management.** Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO. Ansprechpartner für Datenschutz ist Maurice Alexander Holtus, Kohlhökerstr. 59–60, 28203 Bremen, Telefon +49 1520 4298335, hi@the-plus.io.
- **Überprüfung der Maßnahmen.** Dieses Dokument wird mindestens jährlich sowie anlassbezogen (wesentliche Änderung der Verarbeitung, neuer Auftragsverarbeiter, Sicherheitsvorfall) überprüft und fortgeschrieben. Ergebnis und Datum werden schriftlich festgehalten.
- **Umgang mit Sicherheitsvorfällen.** Feststellung, Eindämmung, Bewertung der Meldepflicht nach Art. 33 DS-GVO und Meldung an den Auftraggeber unverzüglich, spätestens innerhalb von **24 Stunden** nach Kenntnis, mit Beschreibung, betroffenen Datenkategorien, Umfang und ergriffenen Maßnahmen.
- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2).** Erhoben wird nur, was das Anmeldeformular des Veranstalters vorsieht. Sitzungsaufzeichnung und automatisches Mitschneiden sind ab Werk aus. Maskierung von Eingaben ist Verbot mit Ausnahmeliste.
- **Auftragskontrolle.** Verarbeitung ausschließlich auf dokumentierte Weisung; Auswahl der Auftragsverarbeiter nach Sitz, Verarbeitungsort und Vertragslage; Verträge nach Art. 28 Abs. 4 DS-GVO mit allen benannten Unterauftragnehmern.
- **Änderungskontrolle.** Sämtliche Änderungen an der Anwendung sind versioniert und nachvollziehbar. Vor der Auslieferung laufen automatisierte Tests; jede Auslieferung ist auf einen zuvor lauffähigen Stand zurückführbar (Ziff. 4.2). Eine dauerhaft betriebene Vorproduktionsumgebung unterhalten wir nicht — die Rückführbarkeit tritt an ihre Stelle, und das ist hier so benannt statt als Verfahren beschrieben, das es nicht gibt.

Dafür liegen schriftliche Regelungen vor:

- ☒ Dokumentiertes Verfahren zur Überprüfung, Bewertung und Evaluierung der TOM

- □ Informationssicherheitskonzept/-handbuch
- □ Dokumentierte Prozesse für den IT-Betrieb, z. B. Ausgabe und Rücknahme von Mobilgeräten

6 · WEITERE DOKUMENTIERTE REGELUNGEN

- ☒ interne Verhaltensregeln
- ☒ Risikoanalyse (Ziff. 4.3)
- ☒ Wiederanlaufkonzept (Ziff. 4.2)
- ☒ allgemeine Datensicherheitsbeschreibung (dieses Dokument)
- □ eigenes Zertifikat — Zertifizierungsstelle: keine. Zertifiziert ist der Rechenzentrumsbetreiber (Ziff. 2.1)

Interne Verhaltensregeln (Kurzfassung)

- Alle Personen mit Zugang zu personenbezogenen Daten sind vor Aufnahme der Tätigkeit schriftlich auf die Vertraulichkeit verpflichtet (Art. 28 Abs. 3 lit. b DS-GVO). Die Verpflichtung gilt über das Ende der Tätigkeit hinaus.
- Zugriff nur, soweit für die Aufgabe erforderlich. Kein Zugriff „aus Neugier".
- Keine Speicherung von Teilnehmerdaten auf privaten Geräten, in privaten Konten oder in Werkzeugen, die nicht als Auftragsverarbeiter benannt sind.
- Keine echten Teilnehmerdaten in Entwicklung, Test oder Vorführung.
- Sicherheitsvorfälle und Verdachtsfälle werden unverzüglich der Geschäftsführung gemeldet.

7 · LÖSCHUNG UND RÜCKGABE

Nach Abschluss der Veranstaltung übergeben wir alle Auftragsdaten vollständig in einem gängigen, maschinell lesbaren Format und löschen sie anschließend nachweisbar, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Das Löschprotokoll legen wir auf Anforderung vor.