Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

Verantwortlicher **– Auftraggeber –**	**Beispielstadt** Kreisverband Beispielstadt Rotkreuzstraße 1 80000 Beispielstadt Vertreten durch: Maria Mustermann, Vorsitzende Ansprechpartner Datenschutz: nicht benannt
Auftragsverarbeiter **– Auftragnehmer –**	**IT-Meindl** · Inhaber Tobias Meindl Germanenweg 2 85774 Unterföhring info@it-meindl.de

§ 1 Gegenstand und Dauer

(1) Der Auftragnehmer stellt dem Auftraggeber das *Digitale Wachbuch* als webbasierte Anwendung zur Verfügung und betreibt für ihn eine eigene Instanz. Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten, die der Auftragnehmer dabei im Auftrag vornimmt.

(2) Art, Umfang und Zweck der Verarbeitung, die Arten der Daten und die Kategorien betroffener Personen ergeben sich aus **Anlage 1**.

(3) Der Vertrag beginnt mit der Bereitstellung der Instanz und läuft, solange der zugrunde liegende Nutzungsvertrag besteht. Er endet mit diesem, ohne dass es einer gesonderten Kündigung bedarf. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt; ein wichtiger Grund liegt insbesondere vor, wenn der Auftragnehmer wesentliche Pflichten aus diesem Vertrag verletzt.

(4) Dieser Vertrag geht dem Nutzungsvertrag vor, soweit er Regelungen zur Verarbeitung personenbezogener Daten trifft.

§ 2 Weisungsrecht

(1) Der Auftragnehmer verarbeitet personenbezogene Daten **ausschließlich auf dokumentierte Weisung** des Auftraggebers. Das gilt auch für die Übermittlung in ein Drittland; eine solche findet nach derzeitigem Stand nicht statt (siehe Anlage 3).

(2) Die Einstellungen, die der Auftraggeber in der Anwendung vornimmt, gelten als Weisung. Weitergehende Weisungen erteilt er in Textform an info@it-meindl.de. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Weisungsbefugt sind die vom Auftraggeber als Voll-Administratoren benannten Personen sowie die oben genannte Vertretung.

(4) Hält der Auftragnehmer eine Weisung für rechtswidrig, **teilt er dies dem Auftraggeber unverzüglich mit**. Er ist berechtigt, die Ausführung auszusetzen, bis der Auftraggeber die Weisung bestätigt oder ändert.

(5) Der Auftragnehmer weist den Auftraggeber darauf hin, wenn dessen Weisungen oder Einstellungen aus seiner Sicht zu einem Datenschutzrisiko führen. Eine Rechtsberatung schuldet er nicht.

§ 3 Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für die Rechtsgrundlage und die Information der betroffenen Personen.

(2) Er legt die Aufbewahrungsdauer der in seiner Instanz gespeicherten Daten fest und veranlasst deren Löschung, soweit die Anwendung ihm dies ermöglicht.

(3) Er benennt dem Auftragnehmer die Personen, die Administratorenrechte erhalten, und entzieht diese unverzüglich, wenn die Voraussetzungen entfallen.

(4) Er informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

§ 4 Vertraulichkeit

(1) Der Auftragnehmer verarbeitet die Daten vertraulich und stellt sicher, dass sich alle Personen, die Zugang zu ihnen haben, zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Die Verpflichtung besteht auch nach Beendigung dieses Vertrags fort.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die nach Art. 32 DSGVO erforderlichen Maßnahmen. Sie sind in **Anlage 2** beschrieben.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf sie anpassen, **darf das Schutzniveau dabei aber nicht unterschreiten**. Wesentliche Änderungen dokumentiert er und teilt sie dem Auftraggeber mit.

(3) Anlage 2 benennt auch Punkte, an denen das Schutzniveau derzeit hinter dem Zielzustand zurückbleibt, samt geplanter Abhilfe. Der Auftraggeber kann so beurteilen, ob die Maßnahmen für seine Verarbeitung angemessen sind.

