Anlage 5 zum EVB-IT Systemvertrag DiWeNY und **Anlage 1** zum EVB-IT Cloudvertrag DiWeNY

Vereinbarung gem. Art. 28 DSGVO über die Auftragsverarbeitung personenbezogener Daten

zwischen

Staatsbad Norderney GmbH, vertreten durch den Geschäftsführer Wilhelm Loth, Am Kurplatz 3, 26548 Norderney

Vertragsnummer/Kennung Auftraggeber: _____

„Auftraggeber“

und
[…]
Vertragsnummer/Kennung Auftragnehmer: _____

„Auftragnehmer“

wird folgender Vertrag geschlossen:

Präambel

Der Auftragnehmer erbringt auf Grundlage des EVB-IT Systemvertrags „Digitale Wellen für Norderney (DiWeNY)“ und des damit verbundenen EVB-IT Cloudvertrags DiWeNY (zusammen nachfolgend „Hauptvertrag“) für den Auftraggeber Leistungen zur Lieferung, Installation, Integration und Inbetriebnahme eines Zutrittskontroll- und Kassensystems für das bade:haus Norderney einschließlich Hardware, Automaten und Schnittstellen zur Commerce-Plattform und zur Norderney-App, zum Systemservice sowie zur cloudbasierten Bereitstellung der Software (Software as a Service) einschließlich Hosting, Pflege, Support und Hotline. Hierbei verarbeitet der Auftragnehmer personenbezogene Daten, für die der Auftraggeber im Sinne der DSGVO verantwortlich ist.

Mit dieser Vereinbarung zur Auftragsverarbeitung (nachfolgend „AVV“) werden die damit verbundenen datenschutzrechtlichen Pflichten konkret geregelt. Die AVV ist Bestandteil beider Verträge und gilt für alle Leistungsteile einheitlich. Bei Widersprüchen gehen die Regelungen dieser AVV vor.

1 Umfang der Beauftragung

1.1 Die Regelungen dieser AVV gelten, sobald der Auftragnehmer im Rahmen seiner hauptvertraglichen Leistungen Zugang oder Zugriff auf personenbezogene Daten (nachfolgend „Daten“) erhält, für die der Auftraggeber verantwortlich ist. Das gilt insbesondere für den Betrieb und das Hosting der Cloudsoftware, die Datenübernahme aus dem Vorsystem, die Einrichtung und den Betrieb der Schnittstellen, den Fernzugriff (Teleservice) sowie die Störungsbeseitigung, Wartung und den Support. In diesen Fällen verarbeitet der

Auftragnehmer die Daten im Auftrag und nach Weisung des Auftraggebers i. S. v. Art. 28 DSGVO. Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn.

1.2 Art, Umfang und Zweck der Verarbeitung, die Arten der Daten und die Kategorien betroffener Personen ergeben sich aus Annex 1. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags einschließlich eines Übergangszeitraums nach Nummer 3.2.3 des Cloudvertrags; Ziffer 11 bleibt unberührt.

1.3 Die Verarbeitung, das Hosting und die Datenhaltung finden ausschließlich in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) statt (Nummer 1.1 Cloudvertrag; LB Ziff. 2.1.1). Eine Verarbeitung außerhalb der EU/des EWR – einschließlich eines Zugriffs aus einem Drittland, etwa im Rahmen von Support oder Fernwartung – ist nur nach vorheriger Zustimmung des Auftraggebers in Textform zulässig und nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

1.4 Die Verarbeitung darf erst beginnen, wenn diese AVV wirksam unterzeichnet ist.

2 Verantwortlichkeit des Auftraggebers

2.1 Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich.

2.2 Der Auftraggeber stellt dem Auftragnehmer die Daten rechtzeitig zur Verfügung, insbesondere die Exportdateien der Altdaten nach Nummer 13 des Systemvertrags, und ist für deren Qualität verantwortlich. Er informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten in Bezug auf datenschutzrechtliche Bestimmungen oder seine Weisungen feststellt.

