Datenschutzinformation für Kunden und Ansprechpartner

ETN Internet GmbH & Co. KG · für die Marken SURFN., SURFN.BUSINESS und SURFN.COMPANY · Fassung 1.0 · Stand 17.10.2026

1. Verantwortliche und Datenschutzkontakt

Verantwortlich ist die **ETN Internet GmbH & Co. KG**, An der Haarbrücke 4, 49716 Meppen, Amtsgericht Osnabrück HRA 203268. Persönlich haftende Gesellschafterin ist die ETN Verwaltungs GmbH (Amtsgericht Osnabrück HRB 206393), vertreten durch ihren Geschäftsführer Sebastian Hoogland.

Telefon: +49 5931 99880 · E-Mail: info@surfn.de

Datenschutzbeauftragter ist **Volker Wassermann, bridge4IT GmbH**. Datenschutzanfragen richten Sie an datenschutz@etn.group. Vertrauliche Post an den Datenschutzbeauftragten richten Sie unmittelbar an bridge4IT GmbH, zu Händen Volker Wassermann – persönlich/vertraulich, Nordring 102, 47661 Issum.

Diese Information betrifft Angebote, Verträge, Anschluss und Betrieb sowie die Kundenbetreuung für die oben genannten Marken. Für Websitebesuche gilt die Datenschutzerklärung auf etn.group.

2. Daten, Zwecke und Rechtsgrundlagen

Wir verarbeiten nur die für den jeweiligen Vorgang benötigten Angaben, insbesondere: - Namen, Anschrift und Kontaktdaten, bei Organisationen auch Funktionen und Vertretungsangaben; - Kunden- und Vertragsnummern, Anschlussadresse und gebuchte Tarife; - technische Anschlussdaten (zugeteilte IP-Adressen, Kennungen der Endgeräte und Antennen, Rufnummern); - Kommunikationsinhalte mit uns, Abrechnungs- und Zahlungsangaben; - Verkehrsdaten, soweit sie für Abrechnung, Störungsbeseitigung und Sicherheit erforderlich sind.

Vorgang	Zweck und Rechtsgrundlage
Verfügbarkeitsprüfung, Angebot, Vertragsschluss und -verwaltung	Art. 6 Abs. 1 Buchst. b DSGVO; bei Ansprechpartnern einer Organisation Buchst. f (Interesse an der Geschäftsbeziehung).
Bereitstellung des Anschlusses (Installation, Antenne, Portierung, Anbieterwechsel)	Buchst. b; für Anbieterwechsel und Rufnummernmitnahme zusätzlich Buchst. c mit § 59 TKG.
Bestandsdaten des Telekommunikationsvertrags	§ 172 TKG in Verbindung mit Buchst. b und c.
Verkehrsdaten (z. B. Verbindungsdaten bei Telefonie, Zuordnung von IP-Adressen)	Nur im Rahmen der §§ 9 bis 12 TDDDG: Entgeltermittlung und -abrechnung, Störungserkennung und -beseitigung, Missbrauchsabwehr.
Einzelverbindungsnachweis	Nur auf Ihren Wunsch, § 11 TDDDG.
Notruf	Übermittlung von Rufnummer und Standort an die Notrufabfragestelle, § 164 TKG; Buchst. c.
Störungsannahme und Support	Buchst. b, bei Ansprechpartnern Buchst. f; Entstörung nach § 58 TKG (Buchst. c).
Kontakt per WhatsApp und SMS	Buchst. b, wenn Ihr Anliegen einen Vertrag betrifft, sonst Buchst. f (Beantwortung Ihrer Anfrage). Einzelheiten unten.
Rechnungen und Zahlungen (SEPA-Lastschrift, Überweisung)	Buchst. b; Aufbewahrungspflichten nach Buchst. c.
Abgleich offener Forderungen innerhalb der ETN-Gruppe vor Vertragsschluss und bei Zahlungsverzug; Vorauskasse statt Auskunftei	Buchst. f (Vermeidung von Zahlungsausfällen), Prüfung durch einen Mitarbeiter; **keine** Abfrage bei Auskunfteien.
Elektronischer Vertragsschluss (paperless)	Buchst. b bzw. f (verlässlicher Vertragsschluss, Beweissicherung).
Netz- und Informationssicherheit, Behandlung von Sicherheitsvorfällen	Buchst. c mit §§ 165, 168 TKG; Buchst. f.
Bearbeitung von Sicherheitsmeldungen (z. B. BSI/CERT-Bund) und Information betroffener Kunden	Buchst. c mit § 169 Abs. 4 bis 6 TKG und § 12 TDDDG; Buchst. f (Schutz des Netzes und anderer Nutzer). Einzelheiten unten.
Nachrichten an einzelne Mitarbeiterinnen und Mitarbeiter	Buchst. b, wenn Ihr Anliegen einen Vertrag betrifft, sonst Buchst. f (Bearbeitung Ihres Anliegens). Einzelheiten unten.
Auskünfte an Behörden	Nur bei gesetzlicher Pflicht, §§ 173 bis 177 TKG; Buchst. c.
Information über eigene ähnliche Leistungen	E-Mail an Bestandskunden nach § 7 Abs. 3 UWG; Buchst. f. Widerspruch jederzeit möglich.
Rechtsansprüche	Buchst. f.

