Auftragsverarbeitungsvertrag nach Art. 28 DSGVO (Stand: 02/2026)

Zwischen

_____

Name

_____

Anschrift

_____

Folgend:
Auftraggeber

und

orderbird GmbH
Ritterstraße 12
10969 Berlin

Folgend:
Auftragnehmerin

Auftraggeber und Auftragnehmerin (nachfolgend zusammen auch „Parteien“) haben einen Vertrag über die Bereitstellung einer Software im Rahmen einer SaaS-Lösung geschlossen (nachfolgend „Hauptvertrag“). Soweit die Auftragnehmerin hierüber personenbezogene Daten Dritter verarbeitet, schließen die Parteien diesen Auftragsverarbeitungsvertrag, um die Pflichten der Parteien zum Datenschutz im Detail zu regeln.

1. Gegenstand der Vereinbarung

1.1. Die Auftragnehmerin verarbeitet Daten, die im Rahmen der Nutzung der Software vom Auftraggeber übermittelt werden. Im Wesentlichen umfasst der Auftrag des Auftraggebers daher die Datenverarbeitungsphase „Speicherung“ der Daten, die in verschiedenen Verfahren verarbeitet werden.

1.2. Die Vereinbarung kommt zustande, wenn sie durch den Auftraggeber unterschrieben wird und der Auftragnehmerin zugesendet wird.

1.3. Gesonderte Kosten für die Datenverarbeitung fallen nicht an und sind mit der Vergütung des Hauptvertrages abgegolten.

1.4. Als personenbezogene Daten im Rahmen der Erfüllung des Hauptvertrages werden Kunden- und Mitarbeiterdaten (beispielsweise Name, Firmenname, Kundennummer,

Adresse, Schichtwechsel) sowie Kommunikationsdaten (zum Beispiel E-Mail-Adresse, Telefonnummer), Username, Passwort sowie PIN des das Kassensystem bedienenden Mitarbeitenden, Vertragsabrechnungs- und Zahlungsdaten sowie im Falle der Nutzung des Reservierungssystems Daten zu Reservierungen (Datum/Uhrzeit der Reservierung, Gästeanzahl, Essenswünsche, Sitzplatzwünsche, Kommentare/Anmerkungen zur Reservierung) verarbeitet. Die von der Auftragnehmerin verarbeiteten Kartenzahlungsdaten betreffend Kunden des Auftraggebers sind auf die letzten vier Ziffern der Bankkarte, den gezahlten Betrag sowie ggf. das Gerät, mit dem bezahlt wurde, beschränkt. Die Auftragnehmerin hat keine Möglichkeit, vollständige Zahlungsdaten einzusehen.

1.5. Die betroffene Personenkategorie der durch die Verarbeitung Betroffenen umfasst Mitarbeiter und Kunden des Auftraggebers.

2. Bereitstellung von Daten durch den Auftraggeber

2.1. Der Auftraggeber stellt die Daten über die Softwareanwendung orderbird.POS, orderbird MINI sowie das Verwaltungs- und Buchhaltungsmodul „my.orderbird“ zur Verfügung.

3. Rechte und Pflichten des Auftraggebers

3.1. Der Auftraggeber ist im Rahmen dieses Vertrages für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen allein verantwortlich.

3.2. Er vereinbart dazu mit der Auftragnehmerin die diesem Vertrag als Anlage beigefügten technischen und organisatorischen Maßnahmen. Er trägt dafür Sorge, dass diese Maßnahmen für die zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

3.3. Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung in schriftlicher oder elektronischer Form zu erteilen. Die Weisungen werden zu Beginn der Zusammenarbeit durch den Hauptvertrag festgelegt. Der Auftraggeber kann im Rahmen der Beauftragung Einzelweisungen zum Schutz personenbezogener Daten erteilen und die Einhaltung der Vorschriften über den Datenschutz und der von ihm getroffenen Weisungen überprüfen. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

3.4. Der Auftraggeber nennt der Auftragnehmerin eine weisungsberechtigte Person.

3.5. Der Auftraggeber informiert die Auftragnehmerin unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

4. Pflichten der Auftragnehmerin

4.1. Die Auftragnehmerin verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, soweit gesetzliche Vorschriften nichts anderes bestimmen.

4.2. Die Auftragnehmerin informiert den Auftraggeber unverzüglich, wenn sie der Auffassung ist, dass eine Weisung gegen gesetzliche Vorschriften verstößt. Die Auftragnehmerin darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

4.3. Die Auftragnehmerin gestaltet ihre innerbetriebliche Organisation so, dass sie den gesetzlichen Vorgaben im Bereich Datenschutz gerecht wird.

