

Erweiterte Datenschutzerklärung (inkl. NFC-Visitenkartenservice)

Datenschutzerklärung (FTC – Filling Time Control & Portal & weitere Dienste)

Stand: 30.11.2025

1. Verantwortlicher

Dive Tools

Käthestrasse 9 – 16540 Hohen Neuendorf

info@ctc-ftc.de · www.dive-tools.de

Vertretungsberechtigt: Olaf Berndt

Datenschutzbeauftragte:r (falls bestellt):

Olaf Berndt – info@ctc-ftc.de

2. Geltungsbereich

Diese Hinweise erläutern die Verarbeitung personenbezogener Daten bei:

- Nutzung von FTC-Geräten (RFID-Zugangs-/Füllsteuerung, Telemetrie, OTA),
 - Nutzung des FTC-Portals unter ctc-ftc.de (Geräte-Parametrisierung durch Manager, Füllübersichten, Abrechnung/Belege, sofern durch Portal ausgeführt),
 - Support- und Verwaltungsprozessen des Portalbetreibers,
 - Nutzung des NFC-Visitenkartenservice (z. B. Online-Registrierungsformular für digitale Visitenkarten, Erstellung und Bereitstellung von NFC-/QR-basierten Kontaktseiten und vCard-Dateien).
-

3. Rollen & Verantwortlichkeiten

- Portalbetreiber = Verantwortlicher (Art. 4 Nr. 7 DSGVO) für sämtliche Endkundendaten, die im Portal und den verbundenen Diensten (inkl. NFC-Visitenkartenservice) verarbeitet werden (z. B. Karten-/RFID-Zuordnung, Füll-/Nutzungsdaten, Kontaktkarten-Daten, Rechnungs-/Zahlungsdaten, sofern im Portal abgewickelt).
- Manager/Tauchbasen = Nutzungsberechtigte des Portals. Sie betreiben die FTC-Geräte und parametrisieren diese. Im Portal erhalten sie rollengesteuerten Lesezugriff auf Fülldaten ihrer eigenen Geräte (z. B. Zeitpunkte, Mengen, Kosten), ohne Einsicht in Bank-/Zahlungsdaten und ohne Administrationsrechte über Endkundendaten außerhalb ihrer Geräte.
- Auftragsverarbeiter des Portalbetreibers sind ausschließlich Infrastruktur-/Dienstleister (z. B. Hosting/E-Mail). Manager sind keine Auftragsverarbeiter für Endkundendaten des Portals.
- **Eigenständige Verarbeitungen der Manager außerhalb des Portals (z. B. lokale Kasse, eigene CRM-Listen, eigene Visitenkartenverwaltung) liegen in deren eigener Verantwortlichkeit und sind nicht Gegenstand dieser Erklärung.**

4. Daten, Zwecke & Rechtsgrundlagen

4.1 Portal-Konten (Manager/Admin/User)

Daten: Name, E-Mail, Rollen/Rechte, Passwort-Hash, Protokolle (Login-Zeit, IP, Änderungen).

Zweck: Konto-/Rechteverwaltung, IT-Sicherheit, Nachvollziehbarkeit.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b (Nutzungsvertrag), lit. f (Sicherheit).

4.2 RFID/Kartenverwaltung (Endkunden)

Daten: Karten-/RFID-UID (empfohlen: Pseudonymisierung/Hash), zugeordneter Profilname (falls verwendet), Rollen (z. B. user/admin/setup).

Zweck: Zugangskontrolle, Bedienung der FTC-Geräte, Missbrauchsprävention.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b (Nutzungsverhältnis mit Portal), lit. f (Betrieb/Sicherheit).

4.3 Füll-/Nutzungsprotokolle & Abrechnung

Daten: Device-ID, Start/Stop, Füllmengen/Parameter, ggf. Kartenbezug, Kosten, Beleg-/Rechnungsdaten (sofern Portal rechnet).

Zweck: Darstellung für Manager (nur ihre Geräte), Abrechnung/Belegerstellung (sofern durch Portalbetreiber), Nachweis/Statistik.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b (Leistungserbringung), lit. c (HGB/AO-Pflichten), lit. f (Betrieb/Qualität).

4.4 Zahlungs-/Bankdaten (falls im Portal abgewickelt)

Daten: Rechnungsadresse, IBAN/SEPA-Mandat, Zahlungsvorgänge.

Zweck: Zahlungsabwicklung, Buchhaltung, Nachweis.

Sichtbarkeit: Nicht für Manager/Tauchbasen einsehbar.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b, lit. c.

4.5 Gerätesignale („Heartbeat“), Remote-Befehle & OTA

Daten: Firmware, Status, RSSI, Uptime, Zeitstempel; Befehlswarteschlange (relay_on/off, reboot, update), Ausführungsprotokolle.

Zweck: Fernwartung, Stabilität, Sicherheitsmonitoring, Updates.

Rechtsgrundlage: Art. 6 Abs. 1 lit. f.

4.6 Support & Kommunikation

Daten: Kontaktdaten, Ticket-/E-Mail-Inhalte, technische Metadaten.