3 Weisungsbefugnisse des Auftraggebers

3.1 Dem Auftraggeber steht hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht zu. Weisungen erfolgen in Textform; mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform. Änderungen des Verarbeitungsgegenstands und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

3.2 Weisungsberechtigte Personen des Auftraggebers und Weisungsempfänger des Auftragnehmers sind ausschließlich die in Ziffer 11.1 des EVB-IT Systemvertrags genannten Personen. Änderungen bei den benannten Personen teilen die Parteien einander unverzüglich in Textform mit.

3.3 Der Auftragnehmer verarbeitet die Daten ausschließlich nach den Weisungen des Auftraggebers, sofern er nicht gesetzlich zu einer anderen Verarbeitung verpflichtet ist. In diesem Fall teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung in Textform mit, sofern das Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.4 Eine Verarbeitung der Daten zu eigenen Zwecken des Auftragnehmers ist ausgeschlossen, auch in anonymisierter oder aggregierter Form (Nummer 9 „Datenhoheit“ Cloudvertrag). Das gilt insbesondere für Produktentwicklung, Benchmarking, Werbung sowie das Training oder die Verbesserung von KI-Systemen.

3.5 Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen diese AVV oder geltendes Datenschutzrecht verstößt, weist er den Auftraggeber unverzüglich darauf hin. Er darf die Ausführung der Weisung bis zu ihrer Bestätigung durch den Auftraggeber aussetzen.

4 Anforderungen an das Personal des Auftragnehmers

Der Auftragnehmer setzt ausschließlich Personen ein, die er vor Aufnahme ihrer Tätigkeit zur Vertraulichkeit verpflichtet und mit den maßgeblichen Datenschutzbestimmungen vertraut gemacht hat oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Das gilt auch für das Montage- und Servicepersonal vor Ort im bade:haus. Die Verpflichtung ist zu dokumentieren und dem Auftraggeber auf Anforderung nachzuweisen.

5 Einschaltung von Subunternehmern

5.1 Der Auftragnehmer beauftragt Subunternehmer (weitere Auftragsverarbeiter) nur mit vorheriger Zustimmung des Auftraggebers in Textform. Nummer 8.4 des Cloudvertrags bleibt unberührt.

5.2 Der Auftragnehmer setzt Subunternehmer nur ein, soweit sichergestellt ist, dass sie die Voraussetzungen von Art. 28 DSGVO erfüllen, und überträgt ihnen sämtliche datenschutzrechtlichen Pflichten aus dieser AVV. Dem Auftraggeber sind im Unterauftragsverarbeitungsvertrag unmittelbar sämtliche Kontrollrechte nach Ziffer 10 einzuräumen (echter Vertrag zugunsten Dritter). Der Auftragnehmer haftet für ein Verschulden des Subunternehmers wie für eigenes Verschulden.

5.3 Zur Prüfung der Zustimmung stellt der Auftragnehmer dem Auftraggeber den Entwurf des Unterauftragsverarbeitungsvertrags zur Verfügung; kommerzielle Inhalte ohne datenschutzrechtliche Bedeutung dürfen geschwärzt werden. Er bestätigt in Textform, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der technischen und organisatorischen Maßnahmen sorgfältig ausgewählt und sich von deren Einhaltung überzeugt hat.

5.4 Der Auftraggeber erteilt seine Zustimmung, wenn keine berechtigten Interessen, insbesondere Gründe in der Person des Subunternehmers oder datenschutzrechtliche Gründe, entgegenstehen.

5.5 Der Zustimmungspflicht unterliegen auch Leistungen, bei denen ein Zugriff auf Auftraggeberdaten nicht ausgeschlossen werden kann. Dazu gehören insbesondere Rechenzentrums- und Hosting-Anbieter, Anbieter von Backup-, Fernwartungs-, Ticket- und Kollaborationssystemen, E-Mail- und SMS-Versanddienstleister (Terminerinnerungen, Rechnungsversand), Hersteller der Automaten und Schrankschlösser mit Fernzugriff, Montage- und Servicepartner sowie Anbieter von KI-Systemen.

5.6 Der Auftragnehmer setzt derzeit die in Annex 2 aufgeführten Subunternehmer ein und bestätigt, dass er sie nach Art. 28 DSGVO verpflichtet hat. Der Auftraggeber stimmt diesen Subunternehmern hiermit zu.