§ 6 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt die **allgemeine schriftliche Genehmigung** zum Einsatz weiterer Auftragsverarbeiter. Die derzeit eingesetzten sind in **Anlage 3** aufgeführt.

(2) Beabsichtigt der Auftragnehmer, einen weiteren Unterauftragsverarbeiter hinzuzuziehen oder zu ersetzen, teilt er dies dem Auftraggeber **mindestens vier Wochen vorher** in Textform mit. Der Auftraggeber kann innerhalb von zwei Wochen nach Zugang aus wichtigem datenschutzrechtlichem Grund widersprechen.

(3) Widerspricht der Auftraggeber und lässt sich keine Einigung erzielen, steht ihm ein **Sonderkündigungsrecht** zum Zeitpunkt der beabsichtigten Änderung zu.

(4) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die den Pflichten aus diesem Vertrag entsprechen. Er haftet für dessen Verhalten wie für eigenes.

(5) Nicht als Unterauftragsverarbeitung gelten Nebenleistungen, bei denen kein Zugriff auf personenbezogene Daten des Auftraggebers vorgesehen ist, etwa Telekommunikationsleistungen oder Wartung von Endgeräten.

§ 7 Unterstützung bei Betroffenenrechten

(1) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet er die Anfrage unverzüglich an den Auftraggeber weiter und beantwortet sie nicht selbst.

(2) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Auskunfts-, Berichtigungs-, Löschungs-, Einschränkungs- und Übertragbarkeitsansprüchen (Art. 12–23 DSGVO).

(3) Die Anwendung stellt dem Auftraggeber hierfür Funktionen bereit, mit denen er die Ansprüche **selbst** erfüllen kann: einen Datenexport je Mitglied, das Bearbeiten und Löschen von Mitgliederdaten sowie Ausdrucke und Exporte der Dokumentation. Ist eine Unterstützung darüber hinaus erforderlich, erbringt der Auftragnehmer sie ohne gesonderte Vergütung.

§ 8 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten **unverzüglich, spätestens jedoch 48 Stunden** nach Kenntniserlangung in Textform. Die Frist ist kürzer als die Meldefrist des Auftraggebers gegenüber der Aufsichtsbehörde (72 Stunden, Art. 33 Abs. 1 DSGVO), damit diesem Zeit zum Handeln bleibt.

(2) Die Meldung enthält, soweit bekannt: Art der Verletzung, betroffene Datenkategorien, ungefähre Zahl betroffener Personen und Datensätze, wahrscheinliche Folgen sowie ergriffene und vorgeschlagene Maßnahmen.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei dessen Pflichten nach Art. 32 bis 36 DSGVO, einschließlich einer etwaigen Datenschutz-Folgenabschätzung.

§ 9 Nachweise und Kontrollrechte

(1) Der Auftragnehmer weist die Einhaltung der Pflichten aus diesem Vertrag auf Anfrage nach, insbesondere durch diesen Vertrag samt Anlagen und eine Selbstauskunft zu den Maßnahmen aus Anlage 2.

(2) Reichen diese Nachweise im Einzelfall nicht aus, kann der Auftraggeber die Verarbeitung **nach Ankündigung mit einer Frist von vier Wochen** zu den üblichen Geschäftszeiten überprüfen oder durch einen zur Verschwiegenheit verpflichteten Prüfer überprüfen lassen. Die Prüfung darf den Betrieb nicht unangemessen beeinträchtigen.

(3) Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die zum Nachweis der Einhaltung von Art. 28 DSGVO erforderlich sind.

§ 10 Löschung und Rückgabe nach Beendigung

(1) Der Auftraggeber entscheidet, ob die Daten nach Vertragsende **gelöscht oder zurückgegeben** werden. Er teilt seine Wahl **spätestens zum Vertragsende** in Textform mit. Trifft er keine Wahl, werden die Daten gelöscht.

(2) Wählt er die Rückgabe, stellt der Auftragnehmer ihm **innerhalb von 14 Tagen** einen Auszug der Instanzdatenbank in einem gängigen Format bereit.

