VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

zwischen

.....

Vertretungsberechtigter Geschäftsführer: .....

(im folgenden Auftraggeber genannt)

und

NETZCOCKTAIL GmbH, Dorpatweg 10, 48159 Münster
Vertretungsberechtigter Geschäftsführer: Marc-Henning Hütte

(im folgenden Auftragnehmer genannt)

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand
Der Gegenstand des Auftrags ergibt sich aus der zwischen den Parteien geschlossenen Leistungsvereinbarung einschließlich der hierzu vereinbarten Angebote, Leistungsbeschreibungen und Ergänzungen (im Folgenden „Leistungsvereinbarung").

Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers im Rahmen der Erbringung der vereinbarten Dienstleistungen.

Art und Zweck der Verarbeitung richten sich nach der jeweiligen Leistungsvereinbarung.

(2) Dauer
Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt hiervon unberührt. Insbesondere kann der Auftraggeber den Vertrag außerordentlich kündigen, wenn der Auftragnehmer schwerwiegend gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages verstößt, rechtmäßige Weisungen des Auftraggebers nicht ausführt oder Kontrollrechte des Auftraggebers vertragswidrig verweigert.

Schwerwiegende Verstöße gegen die in diesem Vertrag vereinbarten sowie aus Art. 28 DSGVO resultierenden Pflichten gelten als wichtiger Grund.

§2 Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten
Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich insbesondere aus der zwischen den Parteien geschlossenen Leistungsvereinbarung einschließlich der hierzu vereinbarten Angebote, Leistungsbeschreibungen und Ergänzungen.

Die Erbringung der vertraglich vereinbarten Leistungen findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

Eine Verarbeitung in Drittstaaten erfolgt nur unter Einhaltung der Voraussetzungen der Art. 44 ff. DSGVO.

(2) Art der Daten
Gegenstand der Verarbeitung personenbezogener Daten sind insbesondere folgende Datenarten bzw. Datenkategorien:

- Personenstammdaten
- Kommunikationsdaten (z. B. Telefonnummer, E-Mail-Adresse)
- Vertragsstammdaten
- Abrechnungs- und Zahlungsdaten
- Nutzungs- und Protokolldaten
- Inhaltsdaten, soweit diese durch den Auftraggeber im Rahmen der beauftragten Leistungen verarbeitet werden

(3) Kategorien betroffener Personen
Die Kategorien der von der Verarbeitung betroffenen Personen umfassen insbesondere:

- Kunden
- Interessenten
- Mitarbeiter des Auftraggebers
- Nutzer der vom Auftraggeber betriebenen Webseiten und Systeme

(4) Verarbeitung besonderer Kategorien personenbezogener Daten
Eine Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO ist grundsätzlich nicht Gegenstand der vereinbarten Leistungen.

Soweit der Auftraggeber dennoch entsprechende Daten verarbeitet oder übermittelt, erfolgt dies ausschließlich auf Weisung und Verantwortung des Auftraggebers.

Der Auftraggeber ist verpflichtet, den Auftragnehmer vorab in Textform zu informieren, sofern besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO verarbeitet werden sollen.

§ 3 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz personenbezogener Daten.

Die zum Zeitpunkt des Vertragsschlusses bestehenden technischen und organisatorischen Maßnahmen sind vom Auftragnehmer dokumentiert und können dem Auftraggeber auf Anfrage zur Verfügung gestellt werden.

(2) Der Auftragnehmer gewährleistet ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten.

Dabei berücksichtigt der Auftragnehmer insbesondere den Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schweregrade der Risiken für die Rechte und Freiheiten natürlicher Personen gemäß Art. 32 DSGVO.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung.

Der Auftragnehmer ist berechtigt, alternative oder ergänzende Maßnahmen umzusetzen, sofern hierdurch das Schutzniveau der vereinbarten Maßnahmen nicht unterschritten wird.

Wesentliche Änderungen der technischen und organisatorischen Maßnahmen sind zu dokumentieren.

§ 4 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf personenbezogene Daten, die im Auftrag verarbeitet werden, ausschließlich auf dokumentierte Weisung des Auftraggebers berichtigen, löschen oder in ihrer Verarbeitung einschränken.