5.7 Der Auftragnehmer überprüft die Einhaltung der Pflichten durch die Subunternehmer regelmäßig, mindestens jährlich. Der Nachweis kann auch durch genehmigte Verhaltensregeln (Art. 40 DSGVO) oder Zertifizierungen (Art. 42 DSGVO) erfolgen.

6 Sicherheit der Verarbeitung

6.1 Der Auftragnehmer trifft nach Art. 32 DSGVO die erforderlichen technischen und organisatorischen Maßnahmen, um unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie des Risikos für die Rechte und Freiheiten der Betroffenen ein angemessenes Schutzniveau zu gewährleisten.

6.2 Die Maßnahmen sind in Annex 3 dargestellt. Die Mindestanforderungen in Annex 3 Teil A sind verbindlich. Die Anforderungen an die IT-Sicherheit nach Nummer 8.2 des Cloudvertrags und Anlage 3 zum Cloudvertrag (Kriterienkatalog), insbesondere der Nachweis eines ISMS nach ISO/IEC 27001 oder BSI C5 für das Rechenzentrum, bleiben unberührt.

6.3 Ein Fernzugriff auf Systeme und Geräte im bade:haus (Teleservice) erfolgt nur nach Freigabe durch den Auftraggeber, über gesicherte und verschlüsselte Verbindungen mit personalisierten Zugängen und wird protokolliert (Nummer 5 des Systemvertrags). Das Protokoll ist dem Auftraggeber auf Anforderung vorzulegen.

6.4 Personen-, Artikel-, Zeit- oder Abrechnungsdaten werden nicht auf den Transpondermedien gespeichert (LB Ziff. 2.1.1). Soweit Kassen, Zutrittsterminals oder Automaten bei Ausfall der Internetverbindung Daten lokal zwischenspeichern, sind diese verschlüsselt abzulegen und nach erfolgreicher Synchronisation zu löschen.

6.5 Für Test-, Schulungs- und Migrationszwecke sind Daten zu anonymisieren oder zu pseudonymisieren, soweit der Zweck dies zulässt. Die Verwendung von Echtdaten in Test- oder Schulungsumgebungen bedarf der vorherigen Zustimmung des Auftraggebers in Textform. Testimporte der Altdaten (Nummer 13 des Systemvertrags) erfolgen ausschließlich in der Umgebung des Auftragnehmers innerhalb der EU/des EWR; Exportdateien sind nach Abschluss des Live-Imports zu löschen.

6.6 Arbeiten Mitarbeiter des Auftragnehmers außerhalb seiner Betriebsstätten (mobiles Arbeiten), stellt der Auftragnehmer sicher, dass der Zugriff nur über gesicherte Verbindungen (z. B. VPN mit Zwei-Faktor-Authentifizierung) und ausschließlich mit dienstlichen Geräten erfolgt. Die Speicherung von Auftraggeberdaten auf privaten Geräten oder Datenträgern ist untersagt. Der Auftraggeber kann diese Erlaubnis in Textform widerrufen.

6.7 Der Auftragnehmer darf alternative Maßnahmen nach vorheriger Zustimmung des Auftraggebers in Textform umsetzen, sofern das Schutzniveau nach Annex 3 nicht unterschritten wird. Erweisen sich die Maßnahmen als unzureichend oder erfordert der technische Fortschritt weitere Maßnahmen, setzt der Auftragnehmer diese auf Weisung des Auftraggebers um und informiert ihn unverzüglich, wenn er Anlass zu dieser Annahme hat.

7 Betroffenenrechte

7.1 Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen (Art. 12 bis 22 DSGVO). Die Software muss es dem Auftraggeber ermöglichen, Daten einzelner Gäste selbst zu beauskunften, zu berichtigen, zu sperren und zu löschen, soweit dem keine gesetzlichen Aufbewahrungspflichten (insbesondere § 147 AO, GoBD, KassenSichV) entgegenstehen.

7.2 Auskünfte an Dritte oder Betroffene erteilt der Auftragnehmer nur nach vorheriger Zustimmung des Auftraggebers. Unmittelbar an ihn gerichtete Anfragen leitet er unverzüglich an den Auftraggeber weiter.