Kontakt per WhatsApp und SMS (SURFN. für Privatkunden und kleine Geschäftskunden). Wenn Sie uns über WhatsApp oder per SMS an +49 5931 9989699 schreiben, verarbeiten wir Ihre Mobilnummer, Ihren Profilnamen, den Inhalt Ihrer Nachrichten und angehängte Dateien sowie Zeitpunkte und Zustellstatus. Wir verwenden diese Angaben, um Ihr Anliegen zu bearbeiten, und ordnen sie Ihrem Kundenkonto zu, wenn die Nummer dort hinterlegt ist. Die Nutzung ist freiwillig; Sie erreichen uns ebenso per E-Mail oder Telefon. Über diese Kanäle schicken wir Ihnen keine Werbung ohne Ihre Einwilligung. Die Nachrichten speichern wir wie andere Supportvorgänge (Ziffer 6). Für Ihre Nutzung von WhatsApp selbst ist WhatsApp verantwortlich; es gilt dessen Datenschutzrichtlinie.

Sicherheitsmeldungen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI, CERT-Bund) und vergleichbare Stellen teilen uns mit, wenn von einer IP-Adresse in unserem Netz eine Gefahr ausgeht, etwa durch ein mit Schadsoftware infiziertes Gerät oder einen missbrauchbar offenen Dienst. Die Meldung enthält IP-Adresse, Zeitpunkt, Art der Gefahr und technische Verbindungsangaben. Wir ordnen die IP-Adresse anhand unserer Zuordnungsdaten (Ziffer 6) Ihrem Anschluss zu, informieren Sie und weisen auf Möglichkeiten zur Beseitigung hin. Besteht die Gefahr fort, können wir Ihren Internetverkehr auf eine Hinweisseite umleiten oder die Nutzung einschränken, bis die Ursache beseitigt ist (§ 169 Abs. 6 TKG). Je Vorfall halten wir fest, wann was gemeldet wurde, wann wir Sie informiert haben und welcher Stand erreicht ist, damit wir wiederholte Meldungen erkennen. Diese Angaben stammen nicht von Ihnen, sondern von der meldenden Stelle (Art. 14 DSGVO).

Nachrichten an einzelne Mitarbeiterinnen und Mitarbeiter. Schreiben Sie einer Mitarbeiterin oder einem Mitarbeiter direkt an die persönliche dienstliche Adresse, kann diese Person Ihre Nachricht in unserem Kundenverwaltungssystem Ihrem Vorgang zuordnen, zum Beispiel einer Störung, einem Auftrag oder Ihrer Kundenakte. Die Zuordnung erfolgt von Hand, nicht automatisch. Zugeordnete Nachrichten sehen die Kolleginnen und Kollegen, die den Vorgang bearbeiten. Wir speichern sie wie andere Supportvorgänge (Ziffer 6).