Zweck: Bearbeitung von Anliegen, Fehlerbehebung.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b, lit. f.

4.7 Web-/Portalbetrieb (Cookies & Logfiles)

Technisch notwendige Cookies: Session/Security (kein Tracking).

Server-Logfiles: IP, Datum/Uhrzeit, URL, Referrer/UA.

Zweck/Grundlage: Betrieb/Sicherheit (Art. 6 Abs. 1 lit. f).

Optionale Analyse (falls eingesetzt): nur mit Einwilligung (Art. 6 Abs. 1 lit. a).

4.8 NFC-Visitenkartenservice (digitale Kontaktkarten & vCards)

Dieser Abschnitt gilt für den Online-Service zur Erstellung digitaler Visitenkarten (z. B. über ein Registrierungsformular) sowie die Bereitstellung von NFC-/QR-basierten Kontaktseiten und vCard-Dateien.

Verarbeitete Daten:

- Stammdaten: Name, ggf. Titel, Vorname, Nachname, Positions-/Funktionsbezeichnung (z. B. „Geschäftsführung“), Firmenname,
- Kontaktdaten: E-Mail-Adresse, Telefonnummer, ggf. Mobilnummer/WhatsApp-Nummer,
- Adressdaten: Straße, Hausnummer, Postleitzahl, Ort, Land,
- Online-Daten: Website/URL,
- optionale Logodaten: hochgeladene Logodateien (z. B. Firmenlogo) zur Anzeige auf der digitalen Kontaktseite,
- technische Metadaten: Dateinamen der erzeugten Kontaktseiten und vCards, Schlüsselparameter für den geschützten Aufruf (z. B. URL-Parameter), Zeitstempel der Erstellung.

Zwecke der Verarbeitung:

- Entgegennahme und Verwaltung der von Ihnen bereitgestellten Kontaktdaten zur Erstellung einer digitalen Visitenkarte,
- Generierung und Bereitstellung einer individuellen Kontaktseite (z. B. für Aufruf per NFC oder QR-Code) und der zugehörigen vCard-Datei (VCF),
- Anzeige Ihrer Kontaktdaten und ggf. Ihres Logos auf der digitalen Kontaktseite,
- technisch notwendige Speicherung der Konfiguration, um die Kontaktseite dauerhaft anbieten zu können,
- interne Dokumentation/Support (z. B. Unterstützung bei Anpassungen oder Fehlern).

Rechtsgrundlage:

- Art. 6 Abs. 1 lit. b DSGVO (Vertrag bzw. vorvertragliche Maßnahme)
– soweit Sie den Service gezielt zur Erstellung einer persönlichen Kontaktkarte beauftragen bzw. nutzen,
- Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse)
– an einem sicheren, stabilen und komfortablen Bereitstellen des Dienstes, z. B. technische Protokollierung, Missbrauchsabwehr.

Bereitstellung der Daten / Pflichtangaben:

- Für die Erstellung einer funktionsfähigen digitalen Visitenkarte sind insbesondere Name und E-Mail-Adresse erforderlich; weitere Angaben sind optional, werden jedoch typischerweise für eine vollständige Visitenkarte genutzt (z. B. Telefonnummer, Firmenname).
- Ohne die grundlegenden Kontaktdaten kann der NFC-Visitenkartenservice nicht oder nur eingeschränkt genutzt werden.

Speicherdauer:

- Die erstellten Profile (Kontaktdaten, Logoverweise, zugehörige Konfigurationsdateien) werden gespeichert, solange Ihre digitale Visitenkarte aktiv bereitgestellt werden soll oder bis Sie deren Löschung verlangen.
- Soweit gesetzliche Aufbewahrungspflichten greifen (z. B. im Rahmen der Abrechnung/Buchhaltung, falls der Service kostenpflichtig ist), gelten die in Abschnitt 8 genannten Fristen.
- Backups und technische Protokolle können aus Sicherheitsgründen für einen begrenzten Zeitraum (z. B. 7–30 Tage für Server-Logs) vorgehalten werden.

Empfänger / Zugriff:

- Intern: technische Betreuung des Dienstes, Support.
- Extern: Hosting-Dienstleister (z. B. STRATO AG, siehe Abschnitt 6); diese verarbeiten die Daten als Auftragsverarbeiter nach Art. 28 DSGVO.
- Die öffentliche Kontaktseite ist – wie bei einer Visitenkarte üblich – für Personen abrufbar, die den zugehörigen URL/QR-Code oder NFC-Aufruf verwenden. Der Zugang kann technisch (z. B. über einen Schlüsselparameter) beschränkt sein.

Besonderheiten: Logos & Dateien:

- Logos werden ausschließlich verwendet, um Ihre digitale Visitenkarte optisch zu gestalten.
- Sie sind dafür verantwortlich, dass Sie die Rechte an den hochgeladenen Bilddateien besitzen und keine Rechte Dritter verletzen.

5. Herkunft der Daten

- durch Endkund:innen/Manager via Portal (Eingaben, Kartenverwaltung, Nutzung des NFC-Visitenkartenservice/Registrierungsformulars),
- durch FTC-Geräte (Ereignisse, Telemetrie),
- durch Zahlungsdienstleister/Banken (Status),
- systemseitige Protokolle.