7.3 Der Auftragnehmer kann auf Einzelweisung den gesamten zu einer betroffenen Person gespeicherten Datensatz in einem strukturierten, gängigen und maschinenlesbaren Format an den Auftraggeber übergeben.

8 Mitteilungs- und Unterstützungspflichten des Auftragnehmers

8.1 Der Auftragnehmer informiert den Auftraggeber unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung, über Verletzungen des Schutzes personenbezogener Daten in seinem Verantwortungsbereich (Art. 33, 34 DSGVO). Er ergreift unverzüglich alle zumutbaren Maßnahmen, um die Daten zu sichern und nachteilige Folgen für Betroffene zu begrenzen. Die Mitteilung enthält mindestens:

- eine Beschreibung der Art der Verletzung, der Kategorien und ungefähren Anzahl der betroffenen Personen und Datensätze;
- Name und Kontaktdaten eines Ansprechpartners;
- eine Beschreibung der wahrscheinlichen Folgen;
- eine Beschreibung der ergriffenen und vorgeschlagenen Maßnahmen.

8.2 Der Auftragnehmer unterstützt den Auftraggeber im erforderlichen Umfang bei Kontrollen durch Aufsichtsbehörden, bei der Geltendmachung von Betroffenenrechten, bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen (Art. 35, 36 DSGVO) sowie bei der Führung des Verzeichnisses von Verarbeitungstätigkeiten.

8.3 Wird der Zugriff auf die Daten durch Maßnahmen Dritter gefährdet (z. B. Insolvenz, Beschlagnahme, Pfändung), benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

9 Rückgabe und Löschung der Daten

9.1 Nach Beendigung der Leistungen gibt der Auftragnehmer die Daten nach Wahl des Auftraggebers zurück oder löscht sie, sofern keine gesetzliche Pflicht zur weiteren Speicherung besteht. Für Art und Format der Herausgabe sowie den Übergangsbetrieb gilt Nummer 3.2.3 des Cloudvertrags (Herausgabe als SQL-Dump und CSV mit Datenmodellbeschreibung, Bereitstellung in einer für die Kassennachschau und § 147 AO geeigneten Form).

9.2 Die Löschung umfasst auch Kopien, Sicherungen, Datenbankauszüge, Exportdateien sowie Daten in Test-, Schulungs- und Ticketsystemen und bei Subunternehmern. Sie erfolgt erst nach Bestätigung des Datenempfangs durch den Auftraggeber und ist zu protokollieren; das Löschprotokoll ist dem Auftraggeber vorzulegen. Sicherungen, die nicht gezielt gelöscht werden können, werden spätestens mit Ablauf des regulären Sicherungszyklus überschrieben.

9.3 Datenträger in zurückgegebener oder ausgetauschter Hardware (z. B. Kassen-PCs, Automaten) sind vor Weitergabe oder Entsorgung nach dem Stand der Technik zu löschen; die Löschung ist auf Anforderung nachzuweisen.

9.4 Dokumentationen, die dem Nachweis der ordnungsgemäßen Verarbeitung dienen, darf der Auftragnehmer entsprechend den gesetzlichen Aufbewahrungsfristen auch nach Vertragsende aufbewahren.

10 Nachweise und Überprüfungen

10.1 Der Auftragnehmer stellt dem Auftraggeber auf Anforderung alle erforderlichen Informationen zum Nachweis der Einhaltung seiner Pflichten zur Verfügung.

10.2 Der Auftraggeber ist berechtigt, die Einhaltung dieser AVV, insbesondere der technischen und organisatorischen Maßnahmen, selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer zu überprüfen, einschließlich Inspektionen. Inspektionen erfolgen nach angemessener Vorankündigung während der üblichen Geschäftszeiten unter Rücksicht auf die Betriebsabläufe; anlassbezogene Prüfungen bleiben unberührt. Weitergehende Prüfrechte nach Nummer 8.3 des Cloudvertrags bleiben unberührt.

10.3 Der Auftragnehmer kann geeignete Maßnahmen auch durch genehmigte Verhaltensregeln (Art. 40 DSGVO), Zertifizierungen (Art. 42 DSGVO) oder aktuelle Testate unabhängiger Stellen (z. B. ISO/IEC 27001, BSI C5) nachweisen. Das Recht nach Ziffer 10.2 bleibt unberührt.

