Vertrag über die Auftragsverarbeitung (AVV) nach Art. 28 DSGVO

Fassung, Version 1.0, Stand 24.11.2026 · nolyx UG (haftungsbeschränkt), Hobökentwiete 30, 22559 Hamburg

> Fassung 1.0, Stand 24.11.2026. Anlage zu den AGB von Galavero (§ 10 AGB). Gilt mit Abschluss des Hauptvertrags ohne gesonderte Unterschrift. Galavero erzeugt bei der Bestätigung ein PDF dieses Vertrags mit den Angaben des Kunden. Es ist die verbindliche Fassung in elektronischem Format (Art. 28 Abs. 9 DSGVO). Auf Wunsch unterzeichnet nolyx zusätzlich eine Fassung handschriftlich oder mit elektronischer Signatur. Anlagen: 1 Gegenstand, Daten, Betroffene · 2 Technische und organisatorische Maßnahmen · 3 Unterauftragsverarbeiter.

zwischen

dem Kunden gemäß Hauptvertrag (Veranstalter)
– Verantwortlicher, nachfolgend „Kunde“ –

und

nolyx UG (haftungsbeschränkt), Hobökentwiete 30, 22559 Hamburg, HRB 200916 (AG Hamburg), vertreten durch den Geschäftsführer Hendrik Eilers
– Auftragsverarbeiter, nachfolgend „nolyx“ –

§ 1 Gegenstand, Dauer, Rollen

1. nolyx stellt dem Kunden die Software **Galavero** als Dienst über das Internet bereit (Software as a Service). Der Leistungsumfang ergibt sich aus dem Hauptvertrag (Angebot oder Auftrag, AGB, Leistungsbeschreibung). Dabei verarbeitet nolyx personenbezogene Daten im Auftrag des Kunden. Gegenstand, Art und Zweck, Datenarten und Betroffene beschreibt **Anlage 1**.
2. Der Kunde ist Verantwortlicher (Art. 4 Nr. 7 DSGVO). Er entscheidet allein, welche Personen er einlädt, welche Daten er erfasst, importiert und versendet, welche Inhalte er auf Eventseiten veröffentlicht und wie lange er Daten aufbewahrt. Er ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für Rechtsgrundlagen, Einwilligungen (auch nach § 7 UWG), die Information der Betroffenen (Art. 13, 14 DSGVO) und die Wahrung der Betroffenenrechte.
3. Dieser Vertrag gilt für die Laufzeit des Hauptvertrags und darüber hinaus, solange nolyx noch Daten des Kunden verarbeitet (§ 11).
4. **Keine Auftragsverarbeitung**, sondern eigene Verantwortung von nolyx sind:
   a) Vertrags-, Abrechnungs- und Kommunikationsdaten des Kunden und seiner Ansprechpartner;
   b) die Nutzerkonten als Zugang zur Plattform (Name, E-Mail-Adresse, Passwort als Hash, Zwei-Faktor-Anmeldung, Zugehörigkeit zum Kunden) und die Protokolle der Anmeldung und Kontosicherheit;

c) die Protokolle der Zugriffe von Plattformbetreuern (§ 4 Abs. 2), die nolyx zusätzlich als eigenen Nachweis führt;
d) die Missbrauchsabwehr im Plattformversand (§ 4 Abs. 4).
Rollen und Rechte im Team des Kunden sowie Änderungs- und Exportprotokolle im Kundenbereich verarbeitet nolyx dagegen im Auftrag des Kunden. Zu den eigenen Verarbeitungen informiert die Datenschutzerklärung von nolyx.

§ 2 Weisungen

1. nolyx verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Kunden, auch bei Übermittlungen in Drittländer, es sei denn, nolyx ist durch Unionsrecht oder deutsches Recht zur Verarbeitung verpflichtet (Art. 28 Abs. 3 lit. a DSGVO). In einem solchen Fall teilt nolyx dem Kunden die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.
2. Die Weisungen sind abschließend festgelegt durch diesen Vertrag, den Hauptvertrag und **die Nutzung der Funktionen von Galavero durch den Kunden** und seine berechtigten Nutzer (z. B. Kontaktimport, Versandfreigabe eines Mailings, Veröffentlichung einer Eventseite, Löschung). Einzelweisungen erteilt der Kunde in Textform (E-Mail an kontakt@nolyx.de). Mündliche Weisungen bestätigt er unverzüglich in Textform. Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, behandelt nolyx als Antrag auf Leistungsänderung.
3. Ist nolyx der Ansicht, dass eine Weisung gegen Datenschutzrecht verstößt, informiert nolyx den Kunden unverzüglich (Art. 28 Abs. 3 Satz 3 DSGVO). nolyx darf die Ausführung aussetzen, bis der Kunde die Weisung bestätigt oder ändert. Offensichtlich rechtswidrige Weisungen muss nolyx nicht ausführen.
4. Weisungsberechtigt sind die im Kundenkonto als „Kundenadmin“ eingetragenen Personen sowie die im Hauptvertrag benannten Ansprechpartner.

§ 3 Vertraulichkeit

nolyx setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und die mit den maßgeblichen Datenschutzbestimmungen vertraut gemacht wurden (Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO). Die Pflicht besteht nach Beendigung der Tätigkeit fort.

§ 4 Zugriff durch nolyx, Support, Plattformschutz

1. Beschäftigte von nolyx greifen auf Daten des Kunden nur zu, soweit dies für Betrieb, Wartung, Fehlerbehebung, Sicherheit oder einen Supportfall erforderlich ist.
2. Jeder Zugriff eines Plattformbetreuers in der Oberfläche des Kunden wird unveränderlich protokolliert (Person, Zeitpunkt, aufgerufene Seite ohne Parameter). Kundenadmins können

dieses Protokoll in Galavero unter „Einstellungen → Supportzugriffe“ einsehen. Zugriffe auf Datenbank- oder Serverebene erfolgen nur für Betrieb, Wiederherstellung und Fehlerbehebung.