6. Empfänger & Kategorien von Dienstleistern

- Interne Empfänger beim Portalbetreiber: Support, Technik, Buchhaltung.
 - Nutzungsberechtigte (Manager/Tauchbasen): rollenbasierter Lesezugriff auf Fülldaten ihrer Geräte; kein Zugriff auf Bank-/Zahlungsdaten sowie keine administrative Bearbeitung zentraler Endkundendaten des Portalbetreibers.
 - Auftragsverarbeiter:
 - Hosting/E-Mail (z. B. STRATO AG, DE/EU-RZ),
 - ggf. weitere IT-Dienstleister, vertraglich nach Art. 28 DSGVO gebunden,
 - technischer Betrieb des NFC-Visitenkartenservice (Hosting, Backup, E-Mail-Benachrichtigungen).
 - Behörden/Banken: sofern rechtlich erforderlich.
-

7. Drittlandübermittlung

Keine Übermittlung in Drittländer; andernfalls nur mit Garantien (Art. 46 DSGVO, EU-SCC).

8. Speicherdauer

- Portal-Konten & Karten: bis Beendigung/Löschung oder berechtigtem Widerspruch; Protokolle i. d. R. 12–24 Monate.
 - Füll-/Rechnungs- & SEPA-Daten: gem. HGB/AO 6–10 Jahre.
 - Server-Logs/IPs: 7–30 Tage (länger nur bei Sicherheitsvorfällen).
 - Heartbeats/Telemetrie: bis zu 90 Tage (Betriebsdiagnose).
 - Profile und Konfigurationen im NFC-Visitenkartenservice: für die Dauer der Bereitstellung der digitalen Visitenkarte, danach Löschung oder Anonymisierung, soweit keine gesetzlichen Aufbewahrungsfristen entgegenstehen.
-

9. Pflicht zur Bereitstellung

Ohne grundlegende Nutzungs-/Identifikationsdaten ist die Nutzung des Portals/der Geräte und des NFC-Visitenkartenservice nicht möglich.

10. Automatisierte Entscheidungen

Keine automatisierte Entscheidungsfindung i. S. v. Art. 22 DSGVO.

11. Betroffenenrechte

Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch (Art. 15–21 DSGVO). Einwilligungen können jederzeit widerrufen werden (Art. 7 Abs. 3).

Beschwerde: bei der zuständigen Datenschutzaufsichtsbehörde.

Zuständige Aufsichtsbehörde in Brandenburg ist:

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg (LDA Brandenburg)

Website: www.lda.brandenburg.de

Kontakt für Rechte: info@ctc-ffc.de

12. Sicherheit (Art. 32 DSGVO)

TLS, RBAC (rollenbasierte Zugriffe) mit Sichtbarkeitskonzept (Manager: nur Fülldaten eigener Geräte), Passwort-Hashing, Protokollierung, Pseudonymisierung der RFID-UIDs, Mandantentrennung, Backups, Härtung/Updates (OTA-Integrität).

Für den NFC-Visitenkartenservice gelten vergleichbare technische und organisatorische Maßnahmen (z. B. geschützte Konfigurationsdateien, kontrollierte Serverumgebung).

13. Änderungen

Es gilt die jeweils aktuelle Fassung auf ctc-ffc.de.

Sichtbarkeits- & Zugriffsmatrix (Kurzüberblick)

Datenkategorie	Portalbetreiber	Manager/Tauchbasis
Kontodaten (Manager/User)	Vollzugriff (administrativ)	eigenes Konto
RFID/Karten (Endkunden)	Verwaltung/Zuordnung	nur lesend, soweit für eigene Geräte
Fülldaten (Zeit, Menge, Kosten)	Vollzugriff	lesend für eigene Geräte
Zahlungs-/Bankdaten	Vollzugriff, Verarbeitung	kein Zugriff
Telemetrie/Heartbeat	Vollzugriff	lesend für eigene Geräte
Remote-Befehle/OTA	Vollzugriff	sofern Rolle freigeschaltet
NFC-Visitenkartenprofile	Vollzugriff (Erstellung/Verwaltung)	keine eigenständige Bearbeitung im Portal*

* Soweit Manager eigene Kontaktkarten verwenden/verteilen, handeln sie hierfür ggf. auch in eigener Verantwortlichkeit.

Vertragliche Einbindung der Manager (keine AVV erforderlich)

Manager sind keine Auftragsverarbeiter für Endkundendaten des Portals. Stattdessen gilt eine Nutzungs-/Zugriffsvereinbarung mit u. a.:

- Vertraulichkeit, Zweckbindung, kein Export von Bank-/Zahlungsdaten,
- Nutzung der Daten nur für Betrieb/Abrechnung der eigenen Geräte,
- technische und organisatorische Maßnahmen (z. B. sichere Konten, kein Teilen von Logins),
- Protokollierung/Zugriffskontrollen durch den Portalbetreiber.

(Hinweis: Für Hosting/E-Mail/IT-Services des Portalbetreibers bestehen Art.-28-AV-Verträge mit Dienstleistern.)