Auftragsverarbeitungsvertrag (Anlage 2 zu den AGB für OpenEOS)

Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 Abs. 3 DSGVO

Stand: 18. November 2026

zwischen

dem Kunden im Sinne von Ziffer 2 der Allgemeinen Geschäftsbedingungen für OpenEOS (nachfolgend „Verantwortlicher“ oder „Kunde“)

und

LUXCODE by Lukas Lukic-Spitznagel, Brunnenstraße 6, 78112 St. Georgen im Schwarzwald, E-Mail: hello@openeos.de (nachfolgend „Auftragsverarbeiter“ oder „LUXCODE“)

gemeinsam „die Parteien“.

---

1. Gegenstand, Zustandekommen und Rangfolge

1.1 LUXCODE stellt dem Kunden die Software OpenEOS als Software-as-a-Service auf Grundlage der Allgemeinen Geschäftsbedingungen für OpenEOS (nachfolgend „AGB“) bereit. Dabei verarbeitet LUXCODE personenbezogene Daten, für die der Kunde Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO ist. Diese Vereinbarung regelt die Rechte und Pflichten der Parteien bei dieser Verarbeitung im Auftrag nach Art. 28 DSGVO.

1.2 Diese Vereinbarung kommt durch ihre Annahme bei der Registrierung des Kundenkontos im Kundenportal zustande. Die Annahme erfolgt in Textform durch Bestätigung im Registrierungsvorgang; eine Unterschrift ist nicht erforderlich. LUXCODE stellt dem Kunden die angenommene Fassung im Kundenportal dauerhaft abrufbar zur Verfügung.

1.3 Gegenstand, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich aus Anhang A. Die zugelassenen Unterauftragsverarbeiter ergeben sich aus Anhang B, die technischen und organisatorischen Maßnahmen aus Anhang C. Die Anhänge sind Bestandteil dieser Vereinbarung.

1.4 Die Verarbeitung findet in Mitgliedstaaten der Europäischen Union oder in Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum statt. Ausgenommen sind die in Anhang B mit einem Sitz oder Verarbeitungsort außerhalb der EU bzw. des EWR ausgewiesenen Unterauftragsverarbeiter (einschließlich solcher mit Sitz in einem Drittland, für das ein Angemessenheitsbeschluss der Europäischen Kommission besteht, wie der Schweiz); für sie müssen die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sein. Eine weitere Verarbeitung in einem Drittland ist nur zulässig, wenn der Kunde vorher in Textform zugestimmt hat und die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind. Für neue Unterauftragsverarbeiter außerhalb von EU/EWR gilt allein das Verfahren nach Ziffer 6.3; Satz 3 bleibt für sonstige Drittlandverarbeitungen unberührt.

1.5 Diese Vereinbarung ergänzt die AGB. Für Fragen des Datenschutzes geht sie den AGB nach deren Ziffer 1.5 vor. Im Übrigen gelten die AGB, insbesondere Ziffer 10 (Kundendaten) und Ziffer 11 (Haftung).

2. Laufzeit

2.1 Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Nutzungsvertrags über das Kundenkonto nach Ziffer 3.2 der AGB. Sie endet vorbehaltlich Ziffer 2.2 mit dessen Beendigung, ohne dass es einer gesonderten Kündigung bedarf.

2.2 Dieser Vertrag gilt über das Ende des Nutzungsvertrags hinaus fort, solange LUXCODE Daten des Kunden verarbeitet, insbesondere für die Dauer der Archivierung nach Ziffer 10.3 der AGB.

2.3 Die Pflichten aus Ziffer 10 (Löschung und Rückgabe) und Ziffer 4 (Vertraulichkeit) gelten über das Ende der Vereinbarung hinaus, bis sie erfüllt sind.

3. Weisungen des Kunden

3.1 LUXCODE verarbeitet die personenbezogenen Daten ausschließlich im Rahmen dieser Vereinbarung und auf dokumentierte Weisung des Kunden, es sei denn, LUXCODE ist durch Unionsrecht oder das Recht eines Mitgliedstaats zur Verarbeitung verpflichtet; in diesem Fall teilt LUXCODE dem Kunden diese Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet. Die Nutzung der Software durch den Kunden, insbesondere das Anlegen, Ändern und Löschen von Daten und das Setzen von Einstellungen im Kundenportal, gilt als Weisung. Die AGB, diese Vereinbarung und die Leistungsbeschreibung (Anlage 1 der AGB) bilden die Erstweisung.

3.2 Weitergehende oder abweichende Weisungen erteilt der Kunde in Textform über das Kundenportal oder per E-Mail an hello@openeos.de. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Weisungsberechtigt sind die Mitglieder der Organisation des Kunden mit der Rolle „Administrator“.

3.3 Verursacht eine Weisung Aufwand, der über den vereinbarten Leistungsumfang hinausgeht, oder ist sie mit der Software nicht umsetzbar, teilt LUXCODE dies dem Kunden mit. Die Parteien einigen sich dann über die Umsetzung und eine angemessene Vergütung; LUXCODE darf die Ausführung bis zur Einigung zurückstellen, soweit keine gesetzliche Pflicht entgegensteht. Dies gilt nicht für Weisungen, die zur Erfüllung von Pflichten des Kunden nach Art. 12 bis 22 DSGVO (einschließlich der Löschpflichten nach Art. 17 DSGVO) erforderlich sind; diese setzt LUXCODE unverzüglich um, die Vergütung wird nachträglich geklärt.