4.4. Die Auftragnehmerin wird in ihrem Verantwortungsbereich für die Umsetzung und Einhaltung der vereinbarten und als Anlage diesem Vertrag beigefügten allgemeinen und technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers unter Berücksichtigung der gesetzlichen Vorgaben sorgen.

4.5. Eine einseitige Änderung der getroffenen Sicherheitsmaßnahmen bleibt der Auftragnehmerin vorbehalten, wobei sichergestellt wird, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

4.6. Die Auftragnehmerin unterstützt den Auftraggeber nach Aufforderung bei der Erfüllung datenschutzrechtlicher Pflichten, sofern gesetzliche Vorschriften eine derartige Unterstützung durch den Auftragnehmer vorschreiben.

4.7. Die Auftragnehmerin trägt Sorge dafür, dass es Mitarbeitern und anderen für die Auftragnehmerin tätigen Personen, die mit der Verarbeitung der Daten des Auftraggebers befasst sind, untersagt ist, die Daten weisungswidrig zu verarbeiten. Darüber hinaus werden Mitarbeiter und die für die Auftragnehmerin tätige Dritte zur Vertraulichkeit verpflichtet, sofern sie nicht einer vergleichbaren gesetzlichen

Verschwiegenheitspflicht unterliegen. Diese Regelungen sollen auch nach Beendigung des Auftrages gelten.

4.8. Die Auftragnehmerin unterrichtet den Auftraggeber umgehend über technische und organisatorische Unzulänglichkeiten der Datensicherung und bei jeglichem Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten. Sie trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

4.9. Die Auftragnehmerin hat personenbezogene Daten zu berichtigen, zu löschen und zu sperren, wenn der Auftraggeber dies in einer Weisung verlangt.

4.10. Nach Abschluss des Auftrags hat die Auftragnehmerin sämtliche in ihren Besitz gelangten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Hauptvertrag stehen, dem Auftraggeber auszuhändigen. Die Löschung bzw. Vernichtung ist dem Auftraggeber auf Verlangen in Textform zu bestätigen. Gesetzliche Aufbewahrungspflichten bleiben von dieser Vereinbarung unberührt.

5. Nachweismöglichkeiten

Die Auftragnehmerin stellt dem Auftraggeber auf Anfrage die zur Prüfung der Einhaltung der in diesem Vertrag und in Art. 28 DSGVO niedergelegten Pflichten erforderlichen Informationen zur Verfügung und ermöglicht im erforderlichen Umfang Kontrollen (z.B. durch Vorlage von Dokumentationen, Zertifizierungen, Berichten oder Selbstauskünften).

6. Subunternehmer

6.1. Der Einsatz von Subunternehmern zur Erfüllung der vertraglichen Pflichten der Auftragnehmerin ist zulässig und erfordert die vorherige Information des Auftraggebers. Eine Liste der eingesetzten Subunternehmer ist als **Anlage 2** zu dieser Vereinbarung beigefügt.

6.2. Die Auftragnehmerin wird mit diesen Subunternehmern im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten. Das heißt, dass diesen weiteren Subunternehmern im Wege eines Vertrags oder eines anderen Rechtsinstruments nach

dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats mindestens dieselben Datenschutzpflichten aufzuerlegen sind, die in dem Vertrag zwischen dem Auftraggeber und der Auftragnehmerin festgelegt worden sind.

6.3. Sofern der Subunternehmer seine Leistungen außerhalb der EU / des EWR erbringt, stellt die Auftragnehmerin die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Hierbei stützt sich die Auftragnehmerin auf Angemessenheitsbeschlüsse gem. Art. 45 DSGVO sowie Standarddatenschutzklauseln (EU-SCC).

7. Vertragsdauer

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrages.

8. Haftung und Schadensersatz

8.1. Eine zwischen den Parteien im zugrundeliegenden Hauptvertrag vereinbarte Haftungsregelung gilt auch für diesen Auftragsverarbeitungsvertrag.

9. Schriftformklausel, Rechtswahl

9.1. Änderungen und Ergänzungen zu dieser Vereinbarung und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung, die auch in elektronischer Form erfolgen kann.

9.2. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Hauptvertrages vor.