(3) Unabhängig davon kann der Auftraggeber die für ihn wesentlichen Daten **während der Vertragslaufzeit jederzeit selbst ausleiten** – über den Mitgliederexport, die Wachtags-PDFs, die Statistikausdrucke und den Datenexport je Mitglied. Der Auftragnehmer empfiehlt, davon vor Vertragsende Gebrauch zu machen.

(4) Der Auftragnehmer löscht die Instanz und alle Kopien **spätestens 120 Tage nach Vertragsende**. Die Frist trägt dem Umstand Rechnung, dass Sicherungskopien turnusmäßig überschrieben werden. Die Löschung wird auf Anforderung bestätigt.

(5) Von der Löschung ausgenommen sind Daten, für die eine gesetzliche Aufbewahrungspflicht besteht. Sie werden für die Dauer der Aufbewahrung gesperrt und nicht weiter verarbeitet.

§ 11 Haftung

(1) Es gilt Art. 82 DSGVO.

(2) Im Innenverhältnis haftet der Auftragnehmer für Schäden, die durch eine von ihm zu vertretende Verletzung dieses Vertrags entstehen.

§ 12 Schlussbestimmungen

(1) Änderungen und Ergänzungen bedürfen der Textform. Das gilt auch für die Abbedingung dieses Formerfordernisses.

(2) Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen unberührt. An die Stelle der unwirksamen Bestimmung tritt, was ihrem wirtschaftlichen Zweck am nächsten kommt.

(3) Es gilt deutsches Recht.

(4) Bestandteil dieses Vertrags sind Anlage 1 (Gegenstand der Verarbeitung), Anlage 2 (Technische und organisatorische Maßnahmen) und Anlage 3 (Unterauftragsverarbeiter).

ENTWURF – noch nicht angenommen. Dieses Dokument wird erst mit der Annahme im Wachbuch verbindlich.

Fassung 1.0 vom 25.08.2026

Anlage 1 – Gegenstand der Verarbeitung

1. Gegenstand

Betrieb des *Digitalen Wachbuchs* als webbasierte Anwendung für den Wasserrettungsdienst. Der Auftraggeber erhält eine eigene Instanz unter einer eigenen Adresse mit eigener Datenbank.

2. Art und Zweck der Verarbeitung

Erhebung, Speicherung, Veränderung, Auslesen, Verwendung und Löschung personenbezogener Daten zum Zweck der

- Planung und Dokumentation von Wachdiensten,
- Erfassung von Anwesenheiten und Qualifikationen der Einsatzkräfte,
- Dokumentation von Einsätzen und Erste-Hilfe-Leistungen,
- Verwaltung von Ausstattung, Fahrzeugen und Bekleidung,
- Führung einer Vertrauenskasse für Getränke (optional),
- statistischen Auswertung für Jahresberichte und Dienstplanung.

Der Auftragnehmer verarbeitet die Daten nicht zu eigenen Zwecken.

3. Kategorien betroffener Personen

Kategorie	Erläuterung
Mitglieder der Ortsgruppe	Einsatzkräfte, die Dienst leisten
Administratoren	Mitglieder mit Verwaltungsrechten
Hilfeleistungsempfänger	Personen, denen Erste Hilfe geleistet wurde – **ohne Namensnennung**, siehe Ziffer 5
Nutzer der Getränkekasse	sofern das Modul eingesetzt wird
Externe Kontaktpersonen	Empfänger hinterlegter Telefonnummern und E-Mail-Adressen

4. Arten der verarbeiteten Daten

Stammdaten: Vor- und Nachname, Geburtsdatum, Mitgliedsnummer, E-Mail-Adressen, Telefonnummern, Qualifikationen und Ausbildungen, Einwilligungs- und Benachrichtigungseinstellungen.

Zugangsdaten: Passwort (nur als kryptografischer Hash), Geheimnis der Zwei-Faktor-Authentifizierung, Wiederherstellungscodes (nur als Hash), Berechtigungen.