11 Vertragsdauer und Kündigung

Laufzeit und Kündigung dieser AVV richten sich nach dem Hauptvertrag. Sie gilt, solange einer der beiden Verträge besteht oder der Auftragnehmer Auftraggeberdaten verarbeitet oder in Besitz hat. Eine isolierte Kündigung dieser AVV ist ausgeschlossen. Ein schwerwiegender Verstoß des Auftragnehmers gegen diese AVV berechtigt den Auftraggeber zur Kündigung beider Verträge aus wichtigem Grund.

12 Haftung

12.1 Der Auftragnehmer haftet für Schäden des Auftraggebers aus schuldhaften Verstößen gegen diese AVV oder gegen ihn unmittelbar treffende Datenschutzpflichten nach den gesetzlichen Vorschriften. Bei leichter Fahrlässigkeit ist die Haftung je Schadensfall und je Vertragsjahr auf 2.000.000 Euro begrenzt (Deckungssumme nach Nummer 18.3 Systemvertrag). Abweichende Haftungsbegrenzungen des Hauptvertrags, der EVB-IT System-AGB und der EVB-IT Cloud-AGB gelten insoweit nicht.

12.2 Keine Begrenzung gilt bei Vorsatz und grober Fahrlässigkeit, bei der Verletzung von Leben, Körper oder Gesundheit sowie bei Verstößen gegen Ziffer 1.3 (Drittlandverarbeitung) und Ziffer 3.4 (Nutzung für eigene Zwecke).

12.3 Nehmen Betroffene oder Dritte den Auftraggeber wegen eines Verstoßes in Anspruch, den der Auftragnehmer zu vertreten hat, stellt dieser den Auftraggeber im Innenverhältnis nach Art. 82 Abs. 5 DSGVO frei; Ziffer 12.1 Satz 2 gilt entsprechend. Der Auftraggeber informiert den Auftragnehmer unverzüglich und führt Vergleichsverhandlungen nur in Abstimmung mit ihm.

12.4 Die Haftung gegenüber Betroffenen im Außenverhältnis (Art. 82 DSGVO) bleibt unberührt.

13 Schlussbestimmungen

13.1 Ein Zurückbehaltungsrecht (§ 273 BGB) an den Daten und den zugehörigen Datenträgern ist ausgeschlossen.

13.2 Änderungen und Ergänzungen dieser AVV bedürfen der Schriftform; die elektronische Form (§ 126a BGB) genügt. Für Weisungen gilt Ziffer 3.1.

13.3 Sollte eine Bestimmung unwirksam sein, bleibt die AVV im Übrigen wirksam. Die Parteien ersetzen die unwirksame Bestimmung durch eine zulässige Regelung, die ihrem Zweck am nächsten kommt und Art. 28 DSGVO genügt.

13.4 Bei Widersprüchen zwischen dieser AVV und dem Hauptvertrag gehen die Regelungen dieser AVV vor.

Unterschrift Auftraggeber	**Unterschrift Auftragnehmer**
Datum, Auftraggeber	Datum, Auftragnehmer

Annex 1 – Zweck, Art und Umfang der Verarbeitung, Arten der Daten, Kategorien betroffener Personen

Art und Zweck der Verarbeitung

Bereitstellung, Hosting, Betrieb und Pflege des cloudbasierten Abrechnungs- und Zutrittskontrollsystems (Kassen-, Zutritts-, Automaten-, Gastronomie-, Termin- und Kursplanungssoftware, Partnerhotelverwaltung, Fibu-Export, Reporting-Datenbank) für das bade:haus Norderney; Einrichtung und Betrieb der Schnittstellen zur Commerce-Plattform und zur Norderney-App einschließlich Synchronisierung von Kundendaten; Übernahme von Gutschein-, Wertkarten- und Mehrfachkartendaten aus dem Vorsystem HKS; Installation, Inbetriebnahme, Schulung, Systemservice, Fernwartung, Störungsbeseitigung, Support und Hotline; Herausgabe und Löschung der Daten bei Vertragsende.