Soweit sich eine betroffene Person unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit dies vom vereinbarten Leistungsumfang umfasst ist, unterstützt der Auftragnehmer den Auftraggeber bei der Erfüllung von Betroffenenrechten, insbesondere im Hinblick auf Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenportabilität sowie Auskunftserteilung, jeweils auf dokumentierte Weisung des Auftraggebers.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer erfüllt die gesetzlichen Pflichten gemäß Art. 28 bis 33 DSGVO und gewährleistet insbesondere die Einhaltung der folgenden Anforderungen.

b) Der Auftragnehmer wahrt die Vertraulichkeit gemäß Art. 28 Abs. 3 lit. b, Art. 29 sowie Art. 32 Abs. 4 DSGVO.

Der Auftragnehmer setzt ausschließlich Personen zur Verarbeitung personenbezogener Daten ein, die zur Vertraulichkeit verpflichtet und mit den einschlägigen Datenschutzbestimmungen vertraut gemacht wurden.

c) Der Auftragnehmer trifft und unterhält die für die Verarbeitung erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO.

d) Der Auftragnehmer unterstützt den Auftraggeber im angemessenen Umfang bei der Zusammenarbeit mit Aufsichtsbehörden sowie bei sonstigen gesetzlichen Pflichten im Zusammenhang mit der Auftragsverarbeitung.

e) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen oder Maßnahmen von Aufsichtsbehörden, soweit diese die Auftragsverarbeitung betreffen.

   Dies gilt auch, soweit gegen den Auftragnehmer Ermittlungen oder Verfahren im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen dieses Vertrages eingeleitet werden.

f) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um die datenschutzkonforme Verarbeitung personenbezogener Daten sicherzustellen.

g) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der vertraglichen Vereinbarungen und nach Weisung des Auftraggebers, sofern keine gesetzliche Verpflichtung zur anderweitigen Verarbeitung besteht.

   Soweit eine gesetzliche Verpflichtung besteht, teilt der Auftragnehmer dies dem Auftraggeber vor der Verarbeitung mit, sofern eine solche Mitteilung gesetzlich zulässig ist.

h) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten ausschließlich zur Erfüllung der vertraglich vereinbarten Leistungen und nicht zu eigenen Zwecken.

i) Der Auftragnehmer unterstützt den Auftraggeber im erforderlichen Umfang bei der Erfüllung von Betroffenenrechten gemäß Art. 12 bis 22 DSGVO sowie bei der Erstellung von Verzeichnissen von Verarbeitungstätigkeiten und gegebenenfalls erforderlichen Datenschutz-Folgenabschätzungen.

j) Der Auftragnehmer wahrt die Vertraulichkeit der im Rahmen dieses Vertrages verarbeiteten personenbezogenen Daten auch über die Beendigung des Vertrages hinaus.

§ 6 Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, zur Erfüllung seiner vertraglichen Leistungen Unterauftragnehmer einzusetzen.

Nicht als Unterauftragsverhältnisse im Sinne dieser Vereinbarung gelten Nebenleistungen, wie insbesondere Telekommunikationsleistungen, Post- und Transportdienstleistungen, Wartung und Supportleistungen sowie sonstige Leistungen, die der Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Systeme und Datenverarbeitung dienen.

Der Auftragnehmer stellt sicher, dass auch bei ausgelagerten Nebenleistungen angemessene datenschutzrechtliche und datensicherheitsbezogene Maßnahmen eingehalten werden.

(2) Der Auftraggeber erteilt die allgemeine Genehmigung zur Beauftragung von Unterauftragnehmern gemäß Art. 28 Abs. 2 DSGVO.

Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragnehmer ergeben sich aus der nachfolgenden Übersicht:

Firma Unterauftragnehmer	Anschrift / Land	Leistung
23m GmbH	Johann-Krane-Weg 18, 48149 Münster, Deutschland	Hosting Webserver
Zendesk Inc.	989 Market Street, San Francisco, CA 94103, USA	Ticketsystem / Kundensupport

Slack Technologies, LLC	500 Howard Street, San Francisco, CA 94105, USA	Teamkommunikation
Atlassian Pty Ltd	Level 6, 341 George Street, Sydney NSW 2000, Australien	Ticketsystem
Living Concept Werbeagentur GmbH	Dorpatweg 10, 48159 Münster, Deutschland	Grafische Dienstleistungen
Living Concept Holding GmbH	An der Germania Brauerei 6–8, 48159 Münster, Deutschland	Buchhaltung
Der Riese GmbH	Eulerstraße 2, 48155 Münster , Deutschland	Werbemittel

Der Auftragnehmer informiert den Auftraggeber über Änderungen bei den eingesetzten Unterauftragnehmern durch Veröffentlichung auf seiner Website im Bereich Datenschutz unter www.netzcocktail.de oder in sonstiger geeigneter Form.