9.3. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

Ort, Datum	Unterschrift Auftraggeber (gesetzlicher Vertreter)

Anlage 1: Technische und organisatorische Maßnahmen

Anlage 2: Liste der eingesetzten Subunternehmer

Anlage 1 - technische und organisatorische Maßnahmen

Stand: September 2025

Organisationen, die personenbezogene Daten selbst oder im Auftrag verarbeiten, nutzen oder erheben, haben die technischen und organisatorischen Maßnahmen zu veranlassen, die einen datenschutzrechtskonformen Verarbeitungsvorgang ermöglichen. Erforderlich sind Maßnahmen nur dann, wenn bei einer Abwägung mit den Schutzinteressen die Angemessenheit gewahrt ist.

orderbird erfüllt diesen Anspruch durch folgende Maßnahmen, wobei wir zwischen eigenen Maßnahmen und den Maßnahmen in den von uns genutzten Rechenzentren, die von Auftragsverarbeitern betrieben werden, unterscheiden.

I. Eigene Maßnahmen

Nachstehende Maßnahmen treffen wir, soweit wir die Verarbeitungstätigkeit nicht durch Auftragsverarbeiter erbringen:

1. Vertraulichkeit, Integrität, Verfügbarkeit (Art. 32 Abs. 2 b) DSGVO

1.1. Zutrittskontrolle

Nr.	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Chipkarten-/ Transpondersystem	Schriftlich niedergelegte und unmissverständliche Schlüsselverwaltung mit klarer Verantwortlichkeit namentlich benannter Mitarbeiter
2.	Sichere Schlüsselaufbewahrung / Schlüsseltresor	Regelmäßige Überprüfung von vergebenen Zutrittsrechten
3.	Sicherheitsschlösser	Empfang/ Besucher werden durch Mitarbeiter begleitet
4.		Auswahl und Überwachung von Wach- und Reinigungsdiensten unter Datenschutzgesichtspunkten

1.2. Zugangskontrolle

Nr.	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Verschlüsselung von Notebooks / Laptops	Passwortrichtlinie inkl. erhöhter Anforderungen an Länge, Komplexität und Wechsel
2.	Authentifizierung mit personifizierten Zugangsdaten	
3.	Automatische und kennwort-geschützte PC-Bildschirmsperre	
4.	Automatische Sperrung bei fehl-geschlagenen Anmeldeversuchen	
5.	Einsatz von Firewalls zum Schutz der IT-Systeme	
6.	Einsatz von VPN bei Remote-Zugriffen auf IT-Systeme	
7.	Datenlösch-System zum Löschen mittels Festplattendienstprogramm (Mac OS) oder DBAN (Server)	
8.	Protokollierung von Zugriffen auf Anwendungen und IT-Systeme	
9.	Sicherstellung der Festplattenverschlüsselung	
10.	Erzwingen des Bildschirmschoner-Logins	
11.	Möglichkeit der Fernlöschung durch Mobile-Device-Management (MDM)	
12.	Vergeben von Firmware-Kennwörtern (EFI-Passwörtern)	

1.3. Zugriffskontrolle

Nr.	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Protokollierung von Zugriffen auf Anwendungen und IT-Systeme	Gruppierung der Zugriffsbefugnisse nach Aufgaben- und Zuständigkeitsgebiet
2.	Protokollierung von fehlgeschlagenen Zugriffsversuchen auf IT-Systeme	Berechtigungskonzept für Zugänge zu IT-Systemen
3.	Geregelte und technisch zuverlässige Vernichtung von Daten durch Einsatz einer „Datentonne“	Passwortrichtlinie und geschützte Passwortvergabe
4.	Automatische Sperrung bei fehl-geschlagenen Anmeldeversuchen	Verwaltung der Benutzerrechte durch geschulte Systemadministratoren
5.	Einsatz von Firewalls zum Schutz der IT-Systeme	Rechtevergabe durch geschultes Personal
6.	Einsatz von VPN bei Remote-Zugriffen auf IT-Systeme	Berechtigungskonzept mit Minimalprinzip

1.4. Trennungskontrolle

Nr	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Dauerhafte Zuordnung von Verarbeitungs-geräten an individuelle Anwender	Verschiedene Arbeitsplätze für unterschiedliche Verarbeitungsvorgänge und Datenkategorien
2.	Mandantenfähige Systeme zur Funktionstrennung	Steuerung über Berechtigungskonzept
3.	Segmentierung von Netzwerken nach Schutzbedürftigkeit	Kundenvertragsdaten werden in separatemCMS mit eigenem Zugangsberechtigungssystem gespeichert
4.	Separierung von Entwicklungs- und Testumgebungen und Produktivsysteme	Es werden Testdaten generiert, in der Entwicklung, um nicht auf Live-Daten zurückgreifen zu müssen
5.		Festlegung von Datenbankrechten