3.4 Ist LUXCODE der Auffassung, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt, informiert LUXCODE den Kunden unverzüglich. LUXCODE darf die Ausführung der Weisung bis zur Bestätigung oder Änderung durch den Kunden aussetzen.

3.5 LUXCODE verarbeitet die Daten nicht für eigene Zwecke. Der Kunde weist LUXCODE an, aus den Kundendaten aggregierte, anonyme Nutzungs- und Leistungskennzahlen (z. B. Anzahl Vorgänge, Antwortzeiten) zu erzeugen; LUXCODE verwendet ausschließlich diese anonymen Kennzahlen zum Betrieb, zur Sicherheit und zur Verbesserung der Software (Ziffer 10.1 der AGB).

3.6 Nicht Gegenstand dieser Vereinbarung sind die Server-Logfiles (IP-Adresse, Zeitpunkt, aufgerufene Adresse, Statuscode, Browser und Betriebssystem, zuvor besuchte Seite). LUXCODE verarbeitet sie für alle Adressen der Software, auch für die Online-Shops und Helferseiten des Kunden, als eigener Verantwortlicher zur Sicherheit und Stabilität der eigenen Infrastruktur und löscht sie nach 14 Tagen (Datenschutzerklärung von LUXCODE, Ziffer 3.3 und 3.4).

4. Vertraulichkeit

4.1 LUXCODE verpflichtet alle Personen, die Zugang zu den personenbezogenen Daten des Kunden haben, vor Aufnahme ihrer Tätigkeit in Textform zur Vertraulichkeit und unterrichtet sie über die sich aus dieser Vereinbarung ergebenden Pflichten. Die Vertraulichkeitspflicht besteht auch nach Beendigung der Tätigkeit fort.

4.2 Den Kreis der zugriffsberechtigten Personen hält LUXCODE so klein wie möglich und weist ihn dem Kunden auf Anfrage nach (Ziffer 9.1).

4.3 Gesetzliche Offenbarungspflichten bleiben unberührt. Muss LUXCODE aufgrund einer gesetzlichen oder behördlichen Anordnung Daten des Kunden herausgeben, informiert LUXCODE den Kunden vorher, soweit dies rechtlich zulässig ist.

5. Sicherheit der Verarbeitung

5.1 LUXCODE trifft die in Anhang C beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und hält sie für die Dauer dieser Vereinbarung aufrecht. Die Maßnahmen berücksichtigen den Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Risiken für die betroffenen Personen.

5.2 LUXCODE darf die Maßnahmen an die technische Entwicklung anpassen und durch gleichwertige oder bessere Maßnahmen ersetzen. Das Sicherheitsniveau darf dabei nicht unterschritten werden. Wesentliche Änderungen teilt LUXCODE dem Kunden im Kundenportal mit und stellt die aktuelle Fassung von Anhang C dort bereit.

5.3 Der Kunde ist für die Sicherheit in seinem Verantwortungsbereich selbst verantwortlich, insbesondere für den Schutz seiner Zugangsdaten, die Vergabe und Pflege von Benutzerrollen, die Sicherheit seiner Endgeräte und die Nutzung der in der Software angebotenen Sicherheitsfunktionen (z. B. Zwei-Faktor-Authentifizierung).

6. Unterauftragsverarbeiter

6.1 Der Kunde erteilt LUXCODE die allgemeine Genehmigung, die in Anhang B genannten Unterauftragsverarbeiter einzusetzen. Als Unterauftragsverarbeiter gelten Dienstleister, die personenbezogene Daten des Kunden im Auftrag von LUXCODE verarbeiten. Nebenleistungen ohne Zugriff auf diese Daten (z. B. Telekommunikation, Wartung von Betriebsmitteln, Reinigung) sind keine Unterauftragsverarbeitung.

6.2 LUXCODE schließt mit jedem Unterauftragsverarbeiter einen Vertrag nach Art. 28 Abs. 4 DSGVO, der ihm dieselben Datenschutzpflichten auferlegt wie diese Vereinbarung LUXCODE. LUXCODE prüft vor dem Einsatz und danach regelmäßig, dass der Unterauftragsverarbeiter geeignete technische und organisatorische Maßnahmen umsetzt. Kommt ein Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet LUXCODE gegenüber dem Kunden für dessen Pflichterfüllung.

6.3 Beabsichtigt LUXCODE, einen neuen Unterauftragsverarbeiter einzusetzen oder einen bestehenden zu ersetzen, informiert LUXCODE den Kunden mindestens vier Wochen vorher per E-Mail an die hinterlegte Adresse und im Kundenportal unter Angabe von Name, Anschrift, Leistung und Verarbeitungsort. Der Kunde kann der Änderung innerhalb von vier Wochen nach Zugang der Information in Textform widersprechen. Widerspricht der Kunde nicht fristgerecht, gilt die Änderung als genehmigt; LUXCODE weist in der Information auf diese Folge hin.

6.4 Widerspricht der Kunde fristgerecht, bemühen sich die Parteien um eine einvernehmliche Lösung. Gelingt dies nicht innerhalb von zwei Wochen nach dem Widerspruch, kann jede Partei den Nutzungsvertrag mit einer Frist von einem Monat zum Monatsende kündigen; bereits im Voraus gezahlte Vergütung für die Zeit nach dem Vertragsende erstattet LUXCODE. Bis zum Vertragsende setzt LUXCODE den neuen Unterauftragsverarbeiter für die Daten des widersprechenden Kunden nicht ein, soweit dies technisch möglich ist.