(3) Der Auftragnehmer stellt sicher, dass Unterauftragnehmer vertraglich mindestens die Datenschutzpflichten übernehmen, die in dieser Vereinbarung festgelegt sind.

(4) Erfolgt eine Verarbeitung personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, stellt der Auftragnehmer sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO eingehalten werden.

(5) Der Auftragnehmer überprüft die Einhaltung der datenschutzrechtlichen Verpflichtungen seiner Unterauftragnehmer in angemessenem Umfang.

Nachweise über die Einhaltung datenschutzrechtlicher Verpflichtungen durch Unterauftragnehmer werden dem Auftraggeber auf Anfrage in angemessenem Umfang zur Verfügung gestellt, soweit dem keine gesetzlichen, vertraglichen oder berechtigten Vertraulichkeitsinteressen entgegenstehen.

(6) Der Auftragnehmer haftet gegenüber dem Auftraggeber nach Maßgabe der gesetzlichen Vorschriften und der vertraglichen Haftungsregelungen für Verstöße von Unterauftragnehmern gegen die ihnen übertragenen datenschutzrechtlichen Verpflichtungen.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten durch den Auftragnehmer in angemessenem Umfang zu überprüfen oder durch zur Verschwiegenheit verpflichtete Dritte überprüfen zu lassen.

Kontrollen sind rechtzeitig vorher anzukündigen und haben während der üblichen Geschäftszeiten sowie unter Berücksichtigung der berechtigten Betriebs- und Geschäftsgeheimnisinteressen des Auftragnehmers zu erfolgen.

Kontrollen dürfen den Geschäftsbetrieb des Auftragnehmers nicht unangemessen beeinträchtigen und müssen verhältnismäßig sein.

Der Auftragnehmer darf die Kontrolle von angemessenen Sicherheits- und Vertraulichkeitsanforderungen abhängig machen.

(2) Der Auftragnehmer unterstützt den Auftraggeber bei der Durchführung angemessener Kontrollen und stellt auf Anforderung die erforderlichen Informationen und Nachweise in angemessenem Umfang zur Verfügung, insbesondere hinsichtlich der Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO.

(3) Der Nachweis geeigneter technischer und organisatorischer Maßnahmen kann insbesondere erfolgen durch:

- Zertifizierungen gemäß Art. 42 DSGVO,
- genehmigte Verhaltensregeln gemäß Art. 40 DSGVO,
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Stellen,
- Datenschutz- oder IT-Sicherheitsaudits,
- sonstige geeignete Nachweise zur Informationssicherheit und zum Datenschutz.

§ 8 Mitteilung bei Datenschutzverstößen und Unterstützungspflichten

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO geregelten Pflichten, insbesondere im Zusammenhang mit:

- der Sicherheit der Verarbeitung,
- der Meldung von Datenschutzverletzungen,
- Datenschutz-Folgenabschätzungen sowie
- erforderlichen Konsultationen mit Aufsichtsbehörden.

Der Auftragnehmer verpflichtet sich insbesondere:

a) geeignete technische und organisatorische Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus zu treffen,

b) den Auftraggeber unverzüglich über Datenschutzverletzungen sowie sicherheitsrelevante Vorfälle zu informieren, soweit diese die im Auftrag verarbeiteten personenbezogenen Daten betreffen,

c) den Auftraggeber im Rahmen seiner gesetzlichen Informations- und Meldepflichten angemessen zu unterstützen und die hierfür erforderlichen Informationen unverzüglich bereitzustellen,

d) den Auftraggeber bei erforderlichen Datenschutz-Folgenabschätzungen sowie vorherigen Konsultationen mit Aufsichtsbehörden im angemessenen Umfang zu unterstützen.

(2) Soweit Unterstützungsleistungen des Auftragnehmers nicht Bestandteil der vertraglich vereinbarten Leistungen sind und nicht auf einem vom Auftragnehmer zu vertretenden Verstoß beruhen, kann der Auftragnehmer hierfür eine angemessene Vergütung verlangen.