1.5. Weitergabekontrolle

Nr.	Technische Maßnahmen	Organisatorische Maßnahmen
1.	E-Mail-Verschlüsselung bei sensiblen Daten (z.B. in der Kommunikation mit dem Lohnbüro)	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung und der Löschfristen
2.	Einsatz von VPN	Weitergabe in geeigneten Fällen in pseudonymisierter oder anonymisierter Form
3.	Bereitstellung von Informationen über verschlüsselte Verbindungen wie https, sftp	
4.	Nutzung von Signaturverfahren	

2. Verfügbarkeits- und Belastbarkeitskontrolle (Art. 32 c) DSGVO

Nr.	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Verwendung redundant vorgehaltener Systeme	Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
2.	Feuerlöscher in Büros und Infrastruktur-räumen vorhanden	Monitoring aller relevanten Infrastruktur und IT-Systeme
3.	Einsatz von Datenspiegelung (RAID) für relevante IT-Systeme	Backup- und Recovery-Konzept (ausformuliert)
4.		Kontrolle des Sicherungsvorgangs
5.		Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse

3. Incident Response Management

Nr.	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Einsatz von Firewall und deren regelmäßige Aktualisierung	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/ Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde), „Incident Response Richtlinie“
2.	Einsatz von VPN	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
3.	Bereitstellung von Informationen über verschlüsselte Verbindungen wie https, sftp	Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen, Prozess der konstanten Verbesserung
4.	Nutzung von Signaturverfahren	Formaler Prozess zur nachträglichen Aufarbeitung von Sicherheitsvorfällen
5.		Dokumentation von Sicherheitsvorfällen in Ticketsystem

4. Auftragskontrolle (Outsourcing an Dritte)

Nr.	Technische Maßnahmen	Organisatorische Maßnahmen
1.	E-Mail-Verschlüsselung bei sensiblen Daten (z.B. in der Kommunikation mit dem Lohnbüro)	Prüfung der vom der Auftragnehmerin getroffenen Sicherheitsmaßnahmen und deren Dokumentation
2.	Einsatz von VPN	Formaler Prozess zur Prüfung und dem Abschluss von Auftragsverarbeitungsvereinbarungen oder EU-Standardvertragsklauseln
3.	Bereitstellung von Informationen über verschlüsselte Verbindungen wie https, sftp	Schriftliche Weisungen an die Auftragnehmerin
4.	Nutzung von Signaturverfahren	Verpflichtung der Mitarbeiter der Auftragnehmerin auf das Datengeheimnis wird sichergestellt
5.		Vertragliche Sicherstellung der Vernichtung von Daten bei Auftragsbeendigung
6.		Prozess zur laufenden Überprüfung von Auftragsverarbeitern

5. Datenschutz-Management (Art. 32 d) DSGVO

Nr.	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Dokumentation der Abläufe elektronisch abrufbar	Regelmäßige Sensibilisierung der Mitarbeiter für Datenschutzfragen
2.	Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Etablierter Datenvernichtungs-/ Datenlösch-Prozess
3.	Manuelle und automatisierte Kontrolle von hier-für softwareseitig erstellten Protokolldateien	Regelmäßige Überprüfung von Richtlinien auf Aktualität und Wirksamkeit
4.	Zentrale Dokumentation der daten-schutzrelevanten Verfahrensweisen und Arbeitsanweisungen; Zugriffsmöglichkeit für die betroffenen Mitarbeiter nach Relevanz	Etablierter Rückbauprozess bei Produktkündigungen

5.	Sicherstellung des Datensparsamkeits-prinzips auf technischer Ebene: es werden in Abfrageprozessen nur jeweils erforderliche Daten zur Eingabe durch Mitarbeiter abgefragt	On- und Offboarding-Richtlinien für neue und ausscheidende Mitarbeiter
6.		Zentralisierte Überwachung der Einhaltung des adäquaten Datenschutzniveaus von Auftragsverarbeitern
7.		Externe Beratung durch spezialisierte Anwaltskanzlei
8.		Arbeitsrechtlich verbindliche Richtlinie „mobiles Arbeiten“ mit besonderen Vorkehrungen gegen den Verlust von Daten und die unbefugte Kenntnisnahme durch Dritte
9.		Benutzungsrichtlinie Arbeitsmittel/Datenträger
10.		Externer Datenschutzbeauftragter
11.		Aufbewahrung von Formularen, aus denen Daten in automatisierte Verarbeitungen übernommen wurden
12.		Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet

II. Maßnahmen unserer Auftragsverarbeiter

Amazon Web Services EMEA SARL
38 avenue John F. Kennedy,
L-1855 Luxembourg

Cloudflare Inc.
101 Townsend St.
San Francisco, CA94107, USA

Wir bedienen uns für die Durchführung unseres Kerngeschäfts, der Dienstleistungen von branchenführenden Cloud-Anbietern. Dabei handelt es sich im Zeitpunkt des Abschlusses

dieses Vertrags um nachfolgende Unternehmen, wobei beide Unternehmen auf Grundlage von EU-Standard-Vertragsklauseln beauftragt wurden:

Cloudflare sichert gemäß § 6 der Cloudflare-AVV zu, dass Daten, die außerhalb der EEA (European Economic Area) verarbeitet werden sollten, diese gemäß den in der EU geltenden Bedingungen verarbeitet werden.