6.5 Ein Wechsel, der zur Abwehr eines Sicherheitsrisikos oder zur Behebung einer erheblichen Störung unverzüglich erforderlich ist, darf ohne Einhaltung der Frist nach Ziffer 6.3 erfolgen. LUXCODE informiert den Kunden in diesem Fall so früh wie möglich, spätestens unverzüglich nach dem Wechsel; das Widerspruchs- und Kündigungsrecht nach Ziffer 6.3 und 6.4 gilt entsprechend. Dauerhaft wird der Ersatz erst nach Durchlaufen des Verfahrens nach Ziffer 6.3 eingesetzt.

7. Unterstützung bei Rechten betroffener Personen

7.1 Betroffenenrechte (Art. 12 bis 22 DSGVO) werden gegenüber dem Kunden als Verantwortlichem geltend gemacht. Wendet sich eine betroffene Person an LUXCODE, leitet LUXCODE die Anfrage unverzüglich an den Kunden weiter und beantwortet sie nicht selbst, soweit nicht eine gesetzliche Pflicht besteht.

7.2 LUXCODE unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Betroffenenrechte. Die Software bietet dem Kunden hierfür Funktionen zur Auskunft, Berichtigung, Löschung und zum Export der Daten. Soweit der Kunde ein Anliegen nicht selbst über die Software erledigen kann, führt LUXCODE die erforderlichen Maßnahmen auf Weisung des Kunden innerhalb von zehn Werktagen durch.

7.3 Unterstützungsleistungen, die über die Funktionen der Software hinausgehen und auf Umständen beruhen, die der Kunde zu vertreten hat, darf LUXCODE nach Aufwand gemäß vorherigem Angebot (Anlage 1 der AGB, Ziffer 11), hilfsweise zu einer angemessenen, marktüblichen Vergütung, abrechnen. Ziffer 3.3 Satz 3 bleibt unberührt.

8. Unterstützung bei Sicherheit, Meldungen und Datenschutz-Folgenabschätzung

8.1 LUXCODE unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der LUXCODE zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO.

8.2 Stellt LUXCODE eine Verletzung des Schutzes personenbezogener Daten des Kunden fest (Art. 4 Nr. 12 DSGVO), meldet LUXCODE dies dem Kunden unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, per E-Mail an die im Kundenportal hinterlegte Adresse. Die Meldung enthält, soweit bekannt:

a) eine Beschreibung der Art der Verletzung, der betroffenen Datenkategorien und, soweit möglich, der ungefähren Zahl der betroffenen Personen und Datensätze,

b) den Zeitpunkt oder Zeitraum des Vorfalls und der Feststellung,

c) die wahrscheinlichen Folgen der Verletzung,

d) die ergriffenen und vorgeschlagenen Maßnahmen zur Behebung und zur Begrenzung der Folgen,

e) einen Ansprechpartner bei LUXCODE.

Soweit die Informationen nicht gleichzeitig vorliegen, stellt LUXCODE sie ohne unangemessene Verzögerung nach und dokumentiert den Vorfall.

8.3 Die Meldung an die Aufsichtsbehörde (Art. 33 DSGVO) und die Benachrichtigung der betroffenen Personen (Art. 34 DSGVO) sind Sache des Kunden. LUXCODE liefert die hierfür erforderlichen Informationen und stimmt öffentliche Äußerungen zu einem Vorfall, der den Kunden betrifft, mit diesem ab.

8.4 Benötigt der Kunde für eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO) oder eine vorherige Konsultation der Aufsichtsbehörde (Art. 36 DSGVO) Informationen über die Verarbeitung bei LUXCODE, stellt LUXCODE diese Informationen bereit, insbesondere die Beschreibung der Verarbeitung nach Anhang A und der Maßnahmen nach Anhang C. Ziffer 7.3 gilt entsprechend.

9. Nachweise und Kontrollen

9.1 LUXCODE weist dem Kunden die Einhaltung der Pflichten aus dieser Vereinbarung auf Anfrage nach. Der Nachweis erfolgt vorrangig durch die Vorlage dieser Vereinbarung mit ihren Anhängen, durch eine Selbstauskunft von LUXCODE, durch Zertifikate, Prüfberichte oder Bescheinigungen der Unterauftragsverarbeiter (z. B. ISO 27001 der Rechenzentrumsbetreiber) oder durch Berichte unabhängiger Prüfer.

9.2 Darüber hinaus kann der Kunde höchstens einmal jährlich, bei konkretem Anlass (z. B. einer Datenpanne oder einer Anordnung der Aufsichtsbehörde) jederzeit, selbst oder durch einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer eine Prüfung der Verarbeitung bei LUXCODE einschließlich Inspektionen durchführen. Die Überprüfung ist mindestens 14 Tage vorher in Textform anzukündigen, findet zu den üblichen Geschäftszeiten statt und ist auf das Erforderliche zu beschränken. Prüfer dürfen keine Wettbewerber von LUXCODE sein. Geschäftsgeheimnisse von LUXCODE und Daten anderer Kunden bleiben geschützt.

9.3 Die Rechenzentren der Unterauftragsverarbeiter können nicht unmittelbar vom Kunden betreten werden; hier gelten deren Zertifikate und Prüfberichte als Nachweis.

9.4 Den Aufwand für Überprüfungen nach Ziffer 9.2, die nicht durch einen von LUXCODE zu vertretenden Verstoß veranlasst sind, darf LUXCODE nach Aufwand gemäß vorherigem Angebot (Anlage 1 der AGB, Ziffer 11), hilfsweise zu einer angemessenen, marktüblichen Vergütung, abrechnen. Jede Partei trägt die Kosten der eigenen Prüfer.