Die Daten stammen von Ihnen, Ihrer Organisation oder aus der Leistungserbringung, bei Sicherheitsmeldungen von der meldenden Stelle. Bei Portierung und Anbieterwechsel erhalten wir Angaben vom abgebenden Anbieter.

3. Netzbetrieb und Inhalte

Einträge in öffentliche Teilnehmerverzeichnisse und Auskunftsdienste bieten wir nicht an.

Wir sehen keine Inhalte Ihrer Kommunikation ein. Das Fernmeldegeheimnis nach § 3 TDDDG gilt für alle Beschäftigten und Dienstleister.

Zur Sicherung des Netzbetriebs werten wir technische Betriebsdaten unserer Netzknoten aus, etwa Erreichbarkeit, Auslastung und Fehlermeldungen. Kundenbezogen geschieht das nur, soweit es für die Störungsbeseitigung nötig ist.

4. Empfänger

Wir geben Daten nur weiter, soweit dies für die genannten Zwecke erforderlich ist: - **Dienstleister**, die in unserem Auftrag tätig sind (Art. 28 DSGVO, siehe Tabelle); - die **Vision Networks GmbH**, Meppen, die für uns Support und Entstörung leistet, als Auftragsverarbeiterin; - **Vorleister und Netzbetreiber**, soweit für Verbindungen, Zusammenschaltung, Portierung oder die Bereitstellung über fremde Netze nötig: - BT als Vorleister für Sprachverbindungen, - IDT für Verbindungen ins Ausland, - vitroconnect GmbH für Anschlüsse über Vorleistungsnetze (Anschrift und Anschlussdaten); - Kreditinstitute für den Zahlungsverkehr; - Behörden, soweit gesetzlich verpflichtet.

Dienst	Zweck	Ort und Grundlage
Eigene Systeme (CRM, Abrechnung, Sprachplattform)	Vertragsverwaltung, Abrechnung, Vermittlung	eigene Server in Meppen und in angemieteten Rechenzentrumsflächen in Düsseldorf; der Flächenvermieter hat keinen Zugriff auf Systeme und Daten
netcup GmbH, Karlsruhe	Server für die Netzüberwachung (Gerätedaten, IP- und MAC-Adressen)	Rechenzentren in Nürnberg (Deutschland) und Wien (Österreich, EU)
HaloPSA (über NinjaOne, LLC, USA)	Störungs- und Supportfälle	Speicherung in Deutschland (Frankfurt); Zugriffe aus den USA: EU-US-Datenschutzrahmen bzw. Standardvertragsklauseln
Microsoft (Microsoft Ireland Operations Ltd.)	E-Mail, Dokumente	EU; Supportzugriffe aus Drittländern: EU-US-Datenschutzrahmen bzw. Standardvertragsklauseln
Hornetsecurity GmbH, Hannover	E-Mail-Filterung	Deutschland
Paperless GmbH, Frankfurt am Main	elektronische Unterzeichnung	Deutschland
Cloudflare, Inc. (USA)	Zugriffsschutz für CRM, Kundenportal und Website	USA; EU-US-Datenschutzrahmen bzw. Standardvertragsklauseln
Twilio Ireland Limited, Dublin, mit Twilio Inc. (USA) – über die Vision Networks GmbH als weiterer Auftragsverarbeiter	Anbindung von WhatsApp und SMS an unser Kundensystem	EU und USA: EU-US-Datenschutzrahmen bzw. Standardvertragsklauseln
Meta Platforms Ireland Limited, Dublin – WhatsApp Business Platform; das Konto hält die ETN Holding GmbH, Meppen, für die Vision Networks GmbH	Übermittlung von WhatsApp-Nachrichten	EU; Weitergabe an Meta Platforms, Inc. (USA) nach den Übermittlungsregeln von Meta (Art. 44 ff. DSGVO)
Anthropic, PBC, San Francisco (USA) – Claude, Team-Konto mit Datenschutzvereinbarung	KI-gestützte Bearbeitung von Anfragen, Tickets und Dokumenten; nur erforderliche Ausschnitte, keine Verkehrsdaten oder Kommunikationsinhalte, keine Verwendung zum Training	USA; Standardvertragsklauseln laut Datenschutzvereinbarung