Amazon Web Services bietet seinen Kunden die Möglichkeit der Wahl, in welcher Region die Daten gespeichert werden. Wir haben eine Speicherung der Daten ausschließlich in der EU gewählt.

Nachstehende technisch-organisatorischen Maßnahmen treffen unsere im Rahmen der Auftragsverarbeitung hinzugezogenen Unterauftragnehmer. Wo Maßnahmen nicht einheitlich bestehen, wird das durch ein Kürzel zur Bezeichnung des betroffenen Unterauftragnehmers (A = Amazon Web Services Inc., C = Cloudflare Inc.) kenntlich gemacht:

1. Vertraulichkeit, Integrität, Verfügbarkeit (Art. 32 Abs. 2 b) DSGVO

1.1. Zutrittskontrolle

Nr.	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Zutrittskontrollsystem	Personelle Eingangskontrolle zum Unternehmensgelände und den Rechenzentren[A]
2.	Zweistufige Authentifizierung mit personifizierten Zugangsdaten[A]	Vergabesystem für Zutrittskarten für Mitarbeiter und speziell Berechtigte
3.	Schließsystem mit Sicherheitsschlössern	Mindestens zweimalige Authentifizierung vor Zutrittsgewährung zu Rechenzentren erforderlich[A]
4.	Videoüberwachung der Ein- und Ausgänge[A], Einbruchmeldeanlage	Zutrittsrechtevergabe für Mitarbeiter und externe Mitarbeiter nach festgelegten Kriterien
5.		Vergabe und Dokumentation der Berechtigungen über Zutrittsrechtemanagement
6.		Identitätserfassung für Besucher und externe Mitarbeiter[A]
7.		Begleitung von Besucher und externe Mitarbeiter nur durch berechtigte Mitarbeiter[A]
8.		Dokumentation und Auditierung der erfolgten Zutritte[A]

1.2. Zugangskontrolle

Nr.	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Einsatz von Firewalls zum Schutz der IT-Systeme	Berechtigungskonzept für Zugänge zu Datenverarbeitungssystemen, Vergabe der Berechtigungen nach festgelegten Kriterien
2.	Einsatz von VPN bei Remote-Zugriffen auf IT-Systeme	Passwortrichtlinie und geschützte Passwortvergabe

3.	Protokollierung von Zugriffen auf Server, Netzwerke, Ports	Automatische temporäre Sperrung des User-Terminals bei Nichtnutzung, Identifikation und Passworteingabe zum erneuten Öffnen erforderlich[C]
4.	Einsatz von Verschlüsselungsverfahren	Automatische temporäre Sperrung der Benutzerberechtigung bei Eingabe mehrerer fehlerhafter Passwörter, Protokollierung der Passworteingabe[C]
5.	Remote-Zugriff auf interne IT-Systeme nur nach Authentifikation, Einsatz von VPNA	
6.		Alarmierung zuständiger Mitarbeiter bei auffälligen Zugriffen[A], Einsatz von Pagern zur Alarmierung[A], Ununterbrochene Verfügbarkeit zuständiger Mitarbeiter[A], wöchentliche Besprechungen zur Implementierung von Präventivmaßnahmen[A]
7.		Entsorgung ausgedienter Datenträger nach festgelegten Vorgaben[A]

1.3. Zugriffskontrolle

Nr.	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Protokollierung von Zugriffen auf Anwendungen und IT-Systeme	Konzept für Zugriffsbefugnisse nach Aufgaben- und Zuständigkeitsgebiet
2.	Protokollierung auffälliger Zugriffsversuche auf informationsverarbeitende Systeme, Mitteilung an zuständige Mitarbeiter[A]	Vorhalten eines Incident Management Team[A]
3.	Optional: Zugriff nur nach Multi-Faktor Authentifizierung[A]	Mitarbeiterrichtlinien und individuelle Schulungen in Bezug auf die Zugriffsrechte[C]
4.	FIPS 140-2-konforme SSL-Load Balancer[A]	Möglichkeit der Protokollierung von Personen, die personenbezogene Daten löschen, hinzufügen oder ändern[C]
5.	Implementierung von Netzwerkgeräten zur Verwaltung der Schnittstellenkommunikation mit Internet Service Providern (ISPs)[A]	
6.	Redundante Verbindung zu mehrerer Kommunkationsdiensten des Netzwerkes[A]	