3. Der Kunde weist nolyx an, aus den Daten **aggregierte Kennzahlen** zu bilden, die weder auf Personen noch auf den Kunden rückführbar sind (z. B. Anzahl versendeter Mails, Einlassdauer). nolyx darf diese Kennzahlen zu Statistik und Produktverbesserung nutzen. Eine weitergehende Nutzung für eigene Zwecke ist ausgeschlossen. Insbesondere nutzt nolyx Daten des Kunden nicht zum Training von KI-Modellen und verkauft sie nicht an Dritte. Bei der KI-Assistenz hat nolyx das Training mit den übermittelten Daten abgewählt und gibt keine Bewertungen (Feedback) an den Anbieter weiter. Einzelne Unterauftragsverarbeiter verarbeiten Daten in begrenztem Umfang zusätzlich als eigene Verantwortliche, etwa zur Erkennung von Missbrauch und Betrug oder für Nutzungsstatistiken; Anlage 3 nennt diese Fälle.
4. Nutzt der Kunde den **zentralen Plattformversand** von Galavero (gemeinsames Versandkonto), verarbeitet nolyx folgende Daten zusätzlich in eigener Verantwortung zur Sicherung der Zustellbarkeit und zur Missbrauchsabwehr (Art. 6 Abs. 1 lit. f DSGVO): E-Mail-Adressen, die eine Spam-Beschwerde ausgelöst haben oder dauerhaft unzustellbar sind (Hard Bounce), in Galavero nur als kryptografischer Hashwert, jeweils mit Zeitpunkt und Grund, höchstens 3 Jahre. Der Kunde kann diese Sperren nicht aufheben. Diese Sperrliste darf nolyx für alle Versendungen über das gemeinsame Versandkonto anwenden. Abmeldungen eines Gastes gelten demgegenüber nur für den Kunden, bei dem er sich abgemeldet hat. Nutzt der Kunde sein **eigenes Brevo-Konto**, besteht dieses Rechtsverhältnis direkt zwischen dem Kunden und Brevo. nolyx ist dann nur Auftragsverarbeiter für die Steuerung des Versands.

§ 5 Technische und organisatorische Maßnahmen

1. nolyx trifft die in **Anlage 2** beschriebenen Maßnahmen nach Art. 32 DSGVO und bleibt für deren Angemessenheit und Umsetzung verantwortlich. Der Kunde prüft vor Beginn der Verarbeitung, ob diese Maßnahmen für seine Verarbeitung ein dem Risiko angemessenes Schutzniveau bieten, auch für die freiwilligen Angaben zu Unterstützungsbedarf und Barrierefreiheit (Anlage 1 Nr. 3). Bedenken teilt er nolyx in Textform mit.
2. Die Maßnahmen unterliegen dem technischen Fortschritt. nolyx darf sie durch gleichwertige oder bessere ersetzen. Das Schutzniveau darf nicht sinken. Wesentliche Änderungen dokumentiert nolyx und teilt sie dem Kunden in Textform mit.

§ 6 Unterauftragsverarbeiter

1. Der Kunde erteilt nolyx die **allgemeine Genehmigung**, Unterauftragsverarbeiter einzusetzen (Art. 28 Abs. 2 Satz 1 DSGVO). Die in **Anlage 3** genannten gelten als genehmigt.
2. nolyx informiert den Kunden mindestens **30 Tage** vor der Hinzuziehung oder Ersetzung eines eigenen Unterauftragsverarbeiters in Textform (E-Mail an die Kundenadmins und Hinweis in

Galavero). Der Kunde kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Kommt keine Einigung zustande, kann der Kunde den Hauptvertrag zum Zeitpunkt des Wechsels kündigen. Bereits gezahlte Vergütung für nicht mehr erbrachte Leistungen erstattet nolyx anteilig.

3. Ändern die in Anlage 3 genannten Anbieter ihre eigenen Unterauftragsverarbeiter, gelten deren kürzere Fristen (Anlage 3). nolyx leitet solche Mitteilungen unverzüglich, spätestens 3 Werktage nach Eingang, an den Kunden weiter. Der Kunde kann dann innerhalb von 7 Tagen nach der Weiterleitung widersprechen; Abs. 2 Satz 3 und 4 gelten entsprechend.
4. In dringenden Fällen (Ausfall oder Sicherheitsvorfall bei einem Anbieter) kann nolyx einen Unterauftragsverarbeiter mit kürzerer Frist ersetzen. nolyx informiert den Kunden dann vor dem Einsatz, so früh wie möglich, und begründet die Verkürzung. Widerspruchs- und Kündigungsrecht des Kunden bleiben unberührt; die Widerspruchsfrist beträgt mindestens 7 Tage ab der Information.
5. nolyx erlegt jedem Unterauftragsverarbeiter durch Vertrag dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO), und prüft ihn vor Beauftragung auf solche Garantien. Wo die Standardverträge der Anbieter Fristen für Löschung, Meldungen oder Prüfungen anders ausgestalten, nennt Anlage 3 das offen. nolyx bleibt gegenüber dem Kunden für die Erfüllung der Pflichten seiner Unterauftragsverarbeiter verantwortlich (Art. 28 Abs. 4 Satz 2 DSGVO).
6. Optionale Dienste werden nur eingesetzt, wenn der Kunde sie einschaltet bzw. ihnen zustimmt (KI-Assistenz: Freischaltung durch nolyx und ausdrückliche Zustimmung des Kunden; Wallet-Tickets: je Anbieter durch den Kunden, bei Google Wallet zusätzlich mit Einwilligung des Gastes). Bis dahin fließen keine Daten an diese Anbieter.
7. Keine Unterauftragsverhältnisse sind Nebenleistungen wie Telekommunikation, Post, Zahlungsabwicklung für nolyx, Domainregistrierung und DNS-Abfragen, soweit dabei kein Zugriff auf Daten des Kunden besteht.