9.5 Prüfungen durch eine Aufsichtsbehörde beim Kunden oder bei LUXCODE unterstützen die Parteien gegenseitig. LUXCODE informiert den Kunden unverzüglich über Prüfungshandlungen der Aufsichtsbehörde, die die Daten des Kunden betreffen.

10. Löschung und Rückgabe der Daten

10.1 Während der Vertragslaufzeit kann der Kunde seine Daten jederzeit selbst über die Software exportieren (Ziffer 10.2 der AGB) und, soweit die Software dies vorsieht, selbst löschen.

10.2 Nach Beendigung des Nutzungsvertrags stehen die Daten dem Kunden 30 Tage lang zum Export zur Verfügung. Nach Ablauf dieser Frist löscht LUXCODE die personenbezogenen Daten des Kunden innerhalb weiterer 30 Tage vollständig aus den Produktivsystemen, soweit nicht eine gesetzliche Aufbewahrungspflicht von LUXCODE entgegensteht (Ziffer 10.4 der AGB); das Steuerarchiv nach Ziffer 10.3 der AGB bewahrt LUXCODE im Auftrag des Kunden bis zum Ablauf der Aufbewahrungsfrist auf und

löscht es danach. Verlangt der Kunde vor Ablauf der Exportfrist in Textform die frühere Löschung, löscht LUXCODE unverzüglich, sobald die Cloud-TSE abgemeldet ist, die letzten TSE-Exporte gesichert sind und alle Kassenvorgänge in einem Kassenabschluss erfasst sind; das Steuerarchiv nach Ziffer 10.3 der AGB bleibt dabei erhalten, sofern der Kunde nicht auch dessen Löschung verlangt. Verlangt der Kunde – während oder nach der Vertragslaufzeit – auch die Löschung des Steuerarchivs, übergibt LUXCODE ihm zuvor einen vollständigen Export und löscht das Steuerarchiv anschließend; die Verantwortung für die Erfüllung der Aufbewahrungspflichten geht damit vollständig auf den Kunden über.

10.3 In Datensicherungen enthaltene Daten werden nach dem Sicherungszyklus nach Anhang C gelöscht, spätestens acht Wochen nach der Löschung aus den Produktivsystemen. Bis dahin werden sie nicht aktiv verarbeitet und nur zur Wiederherstellung des Gesamtsystems verwendet.

10.4 Daten, die LUXCODE aufgrund gesetzlicher Pflichten aufbewahren muss (z. B. Rechnungsdaten des Kunden), werden für die Dauer der Aufbewahrungspflicht gesperrt und danach gelöscht.

10.5 Auf Verlangen bestätigt LUXCODE dem Kunden die Löschung in Textform.

11. Pflichten des Kunden

11.1 Der Kunde ist für die Rechtmäßigkeit der Verarbeitung, für die Wahrung der Rechte der betroffenen Personen und für die Erfüllung seiner Informationspflichten nach Art. 13 und 14 DSGVO verantwortlich. Dazu gehört insbesondere, dass der Kunde die Gäste und Besteller seines Online-Shops und die Benutzer seiner Kassen über die Verarbeitung informiert. Verarbeitet der Kunde mit der Software Daten seiner Beschäftigten (z. B. Bedienungen und Kellnerabrechnungen), beachtet er die Vorgaben des Beschäftigtendatenschutzes (Art. 88 DSGVO, § 26 BDSG) und, soweit ein Betriebsrat besteht, dessen Mitbestimmungsrecht bei technischen Einrichtungen, die zur Überwachung von Leistung oder Verhalten geeignet sind (§ 87 Abs. 1 Nr. 6 BetrVG).

11.2 Der Kunde hält seine Kontaktdaten und die Angaben zu weisungsberechtigten Personen im Kundenportal aktuell und stellt sicher, dass die hinterlegte E-Mail-Adresse regelmäßig abgerufen wird. Erhält LUXCODE bei einer Meldung nach Ziffer 8.2 binnen 24 Stunden keine Reaktion, versucht LUXCODE, den Kunden über weitere hinterlegte Kontaktwege zu erreichen.

11.3 Der Kunde informiert LUXCODE unverzüglich, wenn er bei der Prüfung der Leistungen Fehler oder Unregelmäßigkeiten in Bezug auf Datenschutzvorschriften feststellt.

11.4 Der Kunde führt das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO für seine Verarbeitungen selbst. LUXCODE stellt ihm hierfür die Angaben aus Anhang A und C zur Verfügung.

12. Verzeichnis, Haftung und Schlussbestimmungen

12.1 LUXCODE führt ein Verzeichnis aller Kategorien von im Auftrag des Kunden durchgeführten Verarbeitungen nach Art. 30 Abs. 2 DSGVO und stellt es der Aufsichtsbehörde auf Anfrage zur Verfügung.

12.2 LUXCODE ist nach Art. 37 DSGVO und § 38 BDSG derzeit nicht zur Benennung eines Datenschutzbeauftragten verpflichtet. Ansprechpartner für den Datenschutz ist der Inhaber, erreichbar unter hello@openeos.de. Ändert sich dies, teilt LUXCODE dem Kunden die Kontaktdaten des Datenschutzbeauftragten im Kundenportal mit.

12.3 Für die Haftung der Parteien untereinander gilt Ziffer 11 der AGB. Die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt; im Innenverhältnis haftet jede Partei entsprechend ihrem Anteil an der Verantwortung für den Schaden (Art. 82 Abs. 5 DSGVO).

