

Vertrag nach Art. 28 DSGVO

Auftragsverarbeitungsvertrag (AVV)

Stand

11. Oktober 2026

Herausgeber

IonKon GmbH

Inhalt

	Vertragsparteien	3
1	Gegenstand und Dauer der Verarbeitung	3
2	Art und Zweck der Verarbeitung	3
3	Art der Daten und Kategorien betroffener Personen	4
4	Weisungsbindung	4
5	Vertraulichkeit der Beschäftigten	4
6	Maßnahmen nach Art. 32 DSGVO	4
7	Bedingungen für den Einsatz von Subauftragsverarbeitern	5
8	Unterstützung bei der Erfüllung der Rechte betroffener Personen	5
9	Unterstützung bei der Einhaltung der Art. 32 bis 36 DSGVO	5
10	Löschung oder Rückgabe nach Vertragsende	6
11	Nachweise und Kontrollen	6
12	Haftung, Laufzeit, Schlussbestimmungen	6
	Anlage 1 · Technische und organisatorische Maßnahmen (TOM)	7

Vertragsparteien

Auftragsverarbeiter ist die IonKon GmbH, Dessauer Straße 280, 06886 Lutherstadt Wittenberg. Verantwortlicher ist der Kunde, der über das Kundenkonto ein individuelles Sprachmodell bei IonKon beauftragt; Name und Anschrift des Kunden ergeben sich aus dem Hauptvertrag (angenommenes Angebot).

1 Gegenstand und Dauer der Verarbeitung

Gegenstand dieses Vertrags ist die einmalige Verarbeitung der vom Kunden hochgeladenen Dokumente zur Erzeugung eines kundenindividuellen Sprachmodells durch IonKon, dessen Auslieferung an den Kunden einschließlich des aus den Kundendaten erzeugten Datensatzes (Rückgabe abgeleiteter Daten) sowie die anschließende Löschung der bei IonKon verbliebenen Kopien. Ohne gebuchtes Hosting findet nach der Lieferung keine laufende Verarbeitung von Kundendaten durch IonKon mehr statt; das ausgelieferte Modell arbeitet dann vollständig auf eigener Hardware beim Kunden, ohne weitere Anbindung an IonKon. Hat der Kunde Hosting gebucht (§ 17 AGB), umfasst dieser Vertrag zusätzlich den laufenden Betrieb des Modells auf einem von IonKon für den Kunden gemieteten Server für die Dauer des Hostings: Speicherung der im Betrieb abgelegten Dokumente, Verarbeitung der Eingaben und Ausgaben der Nutzer, Benutzerkonten sowie die tägliche verschlüsselte Sicherung. Liefert IonKon einen eingerichteten Server, richtet IonKon Modell und Datensatz vor der Lieferung darauf ein; danach findet keine Verarbeitung durch IonKon mehr statt.

Dieser Vertrag gilt für die Dauer des Hauptvertrags und endet, sobald IonKon sämtliche im Rahmen der Verarbeitung entstandenen Kopien der Kundendaten gelöscht hat. Die Löschfristen ergeben sich aus den technischen und organisatorischen Maßnahmen (Anlage 1): Löschung nach Empfangsbestätigung der Lieferung, spätestens nach der technischen Aufbewahrungsobergrenze (Standard 30 Tage ab Bereitstellung, absolute Obergrenze 180 Tage ab Auftragsbeginn).

2 Art und Zweck der Verarbeitung

Die Verarbeitung dient ausschließlich der Erbringung der im Hauptvertrag beschriebenen Leistung: Extraktion und Aufbereitung der vom Kunden hochgeladenen Dokumente, Filterung personenbezogener Daten, Erzeugung synthetischer Trainingsbeispiele sowie das eigentliche Training des kundenindividuellen Modells und dessen Verpackung zur Auslieferung.

Für die Datensynthese setzt IonKon ausschließlich selbst betriebene Software ein, die auf einer eigens für den jeweiligen Auftrag bereitgestellten und nach Abschluss gelöschten GPU-Instanz in der EU oder der Schweiz läuft. Ein externer KI-Anbieter erhält zu keinem Zeitpunkt Zugriff auf Dokumente des Kunden; das ist technisch erzwungen.