7.	Einsatz von Verschlüsselungstechnolo gien (Security Socket Layers (SSL)[A])	

1.4. Trennungskontrolle

Nr	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Trennung von operativem und Unternehmensnetzwerk[A], Getrennte Datenspeicherung auf Datenbankebene nach Modul, Kunde oder unterstützte Funktion[C]	Zugriffvergabe auf verschiedene Netzwerke über Ticketing-System[A] und Berechtigungskonzept
2.	Zugriff auf operatives Netzwerk nur mit SSH-Public-Key-Authentifizierung[A]	Automatische Beendigung der Berechtigung nach 90 Tagen oder mit Ausscheiden des Mitarbeiters aus dem Unternehmen[A]
3.	Einschränkung von Schnittstellen, Batch-Prozessen und Reports für bestimmte Zwecke und Funktionen[C]	

1.5. Weitergabekontrolle

Nr	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Zugriffsschutz auf Systeme auf Betriebs- und Unternehmensebene[A]	Freigabe von Daten nur an berechtigte Personen, einschließlich der Vergabe differenzierter Zugriffsrechte und Rollen[C]
2.	Einsatz von Firewall, VPN- und Verschlüsselungstechnologien zum Schutz der Gateways uns Pipelines über die Daten übertragen werden	Kontrollierte und dokumentierte Löschung der Daten[C]
3.	Verschlüsselung bestimmter Mitarbeiterdaten (z.B. persönlich identifizierbare Informationen wie nationale ID-Nummern, Kredit- oder Debitkartennummern) innerhalb des Netzwerkes[C]	Benachrichtigung des Anwenders bei unvollständiger Datenübertragung (End-to-End-Check)[C]
5.		Protokollierung der Datenübertragung (soweit möglich)[C]

2. Verfügbarkeits- und Belastbarkeitskontrolle (Art. 32 Abs. 1 DSGVO)

Nr.	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Unterbrechungsfreie redundante Stromversorgung der Rechenzentren ohne Auswirkungen auf laufende Prozesse[A], System zur unterbrechungsfreien Stromversorgung (UPS) bei einem elektrischen Ausfall für kritische und wesentliche Lasten in der Anlage[A], Generatoren für die Rechenzentren können die gesamte Anlage mit Strom versorgen[A]	Überwachung und regelmäßige Wartung der elektrischen, mechanischen und lebenserhaltenden Systeme und Geräte zur sofortigen Fehlererkennung[A]
2.	Redundante Netzwerkinfrastruktur[C]	Getrennte Backup-Sicherung[C]
3.	Automatische Brandmeldeanlage mit Rauchmeldern und Löschausrüstung in Rechenzentrumsumgebungen, mechanischen und elektrischen Infrastrukturräumen, Kühlräumen und Generatorausrüsungsräumen[A], Schutz durch durch Nassrohr-, Doppel-verriegelungs- oder Gas-Sprinkleranlagen[A]	Personelle Überwachung von Temperatur und Feuchtigkeit im Rechenzentrum[A]
4.	Klimatisierung der Rechenzentren[A]	Clusterförmige Verteilung der Rechenzentrum weltweit[A] Ausschluss „kalter“ Rechenzentren, alle sind aktiv[A]
5.	System zur Überwachung von Temperatur und Feuchtigkeit in Rechenzentren[A]	Automatisiertes System zur Verlagerung des Kundendatenverkehrs bei Störungen aus dem betroffenen Bereich[A]
6.	N+1-Konfiguration, die gewährleistet, dass im Falle eines Ausfalls eines Rechenzentrums genügend Kapazität zur Verfügung steht, um den Datenverkehr auf die verbleibenden Standorte zu verlagern[A]	Vorhaltung mehrerer geografischer Verfügbarkeitszonen für die Datensicherung, Speisung der Zonen über verschiedene Netze unabhängiger Versorgungsunternehmen[A]
7.	Redundante Verbindung der Verfügbarkeitszonen mit mehreren Tier-1-Transit- anbietern[A]	Räumliche Trennung von Verfügbarkeitszonen in typischen Metropolregionen und Einrichtung von Verfügbarkeitszonen in Überschwemmungs-gebieten mit geringerem Risiko[A]
8.	Vorhaltung von Systemen zur Erzeugung von Backups in den Datenzentren[A]	Möglichkeit der Datenspeicherung in unterschiedlichen Verfügbarkeitszonen[A]