§ 7 Ort der Verarbeitung, Drittländer

1. Die Verarbeitung findet grundsätzlich in der Europäischen Union oder im EWR statt. Die Server von Galavero und ihre Sicherungen stehen in Deutschland.
2. Abweichend davon können einzelne Unterauftragsverarbeiter und deren weitere Auftragsverarbeiter Daten in Drittländern verarbeiten oder von dort darauf zugreifen. Anlage 3 nennt diese Fälle mit Land und Garantie nach Kapitel V DSGVO (Angemessenheitsbeschluss nach Art. 45, z. B. EU-US Data Privacy Framework, oder Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO). Mit Anlage 3 erteilt der Kunde die Weisung zu diesen Übermittlungen.
3. Jede weitere Verarbeitung in einem Drittland kündigt nolyx nach § 6 an. Sie ist nur zulässig, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Mit einem

Unterauftragsverarbeiter, dessen Konzern Sitz in einem Drittland hat, vereinbart nolyx die Verarbeitung in der EU, soweit der Anbieter dies anbietet.

§ 8 Unterstützung des Kunden

1. **Betroffenenrechte:** nolyx unterstützt den Kunden mit geeigneten Maßnahmen bei Anfragen nach Art. 15 bis 22 DSGVO. Galavero bietet dafür Funktionen zum Auffinden, Berichtigen, Exportieren, Sperren und Löschen von Kontakten und Teilnahmedaten. Wendet sich eine betroffene Person direkt an nolyx, verweist nolyx sie an den Kunden und leitet die Anfrage unverzüglich weiter. nolyx beantwortet solche Anfragen nicht selbst.
2. **Art. 32 bis 36 DSGVO:** nolyx unterstützt den Kunden bei Sicherheit, Meldungen von Datenschutzverletzungen, Datenschutz-Folgenabschätzung und vorheriger Konsultation, soweit dies nach Art der Verarbeitung und den nolyx verfügbaren Informationen möglich ist.
3. **Vergütung:** Unterstützung, die in Galavero als Funktion bereitsteht oder auf einem Verstoß von nolyx beruht, ist kostenfrei. Darüber hinausgehende Unterstützung vergütet der Kunde nach Aufwand zum jeweils vereinbarten Stundensatz. nolyx kündigt den voraussichtlichen Aufwand vorher an.

§ 9 Meldung von Datenschutzverletzungen

1. nolyx meldet dem Kunden eine Verletzung des Schutzes personenbezogener Daten des Kunden **unverzüglich, spätestens innerhalb von 24 Stunden**, nachdem nolyx selbst oder durch Mitteilung eines Unterauftragsverarbeiters davon Kenntnis erlangt hat, per E-Mail an die Kundenadmins und telefonisch an den Ansprechpartner. nolyx verpflichtet seine Unterauftragsverarbeiter, Verletzungen unverzüglich mitzuteilen.
2. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO: Art der Verletzung, Kategorien und ungefähre Zahl der Betroffenen und Datensätze, Ansprechpartner, wahrscheinliche Folgen sowie ergriffene und vorgeschlagene Maßnahmen. nolyx meldet zunächst die verfügbaren Informationen und wartet keine abgeschlossene Ursachenanalyse ab. Fehlende Angaben reicht nolyx unverzüglich nach.
3. Meldungen an die Aufsichtsbehörde und die Benachrichtigung der Betroffenen (Art. 33, 34 DSGVO) nimmt der Kunde vor. Eine Meldung von nolyx ist kein Anerkenntnis eines Verschuldens.

§ 10 Kontrollen und Nachweise

1. nolyx stellt dem Kunden auf Anforderung alle Informationen zum Nachweis der Pflichten aus Art. 28 DSGVO bereit (Art. 28 Abs. 3 lit. h DSGVO). Der Nachweis kann auch durch aktuelle Selbstauskünfte, Zertifikate oder Prüfberichte erfolgen, auch solche der Unterauftragsverarbeiter (z. B. ISO/IEC 27001 und BSI C5 von Hetzner).

2. Der Kunde oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer kann Inspektionen durchführen. Vor-Ort-Prüfungen sind mindestens **30 Tage** vorher anzukündigen, finden während der Geschäftszeiten ohne Störung des Betriebs statt und sind auf **einmal pro Kalenderjahr** beschränkt. Diese Beschränkungen gelten nicht bei begründeten Anhaltspunkten für einen Datenschutzverstoß, zur Aufklärung einer Datenschutzverletzung oder wenn eine Aufsichtsbehörde die Prüfung verlangt; dann ist eine Prüfung mit angemessener kürzerer Ankündigung möglich. Prüfer, die im Wettbewerb zu nolyx stehen, kann nolyx ablehnen.
3. Die Kosten einer Prüfung trägt jede Partei selbst. Ergibt die Prüfung einen erheblichen Verstoß von nolyx, trägt nolyx die Kosten der Prüfung.
4. nolyx informiert den Kunden unverzüglich über Kontrollen und Maßnahmen einer Aufsichtsbehörde, soweit sie diesen Auftrag betreffen.
5. Prüfungen bei Unterauftragsverarbeitern erfolgen vorrangig durch Vorlage ihrer aktuellen Zertifikate, Testate und Prüfberichte. Darüber hinausgehende Prüfungen richten sich nach den Prüfrechten, die diese nolyx eingeräumt haben (Anlage 3); nolyx übt diese Rechte auf Verlangen des Kunden aus. Kosten, die ein Unterauftragsverarbeiter dafür berechnet, trägt der Kunde, außer die Prüfung ergibt einen erheblichen Verstoß.