3 Art der Daten und Kategorien betroffener Personen

Gegenstand der Verarbeitung sind die vom Kunden im Rahmen der Bestellung als ZIP-Datei hochgeladenen Dokumente sowie die daraus abgeleiteten Trainings- und Zwischendaten (extrahierter Text, synthetische Trainingsbeispiele, Modellgewichte). Welche personenbezogenen Daten die Dokumente im Einzelnen enthalten, bestimmt der Kunde durch die Auswahl der hochgeladenen Inhalte; in Betracht kommen insbesondere Namen, Kontaktdaten und sonstige in Geschäftsdokumenten übliche Angaben zu Mitarbeitenden, Kunden und Geschäftspartnern des Kunden. Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind vertraglich ausgeschlossen: Der Kunde lädt keine solchen Daten hoch. Ist die Verarbeitung besonderer Kategorien im Einzelfall doch beabsichtigt, bedarf es vor dem Upload einer gesonderten schriftlichen Vereinbarung mit zusätzlichen Schutzmaßnahmen.

Kategorien betroffener Personen sind die Personen, deren Daten in den vom Kunden bereitgestellten Dokumenten enthalten sind, insbesondere Mitarbeitende, Kunden und Geschäftspartner des Kunden.

Bei gebuchtem Hosting kommen die im Betrieb abgelegten Dokumente, die Eingaben und Ausgaben der Nutzer sowie die Benutzerkonten (Name, E-Mail-Adresse, Anmeldedaten) hinzu; betroffen sind zusätzlich die Nutzer des Kunden.

4 Weisungsbindung

IonKon verarbeitet die Daten des Kunden ausschließlich auf dokumentierte Weisung des Kunden. Die Annahme des Angebots durch den Kunden im Kundenkonto sowie der Inhalt dieses Vertrags gelten als Weisung. Weitere oder abweichende Weisungen bedürfen der Textform und einer Bestätigung durch IonKon. Ist IonKon der Auffassung, dass eine Weisung des Kunden gegen die DSGVO oder sonstige Datenschutzbestimmungen verstößt, teilt IonKon dies dem Kunden unverzüglich mit.

5 Vertraulichkeit der Beschäftigten

IonKon stellt sicher, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, und dass ihnen die Daten des Kunden nur im für ihre jeweilige Tätigkeit erforderlichen Umfang zugänglich sind.

6 Maßnahmen nach Art. 32 DSGVO

Die von IonKon getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus ergeben sich aus den als Anlage 1 beigefügten technischen und organisatorischen Maßnahmen (TOM). Die TOM ist Bestandteil dieses Vertrags.

7 Bedingungen für den Einsatz von Subauftragsverarbeitern

IonKon setzt zur Erfüllung dieses Vertrags die folgenden Subauftragsverarbeiter ein; der Kunde erteilt hiermit die allgemeine Genehmigung zu ihrem Einsatz. Alle genannten Anbieter verarbeiten die Daten des Kunden ausschließlich in der Europäischen Union oder der Schweiz; für beide Rechtsräume hat die Europäische Kommission ein gleichwertiges Datenschutzniveau festgestellt.

STRATO GmbH (Deutschland): Betrieb des Webserverns und der Datenbank.

DataCrunch Oy, Cloud-Marke „Verda“ (Finnland): GPU-Rechenleistung für Training und Datensynthese, je Auftrag eine eigene, anschließend gelöschte Instanz; verarbeitet in Finnland.

Akenes SA, Marke „Exoscale“ (Schweiz): verschlüsselter Objektspeicher für die hochgeladenen Dokumente und, bei gebuchtem Hosting, für die tägliche Sicherung in Frankfurt am Main sowie GPU-Rechenleistung für Training und Datensynthese, je Auftrag eine eigene, anschließend gelöschte Instanz; verarbeitet in Frankfurt, Zagreb oder Zürich. Welche Region genutzt wird, entscheidet IonKon je Auftrag nach verfügbarer Kapazität.

Hetzner Online GmbH (Deutschland): nur bei gebuchtem Hosting; Miete des Servers, auf dem das Modell des Kunden betrieben wird, in Rechenzentren in Deutschland (Nürnberg, Falkenstein) oder Finnland (Helsinki), Standort laut Angebot.