12.4 Änderungen dieses Vertrags bedürfen der Zustimmung des Kunden in Textform, ausgenommen Änderungen der Anhänge B und C nach Ziffern 5.2 und 6. Stimmt der Kunde einer gesetzlich veranlassten Änderung nicht zu, kann jede Partei den Nutzungsvertrag mit einer Frist von einem Monat kündigen.

12.5 Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung, die dem Zweck der Bestimmung am nächsten kommt.

12.6 Im Übrigen gelten die Schlussbestimmungen in Ziffer 14 der AGB, insbesondere zu anwendbarem Recht und Gerichtsstand.

12.7 Für eine Übertragung dieses Vertrags im Wege der Vertragsübernahme gilt Ziffer 14.6 der AGB entsprechend. Die übernehmende Gesellschaft tritt als Auftragsverarbeiter an die Stelle von LUXCODE; LUXCODE informiert den Kunden hierüber vorab nach dem Verfahren der Ziffer 6.3.

Anhang A – Gegenstand der Verarbeitung

A.1 Gegenstand und Zweck

Betrieb der Software OpenEOS als Software-as-a-Service für den Kunden: Kassensystem, Online-Shop bzw. Online-Bestellmodul einschließlich Bestellung am Tisch, Bondruck über den Drucker-Agenten des Kunden, Schichtplanung mit öffentlichen Helferseiten, Anbindung einer Cloud-TSE mit Kassenabschlüssen und Steuerarchiv (Ziffer 10.3 der AGB), Benutzer- und Kontoverwaltung, Auswertungen, Datenexport, auf Wunsch des Kunden Assistent-Funktionen (Speisekarten-Import, Icon-Vorschläge) und Support. Die Verarbeitung dient ausschließlich der Erbringung der in den AGB und der Leistungsbeschreibung (Anlage 1 der AGB) beschriebenen Leistungen.

A.2 Art der Verarbeitung

Erhebung, Speicherung, Anzeige, Übermittlung an die TSE zur Signatur, Übermittlung an den Anbieter des Sprachmodells bei eingeschalteten Assistent-Funktionen, Versand von E-Mails (z. B. Bestellbestätigungen, digitale Belege, Nachrichten an Helfer), Übermittlung an vom Kunden eingerichtete Empfänger (Webhooks, Programmierschnittstelle) auf Weisung des Kunden, Auswertung, Sicherung, Archivierung, Export, Löschung. Die Verarbeitung erfolgt automatisiert in den Rechenzentren der in Anhang B genannten Unterauftragsverarbeiter sowie bei Support-Anfragen durch LUXCODE.

A.3 Kategorien personenbezogener Daten

Bereich	Daten
Kassendaten	Verkaufsvorgänge, Belege, Zahlungsart und Zahlungsstatus, Storno-, Erstattungs- und Änderungsprotokolle, Kassenbuch, TSE-Signaturen und TSE-Protokolle, Kassenabschlüsse (DSFinV-K); Zuordnung zum angemeldeten Benutzer oder zur Bedienung (Bediener, mit Namen im Kassenabschluss) und zum Gerät; optional Name, Telefonnummer und Anmerkungen zur Bestellung
Digitale Belege und Bewirtungsbelege	Links auf digitale Kassenbelege (nur Prüfwert des Links, Bezug auf die Bestellungen, Ablaufdatum); E-Mail-Adresse des Gastes beim Versand eines Belegs per E-Mail (nur für den Versand verwendet, nicht gespeichert; im Verlauf der Bestellung nur Zeitpunkt, Gerät und Ergebnis des Versands); Bewirtungsbelege (fortlaufende Nummer, Ausstellungsdatum, Tag der Bewirtung, Name und, wenn angegeben, Anschrift des Bewirtenden bzw. Leistungsempfängers, Positionen, Beträge, Trinkgeld, Zahlungsart und Zahlungsreferenz, TSE-Angaben, Gerät und Bediener)

Bereich	Daten
Online-Shop und Vorbestellungen	Vor- und Nachname, E-Mail-Adresse, Bestellinhalt, Abholung oder Tischnummer, Zahlungsstatus und Zahlungsreferenz, Bestellzeitpunkt; bei der Bestellung am Tisch per QR-Code Name und Anmerkungen
Schichtplanung und Helferseiten	Name, E-Mail-Adresse, Telefonnummer (optional), Anmerkungen, gewählte Schichten, Bestätigungs- und Erinnerungsstatus, Notizen des Kunden, Verwaltungslinks
Benutzerkonten des Kunden	Vor- und Nachname, E-Mail-Adresse, Rolle und Berechtigungen, Passwort (optional, nur als Hash), Kassen-PIN (nur als Hash), Angaben zur Zwei-Faktor-Anmeldung, Anmeldezeitpunkte und Sitzungen (IP-Adresse, Browser), Protokolle von Aktionen in der Software (mit IP-Adresse und Browser)
Bedienungen (Kassenpersonal)	Kassenprofile ohne Benutzerkonto und ohne E-Mail-Adresse: Name (auch nur Vorname oder Spitzname), Kurzname, Farbe, Rolle (Bedienung oder Schichtleitung) und Rechte, Kassen-PIN (nur als nicht umkehrbarer Prüfwert), Anmeldungen an Geräten (Gerät, Beginn und Ende), Zuordnung der Buchungen (Bestellungen, Zahlungen, Stornos und Erstattungen, Pfand-Auszahlungen, Tischübergaben), Kellnerabrechnungen (Zahlen je Schicht, Zwischenstand)
Geräte	Gerätename, Geräte-Token, Browserkennung, letzte Aktivität; beim Drucker-Agenten Rechnername, Betriebssystem und Version
Assistent-Funktionen (nur bei Opt-in)	hochgeladene Speisekarten (Fotos, PDF, Text), Produktnamen, erzeugte Vorschläge, Nutzungszähler
Ansprechpartner des Kunden	Name, Funktion, E-Mail-Adresse, Telefonnummer, Angaben im Kundenportal
Support-Daten	Inhalt von Support-Anfragen, Kontaktdaten des Anfragenden, Protokolle und Fehlermeldungen, die zur Bearbeitung übermittelt werden