9.		Regelmäßige konzerninterne Überprüfung der Verfügbar- und Belastbarkeit der Systeme
10.		Durchführen von Sicherheitsaudits und Penetrationstests[A]
11.		Routine-, Notfall- und Konfigurationsänderungen an der bestehenden Infrastruktur werden gemäß den Industrienormen für ähnliche Systeme autorisiert, protokolliert, getestet, genehmigt und dokumentiert[A]
12.		Vorgaben hinsichtlich der Information von Kunden im Fall einer erforderlichen Änderung[A]

3. Incident Response Management

Nr.	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Einsatz von Firewall und deren regelmäßige Aktualisierung[A]	Incident Management Team[A]
2.	Einsatz von VPN[A]	Einsatz branchenüblicher Diagnoseverfahren[A]
3.	Bereitstellung von Informationen über verschlüsselte Verbindungen[A]	Rund-um-die-Uhr Erreichbarkeit des Incident Management Teams[A]
4.	Nutzung von Signaturverfahren (optional)[A]	Formaler Prozess zur nachträglichen Aufarbeitung von Sicherheitsvorfällen[A]
5.		Dokumentation von Sicherheitsvorfällen in Ticketsystem[A]

4. Eingabekontrolle

Nr.	Technische Maßnahmen	Organisatorische Maßnahmen
1.		Berechtigungsrichtlinie für das Eingeben, Lesen, Ändern und Löschen von Daten[C]
2.		Eingaberechtemanagement[C]

3.		Passwortrichtlinie[C]
4.		Authentifizierungserfordernis des autorisierten Personals[C]
5.		Schutzmaßnahmen für die Dateneingabe in den Speicher sowie für das Lesen, Ändern und Löschen von gespeicherten Daten[C]
		Protokollierung von vorgenommenen Einträgen[C]

5. Datenschutz-Management (Art. 32 d) DGVO

Nr.	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Dokumentation der Abläufe elektronisch abrufbar[A]	
2.	Technische Protokollierung der Eingabe, Änderung und Löschung von Daten[A]	
3.	Manuelle und automatisierte Kontrolle von hierfür softwareseitig erstellten Protokolldateien[A]	

Anlage 2 - Liste der eingesetzten Subunternehmen

Nr.	Produkt	Name und Anschrift des Subunternehmens	Zweck des Einsatzes	Drittland-übermittlung (ja/nein) und ggf. Rechtsgrundlage
1.	orderbird PRO orderbird MINI	Aircall SAS 11-15 Rue Saint-Georges 75009, Paris, France	Support/Telefonsystem	nein
2.	orderbird PRO orderbird MINI	Amazon Web Services EMA SARL, 38 avenue John F. Kennedy L-1855 Luxembourg	Datenspeicherung (Cloudservice)	nein
3.	orderbird PRO orderbird MINI	Atlassian. Pty Ltd Level 6, 341 George Street Sydney NSW 2000, Australia	internes Ticket-management	Nutzung der „Data Residency“-Funktion (Dublin, Frankfurt/Main); zusätzlich EU SCCs
4.	orderbird PRO orderbird MINI	Bambora AB, Box 17026, 10462 Stockholm, Sweden	Zahlungs-abwicklung	nein
5.	orderbird PRO orderbird MINI	Calendly LLC 88 North Avondale Road Suite 603 Avondale Estates, GA 30002, USA	Terminplanungs-plattform	EU-U.S. DPF

6.	orderbird PRO orderbird MINI	Campaign Monitor Holdings Pty Ltd 5 STAPLETON AVE SUTHERLAND NSW C3 2232, Australia	Newsletter-versand	gem. Art. 49 Abs. 1 lit. a DSGVO
7.	orderbird PRO orderbird MINI	Cloudflare Inc. 101 Townsend St. San Francisco, CA9407 USA	Datenspeicherung (Cloudservice)	EU-U.S. DPF
8.	orderbird PRO orderbird MINI	Nexi Germany GmbH Helfmann-Park 7 65760 Eschborn, Deutschland	Abwicklung Kreditkarten-transaktionen	nein
9.	orderbird PRO orderbird MINI	Forethought Technologies, Inc., 2 Embarcadero Center, Floor 8, San Francisco, CA 94111, USA	Support/ Chatfunktion	gem. Art. 49 Abs. 1 lit. a DSGVO
10.	orderbird PRO orderbird MINI	CyberSource Limited, Kennet Wharf, 41-45 Queens Road, Reading, Berkshire, RG1 4BQ, United Kingdom	Bereitstellung der Plattform für die Abwicklung von Transaktionen	Art. 45 DSGVO Angemessenheits beschluss vom 28.06.2021
11.	orderbird PRO orderbird MINI	Datadog, Inc., 620 8th Avenue, Floor 45,	Monitoring der Transaktions-sicherheit	EU-U.S. DPF