BuchhaltungsButler GmbH (Deutschland): Rechnungsstellung und Zahlungsabgleich; erhält nur Stammdaten, keine Trainingsdokumente.

Beabsichtigt IonKon, einen Subauftragsverarbeiter auszutauschen oder einen weiteren hinzuzuziehen, informiert IonKon den Kunden vorab in Textform; der Kunde kann der Änderung aus wichtigem Grund innerhalb von 14 Tagen ab Zugang der Mitteilung in Textform widersprechen. Widerspricht der Kunde nicht innerhalb dieser Frist, gilt der Wechsel als genehmigt. IonKon verpflichtet jeden Subauftragsverarbeiter vertraglich zu denselben Datenschutzpflichten wie in diesem Vertrag.

8 Unterstützung bei der Erfüllung der Rechte betroffener Personen

IonKon unterstützt den Kunden nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch. Wendet sich eine betroffene Person unmittelbar an IonKon, leitet IonKon die Anfrage unverzüglich an den Kunden weiter.

9 Unterstützung bei der Einhaltung der Art. 32 bis 36 DSGVO

IonKon unterstützt den Kunden bei der Sicherheit der Verarbeitung, bei der Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und die betroffene Person sowie bei Datenschutz-Folgenabschätzungen und der vorherigen Konsultation der Aufsichtsbehörde. Wird IonKon eine Verletzung des Schutzes personenbezogener Daten bekannt, die Daten des Kunden betrifft, meldet IonKon dies dem Kunden unverzüglich, spätestens 48 Stunden nach Kenntniserlangung, über die Kontaktadresse info@ionkon.de; die Meldung enthält mindestens

Art der Verletzung, betroffene Datenkategorien, wahrscheinliche Folgen und ergriffene Gegenmaßnahmen, damit der Kunde seine eigene Meldefrist von 72 Stunden nach Art. 33 DSGVO einhalten kann.

10 Löschung oder Rückgabe nach Vertragsende

Der aus den Kundendaten erzeugte Datensatz und das Modell werden dem Kunden mit der Bereitstellung übergeben (Rückgabe abgeleiteter Daten). Nach Beendigung der Verarbeitung löscht IonKon sämtliche bei ihr vorhandenen Kopien der Kundendaten (hochgeladene Dokumente, daraus erzeugte Trainingsdaten und eigene Modellkopien) spätestens nach Ablauf der technischen Aufbewahrungsobergrenze (Standard 30 Tage ab Bereitstellung, absolute Obergrenze 180 Tage ab Auftragsbeginn). Sobald die Löschung erfolgt ist, erteilt IonKon dem Kunden automatisch einen Löschnachweis. Eine Rückgabe der Ausgangsdokumente ist nicht erforderlich, da der Kunde die von ihm hochgeladenen Dokumente bereits im Original besitzt. Bei gebuchtem Hosting gilt für den Server und die im Betrieb abgelegten Daten § 17 Abs. 2 AGB: Bereitstellung der Dokumente zum Download auf Anforderung innerhalb von 30 Tagen nach Vertragsende, danach Löschung des Servers einschließlich der Sicherungen und Löschnachweis.

11 Nachweise und Kontrollen

IonKon weist dem Kunden die Einhaltung der in diesem Vertrag niedergelegten Pflichten auf Anforderung nach und ermöglicht dem Kunden oder einem von ihm beauftragten Prüfer Kontrollen, insbesondere durch Bereitstellung geeigneter Nachweise. Der Kunde kann die Einhaltung dieses Vertrags einmal jährlich sowie bei konkretem Anlass prüfen; Vor-Ort-Prüfungen kündigt der Kunde mit einem Vorlauf von 14 Tagen an. Kontrollen finden während der üblichen Geschäftszeiten von IonKon statt, unter Wahrung der Betriebs- und Geschäftsgeheimnisse von IonKon sowie der Vertraulichkeit und Sicherheit der Daten anderer Kunden, ohne den Betriebsablauf von IonKon unangemessen zu stören. IonKon kann den Nachweis alternativ durch aktuelle Zertifikate oder Prüfberichte erbringen. Die Kosten einer Vor-Ort-Prüfung trägt der Kunde, außer bei festgestelltem wesentlichem Verstoß von IonKon.