§ 11 Löschung und Rückgabe

1. Während der Laufzeit löscht der Kunde Daten selbst über die Funktionen von Galavero oder erteilt dazu eine Weisung. nolyx löscht Daten nicht eigenmächtig. Ausnahmen sind die vom Kunden in Galavero eingestellten oder in **Anlage 1 Nr. 5** genannten Standard-Löschfristen.
2. Nach Ende der Verarbeitungsleistungen gibt nolyx die Daten nach Wahl des Kunden zurück oder löscht sie (Art. 28 Abs. 3 lit. g DSGVO). Ohne abweichende Weisung stellt nolyx dem Kunden seine Daten nach Ende des Hauptvertrags **mindestens 30 Tage** in maschinenlesbarer Form zum Abruf bereit (Export). Danach löscht nolyx alle Daten des Kunden innerhalb von weiteren **30 Tagen** und bestätigt die Löschung auf Anforderung in Textform. Auf Weisung des Kunden löscht nolyx die Daten schon vor Ablauf der Abruffrist; der Kunde verzichtet damit auf den weiteren Abruf.
3. Daten in Sicherungskopien von nolyx werden mit dem regulären Ablauf der Sicherungen gelöscht, spätestens **35 Tage** nach der Löschung im Produktivsystem. Bis dahin sind sie gegen Nutzung gesperrt.
4. Daten, die Unterauftragsverarbeiter im Rahmen dieses Auftrags gespeichert haben, veranlasst nolyx bei Vertragsende zur Löschung. Diese löschen sie nach den in Anlage 3 genannten Fristen ihrer Verträge mit nolyx (z. B. Brevo bis zu 100 Tage nach Aufforderung). nolyx bestätigt die Veranlassung auf Anforderung.
5. Gesetzliche Aufbewahrungspflichten von nolyx bleiben unberührt. Dokumentationen, die der ordnungsgemäßen Auftragsverarbeitung dienen (z. B. Protokolle über Weisungen, Unterauftragsverarbeiter, Supportzugriffe), bewahrt nolyx bis zum Ende der Verjährungsfristen

auf.

§ 12 Haftung

Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Hauptvertrags (§ 13 AGB), soweit nicht zwingendes Recht entgegensteht. Der Kunde stellt nolyx von berechtigten Ansprüchen Dritter und angemessenen Kosten der Rechtsverteidigung frei, soweit sie auf einer rechtswidrigen Weisung oder einer fehlenden Rechtsgrundlage beruhen, die der Kunde zu vertreten hat. Eine Mitverursachung durch nolyx wird nach den Verantwortungsanteilen berücksichtigt (Art. 82 Abs. 5 DSGVO). Für Bußgelder gilt § 14 AGB.

§ 13 Schlussbestimmungen

1. In Fragen der Auftragsverarbeitung geht dieser Vertrag den übrigen vorformulierten Vertragsbestandteilen vor, auch der Leistungsbeschreibung und den AGB. Individuelle Vereinbarungen gehen im gesetzlich zulässigen Umfang vor. Zwingendes Recht bleibt unberührt.
2. Gefährden Pfändung, Beschlagnahme, Insolvenz oder sonstige Maßnahmen Dritter die Daten des Kunden bei nolyx, informiert nolyx den Kunden unverzüglich und weist die Dritten darauf hin, dass die Verfügungsbefugnis über die Daten beim Kunden liegt.
3. Änderungen dieses Vertrags bedürfen der Textform. Für die Änderung von Anlage 2 gilt § 5 Abs. 2, für Anlage 3 gilt § 6.
4. Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam.
5. Es gilt deutsches Recht. Gerichtsstand ist Hamburg, soweit der Kunde Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

Anlage 1 – Gegenstand, Art und Zweck, Daten, Betroffene, Fristen

1. Art und Zweck der Verarbeitung

Bereitstellung und Betrieb von Galavero für die Einladungs-, Gäste- und Einlassorganisation von Veranstaltungen des Kunden, insbesondere:

- Verwaltung eines Adressbestands (Kontakte) einschließlich Import aus Dateien, Dublettenprüfung mit Zusammenführen, Zuordnung von Mentoren und Export;
- Planung von Veranstaltungen, Gästelisten, Kontingenten, Begleitpersonen und Freicodes;
- Versand von Einladungen, Erinnerungen, Vortagsinformationen, Zu- und Absagebestätigungen, Tickets und Kalenderdateien per E-Mail im Namen des Kunden; Verarbeitung von Zustellmeldungen, Rückläufern und Abmeldungen;
- Erzeugen von Briefdaten und persönlichen Codes für den Postversand durch den Kunden;

- Bereitstellen von Gastportal und Eventseiten (Rückmeldung, Begleitungen benennen, Menüwahl, Unterstützungsbedarf angeben, Tickets abrufen), deren Inhalte der Kunde gestaltet;
- Tickets als PDF und als Pass für Apple Wallet bzw. Google Wallet, jeweils nur wenn der Kunde den betreffenden Anbieter einschaltet (Anlage 3);
- Sitzplatz- und Saalplanung, auf Wunsch mit KI-Unterstützung (Anlage 3, optional);
- Einlass am Veranstaltungstag (Scannen, Platzvergabe, Druck von Platzkarten, Servicefälle, Ankunftsbenachrichtigung an Gastgeber des Kunden), ggf. über lokal betriebene Geräte;
- Auswertungen und Abschlussberichte (ohne Namen);
- Betrieb, Sicherung, Wiederherstellung, Fehleranalyse und Support, einschließlich Supportanfragen per E-Mail.