Tätigkeits- und Dienstdaten: An- und Abmeldezeiten mit Funktion und Wachstation, Kommentare, Einsatzbeteiligungen einschließlich Bootsführer, Fahrer, Taucher und Tauchtiefe, Sanitätsdienste, Einträge im Flaschenfüllbuch, Ausleihen, Bekleidungsausgaben, Unterschrift der Wachleitung zum Abschluss eines Wachtags.

Gesundheitsdaten nach Art. 9 DSGVO: Aus der Dokumentation von Erste-Hilfe-Leistungen: Geschlecht, Alter, Schilderung des Geschehens, durchgeführte Maßnahmen, Verdachtsdiagnose, Medikation, Vitalwerte (Blutdruck, Herzfrequenz, Blutzucker), Art der Weiterbehandlung. Ergänzend Freitexte aus Einsatzberichten.

Finanz- und Konsumdaten (nur bei Einsatz der Getränkekasse): Buchungen mit Zeitpunkt, Produkt, Betrag, Kontostand und erfassender Person, Aufladungen, Stornos, Inventuren.

Technische Protokolldaten: IP-Adresse und Browserkennung registrierter Stationsgeräte, Protokoll der Gerätevorgänge, fehlgeschlagene Anmeldeversuche mit IP-Adresse und Benutzername, letzte Nutzung von API-Schlüsseln.

5. Besonderheit: Erste-Hilfe-Dokumentation ohne Namen

> Die Anwendung erhebt **keine Namen der Personen, denen Erste Hilfe geleistet wurde**. Erfasst werden ausschließlich Geschlecht, Alter und der medizinische Befund. Das Wachbuch ist damit **kein Patientenprotokoll** und ersetzt in Bayern auch keines.

Der Auftraggeber bleibt gehalten, in den Freitextfeldern keine Angaben zu machen, die eine Identifizierung ermöglichen.

6. Ort der Verarbeitung

Ausschließlich in der Bundesrepublik Deutschland. Eine Übermittlung in Drittländer findet nicht statt.

7. Dauer der Verarbeitung

Für die Dauer des Nutzungsvertrags. Die Aufbewahrungsdauer der einzelnen Datenbestände legt der Auftraggeber als Verantwortlicher fest; zu beachten sind dabei gesetzliche Aufbewahrungspflichten, insbesondere für Kassenaufzeichnungen der Getränkekasse. Zur Löschung nach Vertragsende siehe § 10.

Anlage 2 – Technische und organisatorische Maßnahmen

Maßnahmen nach Art. 32 DSGVO

1. Vertraulichkeit

Zutrittskontrolle. Der Betrieb erfolgt in einem nach ISO 27001 zertifizierten Rechenzentrum der Klasse Tier 3+ in Frankfurt am Main. Zutrittsschutz, Videoüberwachung und Besucherverwaltung obliegen dem Rechenzentrumsbetreiber (siehe Anlage 3). Der Auftragnehmer selbst betreibt keine Server, auf denen Daten des Auftraggebers liegen.

Zugangskontrolle.

- **Zugang nur über registrierte Stationsgeräte.** Die Anwendung öffnet sich nicht für beliebige Browser. Ein Gerät muss durch einen Voll-Administrator freigeschaltet werden; die Freischaltung ist zeitlich befristet und läuft ohne Verlängerung ab. Verlorene Geräte lassen sich sofort entziehen.
- **Zwei-Faktor-Authentifizierung** (TOTP) für Verwaltungszugänge. Für Voll-Administratoren verpflichtend, nicht abwählbar.
- **Passwörter** werden ausschließlich als kryptografischer Hash mit erhöhtem Kostenfaktor gespeichert. Eine Rückrechnung ist nicht möglich.
- **Begrenzung von Anmeldeversuchen** je IP-Adresse und Benutzername.
- **Optionale Anmeldung über BRK.ID**, sofern der Verband dies anbietet.
- **Automatische Abmeldung** inaktiver Verwaltungssitzungen.