12 Haftung, Laufzeit, Schlussbestimmungen

Für die Haftung gelten die Regelungen der Allgemeinen Geschäftsbedingungen, soweit dieser Vertrag nichts Abweichendes bestimmt. Dieser Vertrag beginnt mit seinem Abschluss, spätestens vor dem Daten-Upload des Kunden, und endet mit vollständiger Löschung der Kundendaten. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag geht dieser Vertrag im Bereich des Datenschutzes vor. Es gilt das Recht der Bundesrepublik Deutschland.

Anlage 1

Technische und organisatorische Maßnahmen (TOM)

Übersicht

Anlage 1 zum Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 lit. c, Art. 32 DSGVO.

Auftragsverarbeiter ist die IonKon GmbH, Dessauer Straße 280, 06886 Lutherstadt Wittenberg.

Gegenstand der Verarbeitung: Einmalige Verarbeitung der vom Kunden bereitgestellten Dokumente zur Erzeugung eines kundenindividuellen Sprachmodells, Auslieferung auf einem lokalen KI-Server, anschließende Löschung. Nach der Lieferung findet keine laufende Verarbeitung von Kundendaten durch IonKon statt; das Modell arbeitet vollständig beim Kunden.

1.1 Zutrittskontrolle (physisch)

- Kundendaten werden ausschließlich in Rechenzentren von Infrastrukturpartnern in der EU oder der Schweiz verarbeitet und gespeichert; ein eigener Serverbetrieb mit Kundendaten in Geschäftsräumen findet nicht statt.
- Physische Sicherheit der Rechenzentren liegt bei den Infrastrukturpartnern; das Verzeichnis der eingesetzten Subauftragsverarbeiter mit Sitz und Zweck steht in Nummer 7 des AVV sowie in Nummer 4.3 dieser TOM.
- Geräterichtlinie: Arbeitsgeräte der Mitarbeitenden sind mit Festplattenverschlüsselung und automatischer Bildschirmsperre gesichert.

1.2 Zugangskontrolle (Systeme)

- Zugriff auf Produktionssysteme ist auf einen minimalen, namentlich dokumentierten Personenkreis beschränkt; die Aufstellung wird auf Anfrage offengelegt.
- Programmatischer Zugriff auf die Trainings-API nur mit geheimen API-Schlüsseln (mindestens 32 Byte Zufall); Schlüssel werden nicht im Quellcode, sondern ausschließlich als Umgebungsvariablen bzw. aus einem Secret-Store bereitgestellt. Ein automatischer Härtetest verweigert den Produktionsstart mit Platzhalter- oder Kurzschlüsseln.
- Integrationsschnittstelle für das eigene Kundenverwaltungssystem: Zugriff nur mit Zugangsdaten, die je Verwendungszweck ausgestellt und auf einzelne Berechtigungen begrenzt werden (Lesen von Aufträgen, Lesen von Kundendaten, Aktivierung, Auftragssteuerung).
- Kundenportal: passwortbasierte Konten (bcrypt), E-Mail-Verifizierung vor Bestellung, Einmal-Tokens (gehasht, einmalverwendbar) für Anmelde- und Zurücksetz-Links, Brute-Force-Begrenzung je E-Mail- und IP-Kombination.

1.3 Zugriffskontrolle (Berechtigungen)

- Die Integrationsschnittstelle prüft je Aufruf die ausgestellte Berechtigung; jeder Zugriff wird mit Zeitpunkt, Ergebnis und betroffenem Datensatz protokolliert.
- Datenbankzugriffe nach dem Least-Privilege-Prinzip: Das Laufzeit-Credential der Anwendung besitzt keine Schemarechte (DDL); Migrationen laufen über ein getrenntes Credential in einem separaten, einmaligen Migrationsschritt. Ein versioniertes Prüfskript kontrolliert die Rechtevergabe fail-closed.
- Das Auditprotokoll ist ausschließlich anfügend; nachträgliche Änderungen sind durch Datenbankrechte ausgeschlossen.

