www.orderbird.com
hello@orderbird.com
+49 30 208983099

orderbird AG
Ritterstraße 12-14
10969 Berlin
Deutschland

Auftragsverarbeitungsvereinbarung

Zwischen

_____

Name

_____

Anschrift

Folgend:

Auftraggeber

Und

orderbird AG
Ritterstraße 12 - 14
10969 Berlin

Folgend:

Auftragnehmerin oder orderbird

Präambel

Mit Vertrag vom _____ (im Folgenden „Hauptvertrag“) haben die Parteien unter anderem eine Pflicht zur Auftragsverarbeitung von Daten begründet. Durch die hier gegenständliche Auftragsverarbeitungsvereinbarung sollen die Pflichten der Parteien zum Datenschutz im Detail geregelt werden.

Die Parteien sind sich einig, dass diese Vereinbarung für alle Tätigkeiten, die im Zusammenhang mit der Verarbeitung personenbezogener Daten gemäß dem zwischen den Parteien geschlossenen Vertrages anfallen und die dabei durch Beschäftigte oder Beauftragte der Auftragnehmerin durchgeführt werden, gilt.

1. Gegenstand der Vereinbarung

1.1. Die Auftragnehmerin verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst die im Rahmen der Nutzung der Software der Auftragnehmerin erfassten Daten, die sich im Bestand des Auftraggebers befinden.

1.2. Der Auftrag wird unentgeltlich erteilt.

1.3. Im Wesentlichen umfasst der Auftrag des Auftraggebers die Datenverarbeitungsphase „Speicherung“ der Daten, die in verschiedenen Verfahren verarbeitet werden.

1.4. Als personenbezogene Daten werden Kunden- und Mitarbeiterdaten (beispielsweise Name, Firmenname, Kundennummer, Adresse) sowie Kommunikationsdaten (zum Beispiel E-Mailadresse, Telefonnummer) und Vertragsabrechnungs- und Zahlungsdaten verarbeitet.

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

2. Bereitstellung von Daten durch den Auftraggeber

2.1. Der Auftraggeber stellt die Daten über die Clientanwendung orderbird.POS und das Verwaltungs- und Buchhaltungsmodul „my.orderbird“ zur Verfügung. Er stellt sicher, dass die Zugangsdaten zur Datenbank sicher aufbewahrt und nicht an Dritte weitergegeben werden. Der Zugriff ist dabei nur auf die vertragsgegenständlichen Daten möglich. Nach Vertragsende wird die Auftragnehmerin die Zugangsdaten vernichten.

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 für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten, insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt sind.

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 Vertrag 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.

3.6. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der Auftragnehmerin vertraulich zu behandeln.

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. Der Auftragnehmerin darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

4.3. Die Auftragnehmerin verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, als die vorgenannten Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

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

4.5. 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. Hierzu gehört auch der Einsatz eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung entsprechend der gesetzlichen Vorgaben.

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

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

4.8. 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.

4.9. 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.

4.10. Die Auftragnehmerin hat personenbezogene Daten zu berichtigen, löschen und zu sperren, wenn der Auftraggeber dies in einer Weisung verlangt. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt die Auftragnehmerin die datenschutzkonforme Vernichtung der betroffenen Datenträger und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung; Vergütung und Schutzmaßnahmen sind dann gesondert zu vereinbaren.

4.11. Nach Abschluss des Auftrags hat die Auftragnehmerin sämtliche in ihren Besitz gelangten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger der Auftragnehmerin sind danach physisch zu löschen. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich zu bestätigen. Gesetzliche Aufbewahrungspflichten bleiben von dieser Vereinbarung unberührt.

5. Nachweismöglichkeiten

5.1. Der Auftraggeber hat das Recht nach Absprache mit der Auftragnehmerin Überprüfungen selbst oder durch einen von ihm beauftragten Prüfer durchzuführen und sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch die Auftragnehmerin in ihrem Geschäftsbetrieb zu überzeugen.

5.2. Die Auftragnehmerin weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten durch die Durchführung von Selbstaudits nach. Diese verwahrt sie für den Auftraggeber und übermittelt sie auf Verlangen an einen vom Auftraggeber benannten Ansprechpartner.

6. Subunternehmer

6.1. Der Einsatz von Subunternehmern zur Erfüllung der vertraglichen Pflichten der Auftragnehmerin ist zulässig und erfordert die vorherige Information des Auftraggebers.