2. Kategorien betroffener Personen

- Kontakte, Gäste und Begleitpersonen des Kunden (eingeladene Personen, Interessenten, Geschäftspartner, Presse, Preisträger u. a.), auch Personen, die sich mit einem Freicode selbst eintragen;
- Gastgeber, Mentoren und Ansprechpartner auf Seiten des Kunden;
- Nutzer von Galavero beim Kunden (Beschäftigte, Agenturen, Einlasspersonal), soweit nicht § 1 Abs. 4;
- Empfänger von Testmails.

3. Arten personenbezogener Daten

- **Stammdaten:** Anrede, Titel, Vor- und Nachname, Sprache, Organisation, Position, Kategorie, Tags, Priorität, zugeordnete Mentoren, Herkunft des Datensatzes (z. B. Import, Freicode);
- **Interne Notiz des Teams** am Kontakt (Freitext bis 5.000 Zeichen): nur für Nutzer mit Kontaktrecht sichtbar, nie in Mails, im Gastportal oder in Exporten an Dritte, wird mit dem Kontakt gelöscht oder beim Anonymisieren geleert. Sie ist nicht für Gesundheitsdaten oder andere besondere Kategorien bestimmt;
- **Kontaktdaten:** E-Mail, Telefon, Mobilnummer, Postanschrift, Website;
- **Dublettenprüfung:** Bewertungen möglicher Dubletten (nur Kennungen und Gründe), Markierung „verschiedene Personen“, Protokoll von Zusammenführungen mit verschlüsselter Momentaufnahme beider Kontakte für das Rückgängigmachen (14 Tage);
- **Einladungs- und Teilnahmedaten:** Eventzuordnung, Kontingent (+N), Rückmeldung mit Zeitpunkt und Weg, benannte Begleitpersonen, Menüwahl, Freicodes und ihre Einlösung, Änderungswünsche (Freitext), Gastgeber, betreuender Mentor, Warteliste;
- **Sitzplatz-, Ticket- und Einlassdaten:** Sitzplatz, Ticket-Kennung (QR-Code mit Zufallswert, ohne Namen), Daten für Ticket-PDF und Wallet-Pass (Eventname, Datum, Ort, Name, Platz, Ticketcode), Einlasszeitpunkt, Scanstation, Servicefälle mit Notizen;

- **Kommunikations- und Protokolldaten:** Versand- und Zustellstatus, Rückläufer, Abmeldungen, Sperren; technische Zugriffsdaten (IP-Adresse, Browserkennung, Zeitpunkt) in Sitzungen und Serverprotokollen; Änderungsprotokolle; kurzlebige Bearbeitungssperren (wer einen Datensatz gerade bearbeitet; beim Aufheben einer Sperre ein Protokolleintrag nur mit Kennungen, ohne Namen oder Inhalte);
- **Freiwillige Angaben zu Unterstützungsbedarf und Barrierefreiheit** (z. B. Rollstuhlplatz, stufenloser Zugang, Freitext zum Unterstützungsbedarf) mit Zeitpunkt der Einwilligung und eines Widerrufs. Diese Angaben können **Gesundheitsdaten im Sinne von Art. 9 DSGVO** sein. Der Kunde stellt sicher, dass dafür eine Rechtsgrundlage besteht (in der Regel ausdrückliche Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO), und erfasst Ernährungs-, Religions- oder Gesundheitsangaben nur, soweit sie für die Veranstaltung erforderlich sind, und nur in den dafür vorgesehenen Feldern;
- **Inhalte**, die der Kunde in Eventseiten, Gestaltungen und Mailvorlagen einstellt (Texte, Bilder);
- **E-Mails an nolyx**, z. B. Supportanfragen, Weisungen und weitergeleitete Anfragen von Gästen, soweit sie Daten nach dieser Anlage enthalten.

4. Ort der Verarbeitung

Rechenzentren der Hetzner Online GmbH in Deutschland: Server in Nürnberg, Sicherungen im Objektspeicher in Falkenstein (getrennter Standort). Ausnahmen mit Drittlandbezug nennt Anlage 3 (§ 7). Am Veranstaltungstag zusätzlich auf lokalen Geräten (Einlass-Server, Scanner, Drucker), die nolyx oder der Kunde vor Ort betreibt; nach der Veranstaltung werden die Daten auf den lokalen Geräten gelöscht (Anlage 2 Nr. 10).