Arten der personenbezogenen Daten

- Stammdaten der Gäste und Karteninhaber: Name, Kundennummer bzw. Kennung des Benutzerkontos, Anschrift, E-Mail-Adresse, Telefonnummer, Tarif- und Ermäßigungsmerkmale
- Gastfoto bei Jahreskarten (ausschließlich zur Sichtkontrolle, keine biometrische Auswertung)
- Medien- und Zutrittsdaten: Transponder-/Medien-ID, QR-Code-/E-Ticket-Kennung, Zutritts- und Zonenübertritte mit Zeitstempel, Verweildauer, Schrankzuordnung, ausgeliehene Handtücher
- Vertrags-, Kauf- und Abrechnungsdaten: gekaufte Leistungen, Wert-, Mehrfachkarten- und Gutscheinsalden, Pfand, Nachzahlungen, Rechnungen, Belege
- Zahlungsdaten: Zahlart, Betrag, Transaktionskennung, ggf. maskierte Kartennummer (keine vollständigen Kartendaten)
- Termin- und Buchungsdaten für Wellnessanwendungen und Kurse: gebuchte Leistung, Termin, Raum, Behandler, Stornierungen, Benachrichtigungen
- Daten der Partnerhotels: Ansprechpersonen, Buchungen, Abrechnungen
- ☒ Benutzer- und Protokolldaten der Beschäftigten: Benutzername, Rolle, Berechtigungen, Kassen-, Schicht- und Bedienerdaten, Änderungsprotokolle
- Kommunikations- und Supportdaten: Inhalte von Tickets, Hotline-Anfragen, Fernwartungsprotokolle
- Technische Daten: IP-Adressen, Geräte- und Logdaten

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)

- keine –

Kategorien betroffener Personen

- Gäste und Besucher des bade:haus (einschließlich Hotelgäste von Partnerhotels)
- Inhaber von Wert-, Mehrfach-, Saison- und Jahreskarten sowie Gutscheinen

- Nutzer der Commerce-Plattform und der Norderney-App, soweit Daten über die Schnittstellen übermittelt werden
- Ansprechpersonen der Partnerhotels und sonstiger Geschäftspartner
- Beschäftigte des Auftraggebers (insbesondere Kassen-, Concierge- und Wellnesspersonal, Administratoren)

Ort der Verarbeitung

Hosting und Datenhaltung: Rechenzentrum Name, Standort – vom Bieter anzugeben, ausschließlich EU/EWR. Lokale Komponenten: Kassen, Terminals und Automaten im bade:haus Norderney. Support und Fernwartung: Standort(e) – vom Bieter anzugeben, ausschließlich EU/EWR.

Annex 2 – Subunternehmer

- vom Bieter auszufüllen –

(Hierzu gehören auch Rechenzentrums-/Hosting-Anbieter, Anbieter von Backup-, Fernwartungs- und Ticketsystemen, E-Mail- und SMS-Versanddienstleister sowie Hersteller und Servicepartner mit Zugriff auf Auftraggeberdaten.)

Unternehmen	Anschrift	Leistung / Zweck	Ort der Verarbeitung

Annex 3 – Technische und organisatorische Maßnahmen des Auftragnehmers

Teil A – Verbindliche Mindestanforderungen des Auftraggebers

☒ Hosting und Datenhaltung ausschließlich in der EU/im EWR; Nachweis ISMS nach ISO/IEC 27001 oder BSI C5 für das Rechenzentrum (Nummer 8.2 Cloudvertrag)

☒ Keine Speicherung von Personen-, Artikel-, Zeit- oder Abrechnungsdaten auf den Transpondermedien; Mifare-Medien mit sicherer Schlüsselverwaltung

☒ Verschlüsselte Zwischenspeicherung auf Kassen, Terminals und Automaten im Offline-Betrieb; Löschung nach Synchronisation

☒ Fernzugriff nur nach Freigabe des Auftraggebers, mit personalisierten Zugängen, Zwei-Faktor-Authentifizierung und Protokollierung

☒ Transportverschlüsselung nach dem Stand der Technik (mindestens TLS 1.2) für alle Schnittstellen und Datenübertragungen, einschließlich Commerce-Plattform, Norderney-App und Fibu-Export