Zahlungsdaten (z. B. vollständige Kartendaten) werden von LUXCODE nicht verarbeitet; sie verbleiben beim Zahlungsdienstleister, mit dem der Kunde unmittelbar vertraglich verbunden ist (Ziffer 7 der AGB). LUXCODE verarbeitet nur den Zahlbetrag, die Zahlungsart, den Zahlungsstatus und die vom Zahlungsdienstleister gemeldeten Angaben zur Zahlung (z. B. Kartenmarke und letzte vier Ziffern) sowie die Zugangsdaten des Kunden für die Anbindung.

A.4 Kategorien betroffener Personen

- Gäste, Besucher und Kunden des Kunden (Käufer an der Kasse, Besteller im Online-Shop),
- Beschäftigte, Mitglieder und ehrenamtliche Helfer des Kunden, die die Software benutzen,
- Helfer, die sich über die Helferseiten für Schichten anmelden,
- Ansprechpartner und Administratoren des Kunden.

A.5 Besondere Kategorien

Die Software ist nicht für die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) und von Daten über strafrechtliche Verurteilungen (Art. 10 DSGVO) bestimmt. Gibt ein Betroffener solche Daten in Freitextfeldern ein (z. B. Allergiehinweise), verarbeitet LUXCODE sie im Rahmen dieses Vertrags und löscht sie mit den Bestelldaten. Der Kunde blendet bei Freitextfeldern einen entsprechenden Hinweis ein und prüft, ob er solche Angaben benötigt.

A.6 Dauer der Verarbeitung

Für die Dauer des Nutzungsvertrags und die anschließenden Export- und Löschfristen nach Ziffer 10 dieser Vereinbarung und Ziffer 10.4, 15.9 und 15.10 der AGB. Bei der Tagesnutzung werden personenbezogene Angaben von Gästen und Helfern 30 Tage nach dem Ende der Veranstaltung bzw. der

letzten Schicht gelöscht oder anonymisiert; Stammdaten bleiben 24 Monate ab dem letzten Nutzungstag im Kundenkonto erhalten. Bedienungen werden 30 Tage nach dem Ende der Veranstaltung, für die sie angelegt sind, anonymisiert, organisationsweit angelegte Bedienungen 30 Tage nach ihrer Deaktivierung oder nach zwölf Monaten ohne Nutzung; ihre Anmeldungen an Geräten werden nach 90 Tagen gelöscht. Links auf digitale Belege werden nach ihrem Ablauf (90 Tage nach der Ausgabe) gelöscht; die E-Mail-Adresse eines Gastes wird nur für den Versand eines Belegs verwendet und nicht gespeichert. Das Steuerarchiv (Ziffer 10.3 der AGB) wird zehn Jahre aufbewahrt, auch über das Vertragsende hinaus (Ziffer 2.2), sofern der Kunde nicht dessen Löschung nach Ziffer 10.2 verlangt; dazu gehören auch Bewirtungsbelege mit dem Namen des Bewirtenden. Zustellprotokolle der Webhooks werden nach 30 Tagen gelöscht.

A.7 Verarbeitungsort

Rechenzentren in Deutschland; E-Mail-Versand über einen Server in Finnland; ab der Freischaltung der Cloud-TSE Signatur durch die Swissbit AG mit Sitz in der Schweiz (Angemessenheitsbeschluss nach Art. 45 DSGVO), nach Angaben des Anbieters in einem Rechenzentrum in Deutschland; Ausnahmen außerhalb der EU nach Anhang B. Support-Tätigkeiten von LUXCODE finden am Sitz von LUXCODE in Deutschland statt.

Anhang B – Unterauftragsverarbeiter

Nr.	Unternehmen	Anschrift	Leistung	Verarbeitungsort
1	IONOS SE	Elgendorfer Straße 57, 56410 Montabaur	Hosting und Betrieb der Software (Server, Datenbanken, Speicher)	Rechenzentren in Deutschland
2	Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen	Speicherung der verschlüsselten Datensicherungen; Betrieb des E-Mail-Servers	Rechenzentrum in Deutschland (Datensicherung); Rechenzentrum in Finnland (E-Mail)
3	Swissbit AG	Industriestrasse 4, 9552 Bronschhofen, Schweiz	Cloud-TSE („Swissbit Cloud TSE 2“, BSI-zertifiziert, derzeit BSI-K-TR-0612-2024): Signatur und Protokollierung der Kassenvorgänge nach § 146a AO, Bereitstellung der TSE-Exporte. Einsatz erst ab der Freischaltung der Cloud-TSE und nach Abschluss eines Vertrags nach Art. 28 Abs. 4 DSGVO; bis dahin keine Verarbeitung	Rechenzentrum nach Angaben des Anbieters in Deutschland; Sitz in der Schweiz; Übermittlungsgrundlage: Angemessenheitsbeschluss der EU-Kommission für die Schweiz (Art. 45 DSGVO)
4	Cloudflare, Inc.	101 Townsend St., San Francisco, CA 94107, USA	DNS und vorgeschalteter Dienst (Weiterleitung mit Entschlüsselung der Verbindung, Zwischenspeicher, Abwehr von Überlastungsangriffen und automatisierten Zugriffen) für Web-App, Online-Shop, Website und Dokumentation; Cloudflare verarbeitet dabei technisch alle übertragenen Inhalte, ohne sie über die Auslieferung hinaus zu speichern	weltweites Netz, Sitz USA; Standardvertragsklauseln und EU-US Data Privacy Framework
5	Functional Software, Inc. (Sentry)	45 Fremont Street, San Francisco, CA 94105, USA	Fehlerdiagnose der Server von Web-App und Programmierschnittstelle	EU-Datenregion, Sitz USA; Standardvertragsklauseln und EU-US Data Privacy Framework