5. Standard-Löschfristen (soweit der Kunde nichts anderes einstellt)

Daten	**Frist**
Angaben zu Unterstützungsbedarf, Barrierefreiheit und Servicefall-Notizen	30 Tage nach Ende der Veranstaltung; der Kunde kann die Frist mit Begründung auf 1 bis 180 Tage ändern
Ticketinhalte (Daten, aus denen Ticket-PDFs erzeugt werden; PDF-Dateien werden nicht gespeichert) und Druckaufträge	30 Tage nach Ende der Veranstaltung
Daten auf lokalen Einlassgeräten	unmittelbar nach Rücksynchronisation, spätestens 7 Tage nach der Veranstaltung
Sitzungsdaten (IP-Adresse, Browserkennung)	25 Stunden nach letzter Aktivität
Bearbeitungssperren	mit dem Verlassen der Seite, spätestens nach 30 Minuten Inaktivität
Momentaufnahme bei Zusammenführung von Kontakten	14 Tage; das Protokoll ohne Inhalte bleibt bis zur Löschung der Kontakte
Serverprotokolle (Webserver)	14 Tage
Zustell- und Versandprotokolle, einschließlich Zustellmeldungen des Versanddienstes	13 Monate nach Versand bzw. Eingang

Daten	Frist
Abmeldungen (je Kunde)	bis zur Löschung durch den Kunden bzw. Vertragsende (Nachweis)
Plattformsperren (Spam-Beschwerde, Hard Bounce; eigene Verantwortung von nolyx, § 4 Abs. 4)	höchstens 3 Jahre; nicht durch den Kunden aufhebbar
Kontakte mit interner Notiz, Einladungen, Teilnahme- und Einlassdaten	bis zur Löschung durch den Kunden, spätestens nach § 11 Abs. 2
Sicherungskopien von nolyx	rollierend, höchstens 35 Tage
Daten bei Unterauftragsverarbeitern	nach Anlage 3

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Stand 23.11.2026. Die Maßnahmen der Rechenzentren beschreibt die Hetzner Online GmbH in ihrer TOM-Dokumentation (https://www.hetzner.com/de/AV/TOM.pdf). Hetzner verfügt für den dort ausgewiesenen Geltungsbereich über ein nach ISO/IEC 27001 zertifiziertes Informationssicherheitsmanagement und einen Prüfbericht nach BSI C5 (Typ 2). Maßgeblich sind Geltungsbereich und Prüfzeitraum der jeweils aktuellen Nachweise. Eine Zertifizierung der Anwendung Galavero selbst folgt daraus nicht.

1. Zutrittskontrolle

- Die zentralen Server stehen ausschließlich in zertifizierten Rechenzentren der Hetzner Online GmbH (elektronische Zutrittskontrolle, Videoüberwachung, Wachpersonal, siehe Hetzner-TOM). Für gebuchte Einlassleistungen kommen lokale Einlassgeräte nach Nr. 10 hinzu.
- nolyx betreibt keine eigenen Serverräume. Arbeitsplätze in verschlossenen Räumen; mobile Geräte mit Festplattenverschlüsselung und Bildschirmsperre.
- Einlassgeräte vor Ort werden außerhalb des Einsatzes verschlossen aufbewahrt und während der Veranstaltung durch Personal beaufsichtigt.

2. Zugangskontrolle

- Persönliche Konten, kein geteilter Zugang. Passwörter nur als Hash (bcrypt/argon2) gespeichert.
- Zwei-Faktor-Anmeldung (TOTP) für alle Plattformbetreuer verpflichtend; für Kundenteams einstellbar verpflichtend.
- Begrenzung von Anmelde- und Codeversuchen (Rate Limiting); Sitzungsablauf nach Inaktivität.
- Serverzugang nur per SSH-Schlüssel, Passwort-Login deaktiviert; Firewall (Hetzner Cloud Firewall und Host-Firewall), Fail2ban; Datenbank nicht aus dem Internet erreichbar.
- Zwei-Faktor-Anmeldung für alle Dienstleisterkonten (Hetzner, Ploi, Brevo, Mistral, Domain, Code-Repository).

- Einlassgeräte werden einzeln gekoppelt; Gerätesitzungen zeitlich begrenzt (1–24 Stunden) und widerrufbar.

3. Zugriffskontrolle

- Rollen- und Rechtekonzept serverseitig (Kundenadmin, Redaktion, Einlass, Service, Gerät); Prüfung jeder Aktion durch Richtlinien (Policies).
- Strikte Mandantentrennung: jeder Datensatz gehört zu genau einem Kunden; fehlender Mandantenkontext verweigert den Zugriff; Prüfung auf Anwendungs- und Datenbankebene.
- Plattformbetreuer erhalten Zugriff nur für Betrieb und Support; jeder Zugriff in Kundenbereichen wird unveränderlich protokolliert und ist für den Kunden einsehbar.
- Exporte von Kontakten nur mit gesondertem Recht; jeder Export wird protokolliert; Kontaktexporte werden nach dem Herunterladen gelöscht, Vollexporte des Kunden spätestens 7 Tage nach Bereitstellung.
- Gastportal: Zugang nur mit persönlichem Code (per HMAC geschützt gespeichert) oder freigegebenem Event-Code; Codes nie in URLs; Gastseiten nicht für Suchmaschinen freigegeben.

4. Trennungskontrolle

- Logische Mandantentrennung (siehe Nr. 3); getrennte Gast-Domain ohne Zugriff auf die Verwaltung und ohne gemeinsame Sitzungs-Cookies.
- Getrennte Test-, Entwicklungs- und Produktivumgebungen; Entwicklung und Tests ausschließlich mit synthetischen Daten.

5. Pseudonymisierung und Verschlüsselung

- Transportverschlüsselung TLS (HTTPS mit HSTS) für alle Verbindungen; Mailversand an den Versanddienst über TLS.
- Verschlüsselung auf Feldebene (AES-256) für besonders schutzwürdige Daten, u. a. Unterstützungsangaben, Notizen, Ticketdaten, Importdateien, Empfängeradressen in Versandprotokollen und Sitzungsdaten.
- Datenbanksicherungen werden vor der Übertragung in den Objektspeicher verschlüsselt; Schlüssel getrennt von den Sicherungen verwahrt. Die Serversicherungen von Hetzner (Abbilder des Servers, höchstens 7 Tage) liegen im Rechenzentrumsverbund von Hetzner; besonders schutzwürdige Felder sind darin bereits auf Feldebene verschlüsselt.
- KI-Funktionen erhalten keine Namen oder Kontaktdaten der Gäste: Sitzplatzvorschläge arbeiten mit Pseudonymen; Regeln im Chat werden lokal auf Platzhalter abgebildet. Interne Notizen und Unterstützungsangaben werden nicht an die KI übermittelt.
- Ticket-QR-Codes enthalten nur einen Zufallswert, keine Namen.