§ 9 Weisungsbefugnis des Auftraggebers

(1) Weisungen des Auftraggebers erfolgen grundsätzlich in Textform.

Mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen.

(2) Hält der Auftragnehmer eine Weisung des Auftraggebers für rechtswidrig oder datenschutzrechtlich unzulässig, informiert er den Auftraggeber hierüber unverzüglich.

Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung bis zur Bestätigung oder Änderung durch den Auftraggeber auszusetzen.

§ 10 Weisungsberechtigte Personen

Weisungsberechtigte Personen des Auftraggebers ergeben sich aus den jeweils benannten Ansprechpartnern des Auftraggebers.

Weisungsempfänger beim Auftragnehmer sind insbesondere die Geschäftsführung sowie die mit der technischen Betreuung beauftragten Mitarbeiter.

Änderungen oder Vertretungen sind der jeweiligen Vertragspartei in Textform mitzuteilen.

§ 11 Löschung und Rückgabe personenbezogener Daten

(1) Der Auftragnehmer erstellt personenbezogene Daten ausschließlich im Rahmen der vertraglichen Leistungserbringung oder soweit dies zur ordnungsgemäßen Datenverarbeitung erforderlich ist.

Hiervon umfasst sind insbesondere Sicherheitskopien, Protokolldaten sowie Daten, die aufgrund gesetzlicher Aufbewahrungspflichten gespeichert werden müssen.

(2) Nach Beendigung der vertraglich vereinbarten Leistungen oder auf Weisung des Auftraggebers hat der Auftragnehmer sämtliche personenbezogenen Daten und Unterlagen, die im Zusammenhang mit dem Auftragsverhältnis verarbeitet wurden, nach Wahl des Auftraggebers entweder herauszugeben oder datenschutzgerecht zu löschen, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Die Löschung erfolgt unter Berücksichtigung technischer und organisatorischer Gegebenheiten innerhalb angemessener, technisch üblicher Fristen.

Eine Löschung aus Sicherungskopien erfolgt im Rahmen der regulären Backup- und Löschzyklen, soweit eine gesonderte Löschung technisch nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

Der Auftragnehmer stellt dem Auftraggeber auf Anfrage eine Bestätigung der Löschung zur Verfügung.

(3) Dokumentationen, die dem Nachweis der ordnungsgemäßen und datenschutzkonformen Verarbeitung dienen, dürfen vom Auftragnehmer entsprechend der gesetzlichen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt werden.

§ 12 Sonstiges

Wird das Eigentum oder der Zugriff des Auftraggebers auf personenbezogene Daten durch Maßnahmen Dritter, insbesondere durch Pfändung, Beschlagnahme, Insolvenzverfahren oder sonstige Ereignisse gefährdet, informiert der Auftragnehmer den Auftraggeber hierüber unverzüglich.

Ein Zurückbehaltungsrecht gemäß § 273 BGB hinsichtlich der im Auftrag verarbeiteten personenbezogenen Daten und der zugehörigen Datenträger wird ausgeschlossen.

Für die Haftung des Auftragnehmers gelten ergänzend die Haftungsregelungen der zugrundeliegenden Leistungsvereinbarung sowie der Allgemeinen Geschäftsbedingungen des Auftragnehmers.

Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Änderungen und Ergänzungen dieser Vereinbarung bedürfen mindestens der Textform.

Münster, 16.07.2026

Ort, Datum / Unterschrift Auftragnehmer	Ort, Datum / Unterschrift Auftraggeber

ANLAGE

TECHNISCH-ORGANISATORISCHE MASSNAHMEN (TOM)

Zutrittskontrolle

Maßnahmen zur Verhinderung des unbefugten Zutritts zu Datenverarbeitungsanlagen und Geschäftsräumen:

Büro- und Geschäftsräume

- Manuelle oder elektronische Schließsysteme
- Regelung und Dokumentation der Schlüsselvergabe
- Zutrittsbeschränkung für betriebsfremde Personen
- Begleitung von Besuchern innerhalb sensibler Bereiche
- Sorgfältige Auswahl von Dienstleistern und Reinigungspersonal

Rechenzentrumsinfrastruktur

- Videoüberwachung sicherheitsrelevanter Bereiche
- Elektronische Zutrittskontrollsysteme
- Mehrstufige Sicherheitszonen
- 24/7 Überwachung und Sicherheitsdienst
- Alarm- und Meldesysteme
- Zutrittsprotokollierung