Nr.	Unternehmen	Anschrift	Leistung	Verarbeitungsort
6	IONOS SE	Elgendorfer Straße 57, 56410 Montabaur	Sprachmodell für die Assistent-Funktionen (AI Model Hub: Speisekarten-Import, Icon-Vorschläge), nur für Kunden, die die Assistent-Funktionen eingeschaltet haben	Rechenzentrum in Berlin (nach Angaben von IONOS)

Den E-Mail-Server betreibt LUXCODE selbst auf Servern des Unterauftragsverarbeiters Nr. 2. Weitere Unterauftragsverarbeiter werden derzeit nicht eingesetzt.

Keine Unterauftragsverarbeiter sind die Zahlungsdienstleister des Kunden (derzeit SumUp), weil der Kunde den Vertrag unmittelbar mit ihnen schließt und sie die Zahlungsdaten als eigenständige Verantwortliche verarbeiten (Ziffer 7 der AGB). Stripe nutzt LUXCODE nur für die Abrechnung der eigenen Vergütung gegenüber dem Kunden; dabei werden keine Daten verarbeitet, für die der Kunde Verantwortlicher ist.

Die jeweils aktuelle Liste ist im Kundenportal abrufbar. Änderungen richten sich nach Ziffer 6. Eine Kopie der Standardvertragsklauseln stellt LUXCODE dem Kunden auf Anfrage an hello@openeos.de bereit.

Anhang C – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Die Maßnahmen gelten für die von LUXCODE betriebene Instanz von OpenEOS. Für die Rechenzentren gelten zusätzlich die Maßnahmen der Unterauftragsverarbeiter, die durch deren Zertifizierungen (insbesondere ISO 27001) nachgewiesen werden.

C.1 Vertraulichkeit

Maßnahme	Umsetzung
Zutrittskontrolle	Die Systeme laufen in Rechenzentren von IONOS SE und Hetzner Online GmbH in Deutschland (E-Mail-Server der Hetzner Online GmbH in Finnland) mit Zutrittskontrolle, Videoüberwachung und Sicherheitspersonal nach deren Zertifizierungen. LUXCODE betreibt keine eigenen Serverräume; am Sitz von LUXCODE werden keine Kundendaten dauerhaft gespeichert.
Zugangskontrolle	Administrativer Zugang zu Servern nur über SSH mit Schlüsselauthentifizierung, Passwortanmeldung deaktiviert. Verwaltungsoberflächen der Hosting-Anbieter und alle Admin-Zugänge mit Zwei-Faktor-Authentifizierung. Passwortregeln für Benutzerkonten in der Software (Mindestlänge 8 Zeichen, Sperre für 15 Minuten nach 5 Fehlversuchen) oder Anmeldung über zeitlich begrenzte Anmeldelinks; Zwei-Faktor-Authentifizierung (App oder E-Mail-Code) für Kundenkonten als Option. Sitzungen laufen nach Inaktivität ab.
Zugriffskontrolle	Rollen- und Berechtigungskonzept in der Software (Rollen Administrator und Mitglied, für Mitglieder einzeln vergebene Modulberechtigungen, z. B. Produkte, Veranstaltungen, Geräte, Mitglieder, Schichtpläne, Berichte, Stornieren und Erstatten) mit dem Grundsatz der geringsten Berechtigung. Kassengeräte melden sich mit eigenem Geräte-Token an; API-Tokens haben beschränkte Berechtigungen und keinen Zugriff auf Zahlungen, Erstattungen, Mitglieder und Löschungen. Strikte Mandantentrennung: jedes Kundenkonto greift nur auf eigene Daten zu, erzwungen in der Anwendung. Administrativer Zugriff von LUXCODE auf Kundendaten nur für Support und Betrieb, mit der Support-PIN des Kunden, protokolliert.
Trennungskontrolle	Logische Trennung der Kundendaten je Kundenkonto. Getrennte Test- und Produktivumgebung (Staging mit eigener Datenbank). Im Testmodus einer Veranstaltung werden Buchungen nicht signiert, solange keine Cloud-TSE aktiv ist; bei aktiver Cloud-TSE werden sie als Trainingsbuchungen signiert und getrennt von echten Verkäufen ausgewiesen. Entwicklungs- und Testsysteme arbeiten ohne echte Kundendaten.

Maßnahme	Umsetzung
Pseudonymisierung und Verschlüsselung	Speicherung auf verschlüsselten Datenträgern. Passwörter, Kassen-PINs und API-Tokens nur als Hash (Passwörter mit bcrypt). Zugangsdaten der Cloud-TSE und Geheimnisse der Zwei-Faktor-Anmeldung werden verschlüsselt gespeichert. Datensicherungen werden vor der Übertragung zu Hetzner verschlüsselt (AES-256); die Schlüssel verbleiben bei LUXCODE. Nutzungs- und Leistungsdaten für eigene Zwecke nur anonymisiert.