1.4 Trennungskontrolle

- Strikte Silo-Trennung pro Kunde: Jeder Auftrag erzeugt ein eigenes Modell ausschließlich aus den Dokumenten dieses einen Kunden. Eine Vermischung von Trainingsdaten oder Modellen verschiedener Kunden ist im Ablauf nicht vorgesehen und durch auftragsgebundene Speicherpfade und auftragsgebundene Verschlüsselungskontexte technisch unterbunden.
- Für jeden Trainingsauftrag wird eine eigene, dedizierte GPU-Instanz erzeugt und nach Abschluss in jedem Ausgang (Erfolg, Fehler, Abbruch) zerstört; unverschlüsselte Zwischenstände auf der Instanz werden gelöscht.
- Die Website-Datenbank (Konten, Bestellungen, Zahlungsstatus) ist von der Verarbeitungs-Datenbank vollständig getrennt; Kundendokumente erreichen die Website-Ebene zu keinem Zeitpunkt (Upload erfolgt direkt in den Objektspeicher, siehe 2.1).

1.5 Pseudonymisierung und Datenminimierung

- Vor der Erzeugung von Trainingsdatensätzen durchläuft der extrahierte Text eine eigene PII-Filterstufe der Pipeline.
- Über die Integrationsschnittstelle sind ausschließlich minimierte Bestell-, Kunden- und Zustandsdaten abrufbar; hochgeladene Kundendokumente sind dort nicht erreichbar.
- Es werden keine Zahlungsmitteldaten (z. B. Kartennummern) gespeichert; Rechnungsstellung und Zahlungsabgleich laufen über die BuchhaltungsButler GmbH.

2.1 Weitergabekontrolle (Transport)

- Sämtliche externen Verbindungen sind transportverschlüsselt (TLS/HTTPS); in Produktion erzwingt die Anwendung HTTPS für öffentliche Basis- und Callback-URLs fail-closed.
- Der Dokumenten-Upload erfolgt über kurzlebige, vorsignierte Formulare (Gültigkeit 1 Stunde) direkt in den EU-Objektspeicher, ohne Transit über Anwendungsserver.

- Status-Rückmeldungen zwischen Verarbeitung und Website sind je Nachricht HMAC-SHA-256-signiert; Nachrichten mit ungültiger Signatur werden ohne Seiteneffekt verworfen. Callback-Ziele werden gegen eine Allowlist geprüft (Schutz vor SSRF), in Produktion ausschließlich HTTPS auf öffentliche Ziele.

2.2 Speicherverschlüsselung

- Artefakte im Objektspeicher (Korpus, Datensätze, Modellstände, Auslieferungspakete) werden anwendungsseitig mit AES-256-GCM verschlüsselt, im Envelope-Verfahren: je Artefakt ein eigener Datenschlüssel, der seinerseits mit dem Master-Key verschlüsselt abgelegt wird; das Format ist versioniert und an den Auftragskontext gebunden (kein Austausch zwischen Aufträgen).
- Der Master-Key wird getrennt von den verschlüsselten Artefakten verwahrt und unterliegt demselben Produktions-Härtetest wie alle Geheimnisse.

2.3 Eingabekontrolle

- Statusübergänge der Aufträge werden mit Zeitstempeln versioniert erfasst (monotone Ereignisfolge, Schutz gegen veraltete oder mehrdeutige Fakten).
- Zugriffe über die Integrationsschnittstelle werden mit Akteur, Aktion, Ressource und Ergebnis im ausschließlich anfügenden Auditprotokoll erfasst.
- Uploads werden vor der Annahme serverseitig validiert; abgewiesen wird, was den vereinbarten Rahmen sprengt.