		New York, NY 10018, USA		
12.	orderbird PRO orderbird MINI	devguard GmbH Im Lindenhof 24 10365 Berlin, Deutschland	Geräte-Management	nein
13.	orderbird PRO	fiskaltrust Österreich GmbH Alpenstraße 99 5020 Salzburg, Österreich	Fiskalisierung Österreich/ Manipulations-schutz	nein
14.	orderbird PRO orderbird MINI	fiskaly Germany GmbH Zeilweg 42 60439 Frankfurt am Main, Deutschland	Fiskalisierung Deutschland/ Cloud TSE	nein
15.	orderbird PRO orderbird MINI	Google LLC 1600 Amphitheatre Parkway Mountain View, California 94043, USA	Kommunikation/ Emails	EU-U.S. DPF
16.	orderbird PRO orderbird MINI	Hans WiNN GmbH & Co. KG Kirschäckerstr. 24 96052 Bamberg, Deutschland	Hardwareversand	nein

17.	orderbird PRO orderbird MINI	Helpjuice Inc, 1010 NE, 2nd Ave Miami, FL33132, USA	Knowledge-Base/ Supportcenter	Art. 46 DSGVO – EU-SCC im DPA
18.	orderbird PRO orderbird MINI	Metabase Inc, 660 4th Street #557, San Francisco, CA 94107, USA	Datenauswertung	Art. 46 DSGVO – EU-SCC im DPA
19.	orderbird PRO orderbird MINI	OpenAI, LLC 3180 18th St. San Francisco, CA 94110, USA	Textoptimierung	Art. 46 DSGVO – SCC im DPA
20.	orderbird PRO orderbird MINI	Parloa GmbH, Münzstr. 5, 10178 Berlin, Deutschland	Support/ Telefondialog	nein
21.	orderbird PRO orderbird MINI	RealtimeBoard Inc. dba Miro, 201 Spear Street, Suite 1100, San Francisco, CA 94105, USA	internes Analysetool	EU-U.S. DPF
22.	orderbird PRO	resmio GmbH*, Katzwanger Straße 150 90461 Nürnberg, Deutschland	Bereitstellung Reservierungs- system	nein
23.	orderbird PRO orderbird MINI	Salesforce.com Germany GmbH, Erika-Mann-Str.	Vertrags- management	nein

		31-37 80636 München, Deutschland		
24.	orderbird PRO	SendPulse Inc.*** 220 E 23rd St #401 New York, NY 10010	CRM Kommunikations-tool/ E-Mail	Art. 46 DSGVO – EU-SCC
25.	orderbird PRO	Functional Software, Inc.,*** 45 Fremont Street, 8th Floor, San Francisco, CA 94105.	internes Applikations Monitoring	Art. 46 DSGVO – EU-SCC
26.	orderbird PRO orderbird MINI	Slack Technologies Limited 500 Howard Street, San Francisco, CA 94150, USA	interne Kommunikation	Art. 46 DSGVO – EU-SCC
27.	orderbird PRO	Stripe Payments Europe Ltd.** 1 Grand Canal Street Lower, Grand Canal Dock Dublin, Ireland	Zahlungs-abwicklung	nein
28.	orderbird PRO orderbird MINI	SupportYourApp Limited 9TH FLOOR, AMTEL BUILDING, 148 DES VOEUX ROAD CENTRAL,	Support-dienstleister	EU-U.S. DPF

		CENTRAL HONG KONG		
29.	orderbird PRO	VONAGE BUSINESS LIMITED*** 101 Crawfords Corner Road, Suite 2416 Holmdel, United States, NJ 07733	CRM Kommunikations-tool/ SMS	Art. 46 DSGVO – EU-SCC
30.	orderbird PRO orderbird MINI	Zapier, Inc. 548 Market St. #62411 San Francisco, CA 94104-5401, USA	interne Prozess-optimierung	EU-U.S. DPF

* nur bei Nutzung des Reservierungssystems

**nur bei Nutzung der Zahlungsoption im Bestellmanagement

***nur bei Nutzung des Bestellmanagements