☒ Verschlüsselung der Daten im Ruhezustand in der Cloud-Datenbank und in Backups

☒ Rollen- und Berechtigungskonzept nach dem Need-to-know-Prinzip, konfigurierbar durch den Auftraggeber; individuelle Benutzerkennungen, keine Gruppenkonten

☒ Mandantentrennung gegenüber anderen Kunden des Auftragnehmers

☒ Tägliche Datensicherung, Aufbewahrung 30 Tage, jährlicher Wiederherstellungstest (Nummer 9 Cloudvertrag)

☒ Konfigurierbare Löschfristen und Löschfunktionen für Gästedaten unter Beachtung der gesetzlichen Aufbewahrungspflichten

☒ Protokollierung von Zugriffen, Änderungen und Löschungen; Protokolle zur Verhaltens- und Leistungskontrolle von Beschäftigten nur nach Vorgabe des Auftraggebers auswertbar

☒ Regelmäßiges Patchmanagement; Bereitstellung und Pflege einer SBOM (Nummer 4.10 Systemvertrag)

☒ Dokumentierter Prozess zur Meldung von Datenschutzverletzungen (Ziffer 8.1)

☒ Löschung von Datenträgern in ausgetauschter oder zurückgegebener Hardware nach dem Stand der Technik

Teil B – Weitere Maßnahmen des Auftragnehmers

- Vom Bieter auszufüllen und zu ergänzen; Nachweise (Zertifikate, Testate) sind beizufügen. –

1. Vertraulichkeit

Zutrittskontrolle (Rechenzentrum, Betriebsstätten)

☐ Zutrittskontrollsystem / Chipkarten

- ☐ Alarmanlage / Videoüberwachung
- ☐ Besucherregelung und -protokollierung
- ☐ Beaufsichtigung von Fremdpersonal
- ☐ weitere Maßnahmen: _____

Zugangskontrolle

- ☐ Zwei-Faktor-Authentifizierung
- ☐ Passwortrichtlinie
- ☐ automatische Sperre nach Fehlversuchen
- ☐ Firewall / Netzwerksegmentierung
- ☐ VPN
- ☐ Verschlüsselung mobiler Endgeräte
- ☐ weitere Maßnahmen: _____

Zugriffskontrolle

- ☐ rollenbasiertes Berechtigungskonzept
- ☐ Begrenzung der Administratoren
- ☐ Protokollierung von Zugriffen
- ☐ Datenträgervernichtung nach DIN 66399
- ☐ weitere Maßnahmen: _____

Trennungskontrolle

- ☐ logische Mandantentrennung
- ☐ Trennung von Produktiv-, Test- und Schulungssystem
- ☐ Pseudonymisierung / Anonymisierung von Testdaten
- ☐ weitere Maßnahmen: _____

2. Integrität

Weitergabekontrolle

- ☐ Transportverschlüsselung (TLS, SFTP, SSH)
- ☐ gesicherter Datenaustausch, Plattform: _____
- ☐ Verpflichtung auf Vertraulichkeit
- ☐ weitere Maßnahmen: _____

Eingabekontrolle

- ☐ Protokollierung von Eingabe, Änderung und Löschung
- ☐ individuelle Benutzerkennungen
- ☐ revisionssichere Protokolle (GoBD)
- ☐ weitere Maßnahmen: _____

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle und Wiederherstellbarkeit

- ☐ redundante Rechenzentrumsinfrastruktur
- ☐ verschlüsselte Backups an getrenntem Standort

☐ regelmäßige Wiederherstellungstests
☐ Monitoring
☐ Notfallkonzept (z. B. BSI-Standard 200-4)
☐ weitere Maßnahmen: _____

4. Regelmäßige Überprüfung

Verfahren zur Überprüfung, Bewertung und Evaluierung

☐ Datenschutzbeauftragter: Name, Kontakt
☐ Informationssicherheitsbeauftragter: Name, Kontakt
☐ Datenschutz-Managementsystem / ISMS
☐ Zertifizierung: _____
☐ Schulungen zu Datenschutz und KI-Kompetenz (Art. 4 KI-VO)
☐ Auftragskontrolle gegenüber Subunternehmern
☐ weitere Maßnahmen: _____