3 Verfügbarkeit und Belastbarkeit

- Die Verarbeitung ist als kurzlebiger, wiederanlauffähiger Workflow orchestriert (Temporal); abgebrochene Läufe können deterministisch fortgesetzt oder kontrolliert als fehlgeschlagen abgeschlossen werden.
- Produktionscontainer laufen ohne Root-Rechte mit schreibgeschütztem Dateisystem, mit Healthchecks, Neustart-Richtlinien und Ressourcenlimits; Container-Images sind über Digests unveränderlich festgeschrieben und werden vor dem Ausrollen skriptgeprüft.
- Ein Abgleichsjob (Reconciliation) erkennt hängende Aufträge und verwaiste Ressourcen und führt sie nach.
- Datensicherung: Die beiden Datenbanken (Trainings-Pipeline und Website) werden per dokumentiertem pg_dump-Export gesichert; Artefakte im Objektspeicher liegen redundant bei Exoscale (Frankfurt am Main) vor. Der Master-Key wird getrennt von beiden Sicherungen aufbewahrt, sodass ein einzelner kompromittierter Bestandteil allein nicht zur Entschlüsselung ausreicht.
- Da Kundendaten nur für die Dauer der Fertigung vorgehalten werden (siehe 4.2), ist der Schaden eines Totalverlusts strukturell begrenzt: Der Kunde besitzt die Quelldokumente, IonKon kann die Fertigung wiederholen.

4.1 Entwicklungs- und Änderungsprozess

Diese TOM werden mindestens einmal jährlich sowie bei wesentlichen Änderungen der Verarbeitung durch die Geschäftsführung überprüft und bei Bedarf fortgeschrieben.

- Änderungen laufen über Versionskontrolle mit Continuous Integration: automatisierte Tests (Web und Backend), statische Analysen und ein Secret-Scanner (Gitleaks) vor jeder Zusammenführung.
- Sicherheitsrelevante Konfiguration ist fail-closed voreingestellt; Test- und Entwicklungsschalter sind in Produktion technisch wirkungslos (doppelte Guards gegen Fehlkonfiguration).
- Adversariale Sicherheitsprüfungen (Red-Team-Durchläufe) werden anlassbezogen durchgeführt und ihre Befunde nachweisbar behoben.

4.2 Löschkonzept

- Trainingsdaten und eigene Modellkopien werden nach Empfangsbestätigung der Lieferung gelöscht; bestätigt der Kunde trotz zweier Erinnerungen nicht, greift die vertragliche Zugangsfiction und die Löschung erfolgt zu diesem Zeitpunkt. Sobald die Löschung erfolgt ist, wird automatisch ein Löschnachweis erteilt.
- Unabhängig davon gilt eine technische Aufbewahrungsobergrenze (Standard 30 Tage ab Bereitstellung, absolute Obergrenze 180 Tage ab Auftragsbeginn), nach deren Ablauf Artefakte automatisch bereinigt werden.
- Kontaktanfragen werden spätestens nach 365 Tagen automatisch gelöscht; die Löschung eines Kundenkontos entfernt kaskadierend alle zugehörigen personenbezogenen Datensätze der Website-Ebene.

4.3 Auftragskontrolle (Subauftragsverarbeiter)

- Vollständiges Verzeichnis der Subauftragsverarbeiter, jeweils mit Auftragsverarbeitungsvertrag: STRATO GmbH (Deutschland), Betrieb des Webserver und der Datenbank; DataCrunch Oy, Cloud-Marke „Verda“ (Finnland), GPU-Rechenleistung für Training und Datensynthese; Akenes SA, Marke „Exoscale“ (Schweiz), Objektspeicher in Frankfurt am Main sowie GPU-Rechenleistung für Training und Datensynthese in Frankfurt, Zagreb oder Zürich je nach verfügbarer Kapazität; Hetzner Online GmbH (Deutschland), nur bei gebuchtem Hosting der Server des Kunden in Deutschland oder Finnland; BuchhaltungsButler GmbH (Deutschland), Rechnungsstellung und Zahlungsabgleich. Verarbeitung von Kundendokumenten findet ausschließlich in der EU oder der Schweiz statt. Ein externer KI-Anbieter wird nicht eingesetzt; die inhaltliche Verarbeitung läuft ausschließlich auf der für den Auftrag bereitgestellten Instanz.
- Weisungsrechte, Kontrollrechte und Meldewege bei Datenschutzvorfällen regelt der AVV (Nummer 9): IonKon meldet eine Verletzung des Schutzes personenbezogener Daten dem Kunden unverzüglich, spätestens 48 Stunden nach Kenntniserlangung, über die Kontaktadresse info@ionkon.de.