6. Weitergabekontrolle

- Keine Weitergabe an Dritte außer den Unterauftragsverarbeitern nach Anlage 3 und an Google Wallet, nur wenn der Kunde Google Wallet einschaltet und der Gast die Ablage wählt (Anlage 3).
- Sicherheits-Header und Content-Security-Policy; Gastseiten laden keine Inhalte von Drittanbietern (keine externen Schriften, Karten, Tracker, Analysedienste).
- Galavero wertet Öffnungen und Klicks von E-Mails nicht aus. Der Versanddienstleister Brevo zählt sie technisch bedingt nur anonymisiert in Summen, ohne Zuordnung zu Empfängern; Links in E-Mails leitet Brevo dafür über eine eigene Weiterleitung.
- Ausgehende Verbindungen der Anwendung nur zu festgelegten Anbietern (Allowlist).

7. Eingabekontrolle

- Änderungsprotokolle für Teilnahmen, Einladungen, Team und Betreiberaktionen; Protokolltabellen sind gegen nachträgliche Änderung gesperrt. Einzige Ausnahme ist die Bereinigung nach Löschfristen: Sie leert nur Inhaltsspalten und wird in derselben Transaktion selbst protokolliert.
- Versand eines Mailings nur nach ausdrücklicher Freigabe; Protokoll der Freigabe.

8. Verfügbarkeitskontrolle und Belastbarkeit

- Tägliche, verschlüsselte Datenbanksicherung an einen getrennten Standort (Hetzner Object Storage), zusätzlich Serversicherungen; Aufbewahrung rollierend bis 35 Tage.
- Wiederherstellungstests mit synthetischen Daten; Umfang, Turnus und Ergebnis werden dokumentiert.
- Überwachung von Erreichbarkeit und Hintergrunddiensten.
- Am Veranstaltungstag, soweit der Einlass mit Geräten von nolyx gebucht ist: lokaler Einlass-Server mit Ersatzgerät und unterbrechungsfreier Stromversorgung, ausgelegt dafür, dass der Einlass auch bei Ausfall der Internetverbindung weiterläuft.
- Zeitnahes Einspielen von Sicherheitsupdates; automatisierte Prüfung der Abhängigkeiten auf bekannte Schwachstellen.

9. Auftragskontrolle

- Unterauftragsverarbeiter nur mit Vertrag nach Art. 28 DSGVO; Auswahl nach Sicherheitsnachweisen (Zertifikate, TOM); Verarbeitung grundsätzlich in der EU, Ausnahmen nach § 7 und Anlage 3.
- Weisungen und Supportfälle werden dokumentiert.

10. Lokale Einlassgeräte

- Daten auf lokalen Geräten nur für die jeweilige Veranstaltung; Datenträger verschlüsselt.
- Nach Rücksynchronisation Löschung der Veranstaltungsdaten auf den Geräten, spätestens 7 Tage nach der Veranstaltung; Druckaufträge werden nicht dauerhaft gespeichert.

11. Datenschutzmanagement und Überprüfung

- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (z. B. kein Tracking, kurze Löschfristen, Namen nicht in Berichten).
- Sicherheitsprüfung bei jeder Funktionserweiterung und vor jeder Freigabe; Überprüfung dieser TOM mindestens jährlich.
- Prozess für Sicherheitsvorfälle mit Meldung an Kunden binnen 24 Stunden (§ 9).
- Ein Datenschutzbeauftragter ist derzeit nicht benannt. nolyx prüft die Pflicht zur Benennung (Art. 37 DSGVO, § 38 BDSG) bei jeder wesentlichen Änderung der Verarbeitung, mindestens jährlich. Ansprechpartner Datenschutz: Hendrik Eilers, kontakt@nolyx.de.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

Anbieter	**Leistung**	**Ort der Verarbeitung**	**Betroffene Daten**	**Einsatz**
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland	Server-Hosting (Rechenzentrum), Objektspeicher für Sicherungen, DNS	Deutschland (Nürnberg/Falkenstein; Sicherungen in Falkenstein)	alle Daten nach Anlage 1	immer
Ploi B.V., Amperestraat 16J, 3861 NC Nijkerk, Niederlande, KvK 94117233, USt-IdNr. NL866641658B01	Serververwaltung und Bereitstellung (administrativer Zugriff auf den Server, Zertifikate)	Niederlande/EU; Daten verbleiben auf den Hetzner-Servern	Zugriff auf alle Daten technisch möglich, keine eigene Speicherung von Kundendaten	immer