Zugangskontrolle

Maßnahmen zur Verhinderung der unbefugten Nutzung von IT-Systemen:

- Benutzerbasierte Authentifizierung mittels Benutzername und Passwort
- Passwortregeln (Mindestlänge, Komplexität)
- Einsatz von Mehrfaktor-Authentifizierung, soweit technisch möglich
- Automatische Sperrmechanismen bei Fehlversuchen
- Rollen- und berechtigungsbasierte Benutzerverwaltung
- Verschlüsselte Datenübertragung (z. B. TLS/VPN)
- Einsatz von Firewall- und Sicherheitslösungen
- Regelmäßige Sicherheitsupdates und Patchmanagement
- Schutzmaßnahmen für WLAN-Netzwerke
- Einsatz aktueller Endpoint-Protection- und Antivirensysteme, soweit eingesetzt

Zugriffskontrolle

Maßnahmen zur Sicherstellung, dass berechtigte Benutzer ausschließlich auf die ihrer Berechtigung unterliegenden Daten zugreifen können:

- Rollenbasierte Berechtigungskonzepte
- Verwaltung und Dokumentation von Benutzerrechten
- Beschränkung administrativer Zugriffe
- Protokollierung sicherheitsrelevanter Zugriffe
- Sichere Aufbewahrung von Datenträgern
- Datenschutzgerechte Löschung von Datenträgern vor Wiederverwendung

Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung von Daten unterschiedlicher Auftraggeber oder Verarbeitungszwecke:

- Mandantentrennung innerhalb eingesetzter Systeme
- Getrennte Speicherung von Produktiv- und Testdaten
- Trennung von Entwicklungs-, Test- und Produktivumgebungen
- Berechtigungskonzepte zur Einschränkung systemübergreifender Zugriffe

Weitergabekontrolle

Maßnahmen zur Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Daten bei der Übertragung oder Speicherung:

- Verschlüsselte Datenübertragung
- Einsatz sicherer Kommunikationswege
- Regelmäßige Sicherheitsupdates von Kommunikationssystemen
- Protokollierung sicherheitsrelevanter System- und Kommunikationsvorgänge
- Datenschutzgerechte Vernichtung von Datenträgern und Papierunterlagen
- Auswahl geeigneter Dienstleister für Transport- und Entsorgungsleistungen

Eingabekontrolle

Maßnahmen zur Nachvollziehbarkeit von Eingabe, Änderung und Löschung personenbezogener Daten:

- Vergabe individueller Benutzerkennungen
- Protokollierung von Eingaben, Änderungen und Löschungen, soweit technisch möglich
- Berechtigungskonzepte für Eingabe-, Änderungs- und Löschrechte
- Nachvollziehbarkeit administrativer Tätigkeiten
- Dokumentation relevanter Verarbeitungsvorgänge

Verfügbarkeitskontrolle

Maßnahmen zum Schutz personenbezogener Daten gegen zufällige Zerstörung oder Verlust:

- Regelmäßige Datensicherungen
- Sichere Speicherung und Übertragung von Backups
- Unterbrechungsfreie Stromversorgung (USV)
- Redundante Systeme und Speichermedien
- Monitoring kritischer Systeme und Dienste
- Schutz vor Schadsoftware und Cyberangriffen
- Regelmäßige Überprüfung der Wiederherstellbarkeit von Datensicherungen
- Brandschutz- und Rauchmeldesysteme
- Dokumentierte Notfall- und Wiederherstellungsverfahren

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Maßnahmen zur Sicherstellung der fortlaufenden Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste:

- Regelmäßige Überprüfung und Aktualisierung der technischen und organisatorischen Maßnahmen
- Dokumentierte Verfahren zum Umgang mit Sicherheitsvorfällen
- Regelmäßige Aktualisierung von Software und Sicherheitssystemen
- Sensibilisierung und Verpflichtung der Mitarbeiter auf Datenschutz und Vertraulichkeit
- Datenschutzfreundliche Voreinstellungen („Privacy by Default“)
- Regelmäßige Überprüfung von Berechtigungen und Zugriffsrechten
- Dokumentation relevanter Datenschutz- und Sicherheitsmaßnahmen