Zugriffskontrolle. Berechtigungen werden je Bereich vergeben; die Rolle allein öffnet nichts. Wer die Bekleidung verwaltet, erhält keinen Zugriff auf die Erste-Hilfe-Dokumentation. API-Schlüssel werden nur als Hash gespeichert, erben die Rechte ihres Besitzers und verlieren einen entzogenen Bereich sofort mit. Zustandsändernde Formulare sind gegen Cross-Site Request Forgery geschützt, API-Aufrufe zusätzlich durch eine Herkunftsprüfung. Der Auftragnehmer greift auf Daten des Auftraggebers nur zu, soweit dies zur Störungsbeseitigung erforderlich ist.

Trennungskontrolle. Jede Ortsgruppe erhält eine eigene Instanz mit eigener Datenbank unter eigener Adresse. Es gibt keine gemeinsame Datenhaltung mehrerer Auftraggeber und damit keine Mandantentrennung, die durch einen Programmfehler aufgehoben werden könnte.

Pseudonymisierung. Die Dokumentation von Erste-Hilfe-Leistungen erfolgt ohne Namen der betroffenen Personen (siehe Anlage 1 Ziffer 5).

2. Integrität

Weitergabekontrolle. Übertragung ausschließlich über HTTPS; unverschlüsselte Verbindungen werden umgeleitet und über HSTS dauerhaft ausgeschlossen. Gesetzte Sicherheitsheader: X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Strict-Transport-Security. Konfigurationsdateien mit Zugangsdaten und interne Verzeichnisse sind über den Webserver nicht abrufbar. Der E-Mail-Versand erfolgt über einen SMTP-Server mit Transportverschlüsselung; der Auftraggeber kann einen eigenen Server hinterlegen.

Eingabekontrolle. Datenbankzugriffe ausschließlich über parametrisierte Abfragen. Änderungen an Mitgliederdaten und Wachtagen tragen einen Zeitstempel. Vorgänge an Stationsgeräten werden protokolliert und nach 180 Tagen automatisch gelöscht. Ein abgeschlossener und unterschriebener Wachtag ist gegen Änderungen gesperrt; zum Abschluss entsteht ein PDF für die revisionssichere Ablage.

3. Verfügbarkeit und Belastbarkeit

- Regelmäßige Sicherungen der Produktivinstanzen durch den Rechenzentrumsbetreiber.
- Das PDF-Archiv abgeschlossener Wachtage liegt in einem über den Webserver gesperrten Verzeichnis

und ist Teil der Sicherung.
- Updates werden zentral verteilt; vor jedem Update wird eine Sicherung angelegt.
- Testinstanzen sind ausgenommen: Sie werden weder gesichert noch automatisch aktualisiert. Personenbezogene Daten dürfen dort nicht gespeichert werden.

4. Verfahren zur Überprüfung und Bewertung

- Automatisierte Prüfungen bei jeder Änderung am Quellcode: statische Analyse, Unit-Tests sowie Integrations- und End-to-End-Tests gegen eine echte Datenbank, ergänzt um Prüfungen auf bekannte Schwachstellen und versehentlich eingecheckte Geheimnisse.
- Gezielte Zugriffsschutz-Tests, jeweils mit Gegenprobe, damit ein entfernter Endpunkt nicht als bestandener Test durchgeht.
- Fehler- und Ereignisüberwachung über eine selbst betriebene Instanz; keine Übermittlung an einen externen Dienst.
- Unterauftragsverarbeiter werden vertraglich verpflichtet (§ 6).

5. Offen ausgewiesene Punkte

Der Auftragnehmer benennt die folgenden Punkte ausdrücklich, damit der Auftraggeber die Angemessenheit der Maßnahmen für seine Verarbeitung beurteilen kann.