Anbieter	**Leistung**	**Ort der Verarbeitung**	**Betroffene Daten**	**Einsatz**
Sendinblue GmbH (Brevo), Köpenicker Str. 126, 10179 Berlin, Deutschland	Versand von E-Mails, Zustell- und Abmeldemeldungen	Speicherung in der EU (Frankreich, Deutschland; Sicherungen Belgien). Weitere Auftragsverarbeiter von Brevo verarbeiten Daten auch in Drittländern oder greifen von dort zu: USA (u. a. Cloudflare, Datadog, Sendinblue Inc.; EU-US Data Privacy Framework bzw. Standardvertragsklauseln), Indien (Silver Line IT Solutions; Standardvertragsklauseln), Kanada (Sendinblue Canada; Angemessenheitsbeschluss)	E-Mail-Adresse, Name, Mailinhalt, Versand- und Zustelldaten	bei Nutzung des zentralen Plattformversands; bei eigenem Brevo-Konto des Kunden ist Brevo dessen eigener Auftragsverarbeiter
Mistral AI SAS, 15 rue des Halles, 75001 Paris, Frankreich, RCS Paris 952 418 325	KI-Assistenz (Sitzplatzvorschläge, Gestaltungs- und Übersetzungshilfe)	EU-Endpunkt (`api.eu.mistral.ai`); Training abgewählt; Mistral speichert Ein- und Ausgaben zeitlich begrenzt zur Missbrauchserkennung als eigener Verantwortlicher (Zero Data Retention nicht vereinbart); Übermittlung in Drittländer nur mit Angemessenheitsbeschluss oder Standardvertragsklauseln	keine Namen oder Kontaktdaten von Gästen; pseudonyme Sitzplatzdaten, Event- und Gestaltungstexte, Eingaben der Nutzer	**nur** wenn nolyx die KI für den Kunden freigeschaltet und der Kunde in Galavero ausdrücklich zugestimmt hat
TrafficPlex GmbH (lima-city), Konsul-Smidt-Str. 90, 28217 Bremen, Deutschland	E-Mail-Postfächer von nolyx (Support, Weisungen, Anfragen von Kunden und Gästen)	Deutschland (Rechenzentrum in Frankfurt am Main)	Inhalte von E-Mails an nolyx, z. B. Supportanfragen mit Event- oder Gästedaten und weitergeleitete Anfragen Betroffener	immer

Abweichende Bedingungen in den Verträgen der Unterauftragsverarbeiter mit nolyx (§ 6 Abs. 3 und 5, § 10 Abs. 5, § 11 Abs. 4):

- **Löschung nach Vertragsende oder Aufforderung:** Brevo innerhalb von 100 Tagen; Ploi innerhalb von 30 Tagen, aus Sicherungen innerhalb von 90 Tagen; Mistral: Zugriff endet 30 Tage nach Ende der Leistung; Hetzner und lima-city auf Weisung von nolyx.
- **Eigene Zwecke:** Brevo verarbeitet Daten auch als eigener Verantwortlicher, u. a. für Statistiken und zur Verteidigung von Rechtsansprüchen. Mistral verarbeitet Ein- und Ausgaben als eigener Verantwortlicher zur Missbrauchserkennung, weil Zero Data Retention nicht vereinbart ist.

- **Neue Unterauftragsverarbeiter der Anbieter:** Hetzner mit Widerspruchsfrist von 14 Tagen (in Ausnahmefällen kürzer), Brevo mit zwei Wochen, Mistral mit zehn Tagen, Ploi mit 30 Tagen; lima-city veröffentlicht eine Liste.
- **Prüfungen:** vorrangig über Zertifikate und Berichte; Brevo: Dokumentenprüfung einmal jährlich, Vor-Ort-Prüfung nur nach Einigung, Mehraufwand kostenpflichtig; Hetzner: angemeldet, grundsätzlich einmal jährlich; Ploi: Vor-Ort-Prüfung nachrangig mit 30 Tagen Vorlauf; Mistral: Vor-Ort-Prüfung einmal jährlich mit 90 Tagen Vorlauf.
- **Meldung von Verletzungen:** Hetzner, Brevo und lima-city unverzüglich; Ploi unverzüglich, spätestens 72 Stunden nach Bestätigung der Verletzung. Die 24-Stunden-Frist nach § 9 läuft ab Kenntnis von nolyx.

Wallet-Tickets (keine Unterauftragsverarbeiter). Der Kunde schaltet Apple Wallet und Google Wallet in Galavero getrennt ein; ab Werk sind beide aus. Jeder Anbieter wird nur eingesetzt, wenn der Kunde ihn einschaltet.

- **Google Wallet** (nur wenn der Kunde Google Wallet einschaltet): Wählt der Gast „Zu Google Wallet“, legt Galavero das Ticket (Eventname, Datum, Ort, Name, Platz, Ticketcode) über die Google Wallet API bei Google an. Google verarbeitet diese Daten als eigener Verantwortlicher nach den Google APIs Terms of Service und den Google Controller-Controller Data Protection Terms. Für personenbezogene Daten aus Europa ist danach Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland, verantwortlich. Übermittlungen in die USA stützt Google auf das EU-US Data Privacy Framework bzw. Standardvertragsklauseln. Bei Widerruf, Löschung oder Ablauf der Löschfrist überschreibt Galavero Name, Platz und Ticketcode des Google-Objekts und setzt es auf inaktiv.
- **Apple Wallet** (nur wenn der Kunde Apple Wallet einschaltet): Galavero erzeugt und signiert die Ticketdatei selbst und liefert sie direkt an das Gerät des Gastes. nolyx übermittelt dabei keine Daten an Apple; Galavero nutzt keinen Aktualisierungsdienst von Apple. Was Apple auf dem Gerät des Gastes verarbeitet, richtet sich nach dem Verhältnis zwischen Gast und Apple.

Änderungen dieser Liste kündigt nolyx nach § 6 Abs. 2 an. Sie erfordern keine erneute Bestätigung dieses Vertrags. Für jeden Stand der Liste erzeugt Galavero eine neue Fassung von Anlage 3 mit Datum der Ankündigung. Die aktuelle Liste ist in Galavero und unter `/rechtliches/unterauftragsverarbeiter` abrufbar.