5. Verarbeitungsorte und Drittlandübermittlungen

Unsere Systeme betreiben wir in Deutschland und Österreich (EU), siehe Tabelle. Bei Verbindungen ins Ausland werden die dafür nötigen Verbindungsdaten an ausländische Netzbetreiber übermittelt; das ist für die Vertragserfüllung erforderlich (Art. 49 Abs. 1 Buchst. b DSGVO). Im Übrigen erfolgen Übermittlungen außerhalb des EWR nur auf Grundlage der Art. 44 ff. DSGVO (siehe Tabelle). Kopien der Garantien erhalten Sie über den Datenschutzkontakt.

6. Aufbewahrung und Löschung

- **Verkehrsdaten zur Abrechnung** (Verbindungsdaten Telefonie): spätestens sechs Monate nach Versand der Rechnung, länger nur bei Einwendungen bis zu deren Klärung (§ 10 TDDDG). Die Rechnungen und die Abrechnungssummen je Rechnung (ohne Zielrufnummern) bewahren wir nach den steuerlichen Fristen auf.
- **IP-Zuordnungs- und Sicherheitsprotokolle:** sieben Tage, länger nur bei konkretem Missbrauchs- oder Störungsfall. Bis zur Umstellung unseres Authentifizierungssystems, spätestens am 15.12.2026, liegen dort noch ältere Zuordnungen. Sie werden nicht genutzt und mit der Umstellung gelöscht.
- **Sicherheitsmeldungen:** die Meldung selbst mit IP-Adresse und Verbindungsangaben 30 Tage nach Abschluss des Vorfalls, höchstens 90 Tage nach Eingang. Nicht zuordenbare Meldungen 30 Tage nach Eingang. Die Angaben je Vorfall ohne IP-Adresse (Datum, Art, Stand, Zeitpunkt unserer Information) zwölf Monate. Kam es zu einer Einschränkung oder Kündigung, bis zum Abschluss eines Streits, sonst bis zum Ablauf der gesetzlichen Verjährungsfrist.
- **Bestandsdaten:** löschen wir, sobald sie nach Vertragsende nicht mehr benötigt werden, spätestens mit Ablauf des Kalenderjahres, das auf das Vertragsende folgt, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht.
- **Geschäftskorrespondenz:** sechs Jahre; **Rechnungs- und Buchungsbelege:** acht Jahre, jeweils ab Ende des Kalenderjahres.
- **Sonstiges:** Support- und Nachweisdaten werden gelöscht, sobald der Zweck entfällt. Für Rechtsansprüche gilt die Verjährungsfrist.

7. Ihre Rechte

Sie haben folgende Rechte: - Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung und Übertragbarkeit; - Widerruf von Einwilligungen; - **Widerspruch** bei berechtigten Interessen und gegen Direktwerbung; - Beschwerde bei der Aufsicht. Zuständig ist für Daten aus Telekommunikationsdiensten auch die **Bundesbeauftragte für den Datenschutz und die Informationsfreiheit** (§ 29 TDDDG), im Übrigen der Landesbeauftragte für den Datenschutz Niedersachsen.

8. Erforderliche Angaben und automatisierte Entscheidungen

Erforderliche Angaben sind für den Vertrag nötig. Eine ausschließlich automatisierte Entscheidung findet nicht statt; der Forderungsabgleich wird durch einen Mitarbeiter geprüft.