Punkt	Stand	Geplante Abhilfe
Aufbewahrungsfristen	Automatisch gelöscht werden derzeit nur Anmeldeversuche (nach einer Stunde) und das Geräteprotokoll (nach 180 Tagen). Dienst-, Einsatz-, Erste-Hilfe- und Buchungsdaten bleiben bis zur Löschung durch den Auftraggeber erhalten.	Einstellbare Aufbewahrungsfristen je Datenbestand mit automatischer Löschung
Zwischendateien für Exporte	CSV- und PDF-Exporte werden kurzzeitig im Anwendungsverzeichnis abgelegt und nach 60 Sekunden gelöscht. Der Dateiname ist in dieser Zeitspanne vorhersehbar.	Auslieferung direkt über den Download ohne Zwischendatei
Geheimnis der Zwei-Faktor-Authentifizierung	Wird unverschlüsselt in der Datenbank gespeichert. Ein Hash scheidet aus, weil der Wert zur Berechnung des Codes zurücklesbar sein muss.	Verschlüsselung mit einem Schlüssel außerhalb der Datenbank

Diese Anlage wird fortgeschrieben. Behobene Punkte entfallen mit der jeweils nächsten Fassung.

Anlage 3 – Unterauftragsverarbeiter

Der Auftraggeber genehmigt den Einsatz der nachfolgend aufgeführten weiteren Auftragsverarbeiter. Für Änderungen gilt das Verfahren aus § 6: Ankündigung mindestens vier Wochen vorher, Widerspruchsrecht, Sonderkündigungsrecht.

Firma	TrafficPlex GmbH (Marke *lima-city*)
Anschrift	Konsul-Smidt-Str. 90, 28217 Bremen, Deutschland
Leistung	Bereitstellung und Betrieb der Serverinfrastruktur, Datenbank, Dateispeicher, Sicherungen sowie des Standard-SMTP-Servers für den E-Mail-Versand
Verarbeitungsort	Deutschland
Datenkategorien	Sämtliche in Anlage 1 genannten Daten, soweit sie gespeichert oder per E-Mail versandt werden
Grundlage	Auftragsverarbeitungsvertrag zwischen dem Auftragnehmer und der TrafficPlex GmbH

Eine Übermittlung personenbezogener Daten in ein Drittland findet nicht statt.

Keine Unterauftragsverarbeiter

Die folgenden Beteiligten werden ausdrücklich genannt, weil die Frage regelmäßig aufkommt. Sie sind **keine** Unterauftragsverarbeiter des Auftragnehmers.

Eigener SMTP-Server des Auftraggebers. Hinterlegt der Auftraggeber in den Einstellungen einen eigenen Mailserver, versendet die Anwendung ausschließlich über diesen. Dessen Betreiber ist dann Auftragsverarbeiter des Auftraggebers, nicht des Auftragnehmers – der Auftraggeber schließt den erforderlichen Vertrag selbst ab. Ohne eigene Hinterlegung wird der Standard-SMTP-Server verwendet; dieser läuft bei der oben genannten TrafficPlex GmbH.

BRK.ID. Aktiviert der Auftraggeber die Anmeldung über BRK.ID, ist der Betreiber des Anmeldedienstes eigenständig Verantwortlicher. Die Anwendung übermittelt keine personenbezogenen Daten dorthin; zum Austausch des Anmeldetokens werden lediglich technische Werte übertragen, und zurück erhält die Anwendung die Mitgliedsnummer sowie die vom Verband bereitgestellten Profilangaben. Die Weiterleitung zum Anmeldedienst führt der Browser der sich anmeldenden Person aus – dabei erfährt der Anmeldedienst deren IP-Adresse, ebenso wie bei jeder anderen Anmeldung am Verbandssystem.

Fehler- und Ereignisüberwachung. Die Überwachung läuft auf einer vom Auftragnehmer selbst betriebenen Instanz innerhalb der oben genannten Infrastruktur. Es findet keine Übermittlung an einen externen Dienstleister statt.

Störungsmeldungen an den Auftragnehmer. Schlägt der E-Mail-Versand fehl, erhält der Auftragnehmer eine technische Störungsmeldung mit Name der Ortsgruppe, Betreff und Fehlermeldung des Mailservers. Der Inhalt der Nachricht wird dabei nicht übertragen. Die Meldung dient ausschließlich der Störungsbeseitigung im Rahmen dieses Vertrags.