C.2 Integrität

Maßnahme	Umsetzung
Weitergabekontrolle	Jede Übertragung zwischen Endgeräten, Software, TSE und Schnittstellen über TLS 1.2 oder höher mit aktuellen Cipher-Suiten; unverschlüsselte Verbindungen werden abgewiesen. API-Zugriffe nur mit personen- oder kontobezogenen Schlüsseln. Datenexporte nur für angemeldete, berechtigte Benutzer. Kein Transport von Kundendaten auf mobilen Datenträgern.
Eingabekontrolle	Protokollierung von Anlage, Änderung und Löschung von Stammdaten, Benutzern und Berechtigungen mit Benutzer und Zeitstempel. Kassenvorgänge werden bei aktiver Cloud-TSE durch die TSE signiert und fortlaufend nummeriert; nachträgliche Änderungen sind nur als dokumentierte Storno- oder Korrekturvorgänge möglich. Server- und Anwendungsprotokolle werden zentral gesammelt und gegen Veränderung geschützt.

C.3 Verfügbarkeit und Belastbarkeit

Maßnahme	Umsetzung
Verfügbarkeitskontrolle	Tägliche automatisierte Datensicherung mit verschlüsselter Ablage bei Hetzner, getrennt vom Produktivstandort; Aufbewahrung der täglichen Sicherungen für 14 Tage und der wöchentlichen für acht Wochen; die beiden jüngsten Sicherungen zusätzlich verschlüsselt auf dem Produktivserver. Regelmäßiger, mindestens halbjährlicher Test der Wiederherstellung. Redundante Stromversorgung, Klimatisierung und Netzanbindung in den Rechenzentren. Firewall, Beschränkung offener Dienste, automatische Sicherheitsupdates des Betriebssystems.
Monitoring	Überwachung von Erreichbarkeit, Auslastung und Fehlern mit Alarmierung an LUXCODE; Fehlerdiagnose mit Sentry (Anhang B Nr. 5). Störungen der Cloud-TSE werden an der Kasse angezeigt und den Administratoren des Kunden per E-Mail gemeldet. Wartungsfenster und Störungsbehebung nach Ziffer 5 der AGB.
Rasche Wiederherstellung	Dokumentiertes Verfahren zur Wiederherstellung aus der Datensicherung; Infrastruktur als Code bzw. dokumentierte Serverkonfiguration, sodass die Systeme auf neuer Infrastruktur neu aufgebaut werden können.

C.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Maßnahme	Umsetzung
Datenschutz-Management	Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO. Jährliche Überprüfung dieser Maßnahmen und der Unterauftragsverarbeiter durch LUXCODE; Anpassung bei wesentlichen Änderungen der Software oder Infrastruktur.
Vorfallsmanagement	Dokumentierter Prozess für Datenpannen: Erkennung, Bewertung, Eindämmung, Meldung an den Kunden innerhalb von 24 Stunden nach Ziffer 8.2, Nachbereitung. Protokollierung aller Vorfälle.
Datenschutzfreundliche Voreinstellungen	Die Software erhebt nur die für die jeweilige Funktion erforderlichen Daten; optionale Felder sind standardmäßig deaktiviert. Die Assistent-Funktionen sind standardmäßig ausgeschaltet und werden nur von einem Administrator des Kunden eingeschaltet. Löschfristen sind in der Software hinterlegt und laufen automatisch ab.
Auftragskontrolle	Verträge in Textform oder elektronischem Format nach Art. 28 Abs. 4 und 9 DSGVO mit allen Unterauftragsverarbeitern; Prüfung ihrer Zertifikate vor Einsatz und jährlich. Weisungen des Kunden nur in Textform (Ziffer 3).

Maßnahme	Umsetzung
Software-Sicherheit	Abhängigkeiten werden regelmäßig auf bekannte Schwachstellen geprüft und aktualisiert (automatische Prüfungen in den öffentlichen Repositories). Sicherheitsrelevante Änderungen durchlaufen Tests vor der Freigabe. Der Quellcode von OpenEOS ist öffentlich einsehbar; Sicherheitsmeldungen können an hello@openeos.de gerichtet werden.

C.5 Löschung

Maßnahme	Umsetzung
Löschkonzept	Automatische Löschung nach den Fristen der AGB (personenbezogene Angaben von Gästen und Helfern 30 Tage nach dem Ende der Veranstaltung bzw. der letzten Schicht, Bedienungen 30 Tage nach dem Ende der Veranstaltung bzw. bei organisationsweit angelegten Bedienungen 30 Tage nach der Deaktivierung oder nach zwölf Monaten ohne Nutzung durch Anonymisierung und ihre Anmeldungen an Geräten nach 90 Tagen, Links auf digitale Belege nach ihrem Ablauf (90 Tage), Stammdaten 24 Monate nach dem letzten Nutzungstag, Kundendaten nach Vertragsende nach Ziffer 10 dieser Vereinbarung, Steuerarchiv nach Ablauf von zehn Jahren). Löschung in Datensicherungen durch automatisches Löschen älterer Sicherungen innerhalb von acht Wochen. Webserver-Logfiles werden nach 14 Tagen gelöscht, Sicherheits- und Änderungsprotokolle nach 90 Tagen, soweit sie nicht zur Aufklärung eines Vorfalls benötigt werden. Datenträger der Rechenzentren werden nach den Verfahren der Unterauftragsverarbeiter sicher gelöscht oder vernichtet.