6.2. Die Auftragnehmerin wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

6.3. Sofern der Subunternehmer seine Leistungen außerhalb der EU / des EWR erbringt, stellt die Auftragnehmerin die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

7. Informationspflichten

7.1. Sollte der Schutz personenbezogener Daten durch Maßnahmen Dritter, etwa durch Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, hat die Auftragnehmerin den Auftraggeber unverzüglich zu verständigen. Das Eigentum des Auftraggebers (zum Beispiel Datenträger, Arbeitskopien, Behältnisse) ist rechtzeitig zu kennzeichnen.

8. Vertragsdauer

8.1. Die Laufzeit dieser Vereinbarung beginnt mit Vertragsabschluss und endet mit Beendigung des zwischen den Parteien abgeschlossenen Vertrages, der die Grundlage bildet.

9. Haftung und Schadensersatz

9.1. Eine zwischen den Parteien im zugrundeliegenden Vertrag vereinbarte Haftungsregelung gilt auch für diese Auftragsverarbeitungsvereinbarung, es sei denn es wurde ausdrücklich etwas anderes vereinbart.

10. Kündigung

10.1. Bei schwerwiegenden oder wiederholten Verstößen gegen diese Vereinbarung steht den Parteien ein wechselseitiges außerordentliches Kündigungsrecht zu.

11. Schriftformklausel, Rechtswahl

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

11.2. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Kundenvertrages vor.

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

Unterschriften

_____, den _____	Berlin _____, den 03.03.2022
(Ort und Datum)	(Ort und Datum)
	Mark Schoen
_____	_____
für den Auftraggeber	für die Auftragnehmerin

Anlage: Technische und organisatorische Maßnahmen

Technische und organisatorische Maßnahmen

Stand: 10. Mai 2021

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

Die orderbird AG 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 klarerVerantwortlichkeit 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 Daten-schutzgesichtspunkten

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 kennwortgeschützte PC-Bildschirmsperre	
4.	Automatische Sperrung bei fehlgeschlagenen 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 Einsatzeiner „Datentonne“	Passwortrichtlinie und geschützte Pass-wortvergabe
4.	Automatische Sperrung bei fehlgeschlagenen Anmeldeversuchen	Verwaltung der Benutzerrechte durch ge-schulte 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 Verarbeitungsgeräten an individuelle Anwender	Verschiedene Arbeitsplätze für unter- schiedliche Verarbeitungsvorgänge undDatenkategorien
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 zurück-greifen 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 sowieder 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 vorgehaltenerSysteme	Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
2.	Feuerlöscher in Büros und Infrastrukturräumen vorhanden	Monitoring aller relevanten Infrastruktur undIT-Systeme
3.	Einsatz von Datenspiegelung (RAID) für relevante IT-Systeme	Backup- und Recovery-Konzept (ausformuliert)
4.		Kontrolle des Sicherungsvorgangs
5.		Regelmäßige Tests zur Datenwiederherstel-lung 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 undMeldung von Sicherheitsvorfällen/ Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde), „Incident Response Richtlinie“
2.	Einsatz von VPN	Dokumentierte Vorgehensweise zum Um-gang 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 sensiblenDaten (z.B. in der Kommunikation mit dem Lohnbüro)	Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und derenDokumentation
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 Auftragnehmer
4.	Nutzung von Signaturverfahren	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis wird sichergestellt
5.		Vertragliche Sicherstellung der Vernichtung von Daten bei Auftragsbeendigung
6.		Prozess zur laufenden Überprüfung vonAuftragsverarbeitern

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

Nr	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Dokumentation der Abläufe elektronisch abrufbar	Regelmäßige Sensibilisierung der Mitarbeiterfür Datenschutzfragen
2.	Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Etablierter Datenvernichtungs-/Daten-lösch-Prozess
3.	Manuelle und automatisierte Kontrolle von hierfür softwareseitig erstellten Protokolldateien	Regelmäßige Überprüfung von Richtlinienauf Aktualität und Wirksamkeit
4.	Zentrale Dokumentation der datenschutz-relevanten Verfahrensweisen und Arbeits-anweisungen; Zugriffmöglichkeit für die betroffenen Mitarbeiter nach Relevanz	Etablierter Rückbauprozess bei Produktkün digungen
5.	Sicherstellung des Datensparsamkeitsprinzip auf technischer Ebene: es werden in Abfrageprozessen nur jeweils erforderliche Daten zur Eingabe durch Mitarbeiterabgefragt	On- und Offboarding-Richtlinien für neue und ausscheidende Mitarbeiter
6.		Zentralisierte Überwachung der Einhaltungdes 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 dieunbefugte Kenntnisnahme durch Dritte
9.		Benutzungsrichtlinie Arbeitsmittel/Datenträger
10.		Externer Datenschutzbeauftragter
11.		Aufbewahrung von Formularen, aus denenDaten in automatisierte Verarbeitungen übernommen wurden
12.		Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet

II. Maßnahmen unserer Auftragsverarbeiter

Wir bedienen uns für die Durchführung unseres Kerngeschäfts, der Dienstleistungen von branchen- führenden 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:

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

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

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 Authentifizierungvor Zutrittsgewährung zu Rechenzentrenerforderlich[A]
4.	Videoüberwachung der Ein- und Ausgänge[A], Einbruchmeldeanlage	Zutrittsrechtevergabe für Mitarbeiter und ex-terne 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 erfolg-ten Zutritte[A]

1.2. Zugangskontrolle

Nr	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Einsatz von Firewalls zum Schutz derIT-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-Systemenur nach Authentifikation, Einsatz vonVPNA	
6.		Alarmierung zuständiger Mitarbeiter beiauffälligen 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 Auf-gaben- und Zuständigkeitsgebiet
2.	Protokollierung auffälliger Zugriffsversuche auf informationsverarbeitende Systeme, Mitteilung an zuständige Mitarbeiter[A]	Vorhalten eines Incident ManagementTeam[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 Datenlöschen, hinzufügen oder ändern[C]
5.	Implementierung von Netzwerkgerätenzur Verwaltung der Schnittstellenkommunikation mit Internet Service Providern (ISPs)[A]	
6.	Redundante Verbindung zu mehrerer Kommunkationsdiensten des Netzwerkes[A]	
7.	Einsatz von Verschlüsselungstechnologien (Security Socket Layers (SSL)[A])	

1.4. Trennungskontrolle

Nr	Technische Maßnahmen	Organisatorische Maßnahmen
1.	Trennung von operativem und Unterneh-mensnetzwerk[A], Getrennte Datenspeicherung auf Daten-bankebene 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 Ausscheidendes 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 Per-sonen, einschließlich der Vergabe differen-zierter Zugriffsrechte und Rollen[C]
2.	Einsatz von Firewall, VPN- und Verschlüsselungstechnologien zum Schutzder Gateways uns Pipelines über die Daten übertragen werden	Kontrollierte und dokumentierte Löschungder 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 un-vollständiger Datenübertragung (End-to- End-Check)[C]
5.		Protokollierung der Datenübertragung (so-weit möglich)[C]

2. Vertraulichkeits- und Belastbarkeitskontrolle (Art. 32 Abs. 2 c) 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 zursofortigen 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 Temperaturund Feuchtigkeit im Rechenzentrum[A]
4.	Klimatisierung der Rechenzentren[A]	Clusterförmige Verteilung der Rechenzent-rum weltweit[A] Ausschluss „kalter“ Rechenzentren, allesind aktiv[A]

5.	System zur Überwachung von Temperatur und Feuchtigkeit in Rechenzentren[A]	Automatisiertes System zur Verlagerung des Kundendatenverkehrs bei Störungenaus dem betroffenen Bereich[A]
6.	N+1-Konfiguration, die gewährleis- tet, dass im Falle eines Ausfalls eines Rechenzentrums genügend Kapazität zur Verfügung steht, um den Datenver- kehr 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 Verfügbar- keitszonen mit mehreren Tier-1-Transit- anbietern[A]	Räumliche Trennung von Verfügbarkeits- zonen in typischen Metropolregionen undEinrichtung von Verfügbarkeitszonen in Überschwemmungsgebieten mit geringe-rem Risiko[A]
8.	Vorhaltung von Systemen zur Erzeugungvon 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 Konfigurationsände-rungen an der bestehenden Infrastruktur werden gemäß den Industrienormen für ähnliche Systeme autorisiert, protokolliert, getestet, genehmigt und dokumentiert[A]
12.		Vorgaben hinsichtlich der Information vonKunden 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 Incdent 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 elektronischabrufbar[A]	
2.	Technische Protokollierung der Eingabe, Änderung und Löschung von Daten[A]	
3.	Manuelle und automatisierte Kontrolle von hierfür softwareseitig erstellten Pro-tokolldateien[A]	