

Arbeitsakte

Testakte: Cyber-Vorfall Ransomware Frischetrans Mainz

cyber-vorfall-ransomware-frischetrans-mainz

Diese Datei bündelt alle Aktenstücke in einem Dokument. Die Einzeldateien liegen im Aktenordner ebenfalls vor.

Inhaltsverzeichnis

Teil	Inhalt
Teil 1	Aktenstücke (Markdown) (22)
Teil 2	E-Mails (4)
Teil 3	Excel-Tabellen (2)
Teil 4	Word-Dokumente (3)
Teil 5	Bildanlagen und Screenshots (3)
Teil 6	PDF-Anhänge (Originaldokumente) (2)

Aktenstücke (Markdown)

Datei: 01_aktenvorblatt_drosten_pekonkur.md

Aktenvorblatt

Kanzlei Drosten & Pekonkur — Rechtsanwälte und Fachanwälte

Aktenzeichen intern: DP-2026-0506-FTM

Anlage: IT-Recht / Datenschutz / Strafrecht

Bearbeiter: RA Lukas Drosten, Fachanwalt für IT-Recht

Eröffnet am: 06.05.2026

Status: Aktiv — Notfall-Mandat

Mandantin

Firmenbezeichnung: Frischetrans Mittelrhein GmbH

Rechtsform: GmbH

Sitz: Binger Straße 142, 55131 Mainz

Handelsregister: HRB 44821, Amtsgericht Mainz

Umsatz (ca.): 38 Mio. EUR p.a.

Mitarbeiter: 280 (Vollzeit und Teilzeit)

Fuhrpark: 64 LKW (Kühlkette / Frischelogistik)

Branche: B2B-Frischelogistik für Großbäckereien und Lebensmittelketten

Geschäftsführerin: Theresia Wallbruck (alleinvertretungsberechtigt)

E-Mail (GF): t.wallbruck@frischetrans-mittelrhein.de

Telefon (GF): +49 6131 8820-100

Mandatsbeschreibung

Frischetrans Mittelrhein GmbH ist in der Nacht vom 05. auf den 06.05.2026 Opfer eines schwerwiegenden Ransomware-Angriffs der Gruppe „AkiraNext“ geworden. Das ERP-System (SAP S/4HANA, on-premises) sowie die Telematik-Schnittstellen wurden vollständig verschlüsselt. Dem Unternehmen liegt ein Erpressungsschreiben mit einer Lösegeldforderung von 1.450.000 USD (Monero) vor.

Aufgrund des Datenabflusses von ca. 2,1 TB (Kundenstammdaten, Mitarbeiterpersonalakten inkl. Gesundheitsdaten aus BEM-Verfahren) bestehen akute Meldepflichten nach Art. 33 DSGVO (LfDI RLP, Frist 72 h), potenziell nach BSI-Gesetz/NIS2-Umsetzungsgesetz sowie strafrechtliche Anzeigepflichten/Anzeigeoptionen.

Parallel bestehen:

- Ansprüche gegen den ERP-Dienstleister **ProcessSpark Cloud AG** (München) wegen verspäteten Sicherheitspatches (CVE-2026-0712)
- Fragen der KI-Verordnungs-Compliance (KI-System „PalettenAuge AI“)
- Open-Source-Compliance-Fragen (AGPL-3.0-Komponente „scheduleHero“ im Tool „TourPlanner“)

Beteiligte und Gegner

Partei	Rolle	Kontakt
Frischetrans Mittelrhein GmbH	Mandantin	Binger Str. 142, 55131 Mainz
Theresia Wallbruck	Geschäftsführerin Mandantin	t.wallbruck@frischetrans-mittelrhein.de
InsoTec Systems GmbH	Externer IT-Dienstleister / SOC	Hanauer Landstraße 204, 60314 Frankfurt a.M.
ProcessSpark Cloud AG	SaaS-ERP-Anbieter, Gegner	Leopoldstraße 88, 80802 München
DachAuge GmbH	KI-System-Anbieter „PalettenAuge AI“	Rosenthaler Str. 34, 10178 Berlin
LfDI Rheinland-Pfalz	Aufsichtsbehörde DSGVO	Hintere Bleiche 34, 55116 Mainz
BSI Außenstelle Frankfurt	Behörde NIS2/KRITIS	Gutleutstraße 163, 60327 Frankfurt
ZAC Mainz (Kriminalpolizei)	Strafverfolgung Cybercrime	Valenciaplatz 1, 55118 Mainz
CyberCovered AG	Cyber-Versicherer	Taunusanlage 17, 60325 Frankfurt
Frischbäcker AG	Betroffener Kunde (systemrelevant)	Industriestraße 12, 68167 Mannheim
Backhaus Süd GmbH & Co. KG	Betroffener Kunde (systemrelevant)	Böblinger Str. 111, 70199 Stuttgart

Geplante Verfahren / Aktenzeichen

Verfahren	Aktenzeichen	Status
Klage ProcessSpark (LG Mainz)	3 O 88/26 (geplant)	Vorbereitungsphase
Strafanzeige Cybercrime (ZAC Mainz)	421 UJs 6611/26	Erstattet 06.05.2026
DSGVO-Meldung LfDI RLP	intern: DP-LDFI-2026-0506	Übermittelt 08.05.2026
BSI-Meldung NIS2	BSI-REF-2026-1847	Übermittelt 07.05.2026

Fristen (Übersicht — Details siehe Aktenstück 22)

Frist	Datum	Erledigt
Art. 33 DSGVO — 72 h Meldung LfDI	09.05.2026, 04:17 Uhr	Ja (08.05.2026, 22:45 Uhr)
BSI NIS2-Meldung	09.05.2026	Ja (07.05.2026, 16:30 Uhr)
Art. 34 DSGVO Benachrichtigung Betroffene	Unverzüglich	In Bearbeitung
Schadensersatzforderung ProcessSpark	Setzung 14-Tages-Frist ab 12.05.2026	Offen
Versicherungsmeldung CyberCovered	72 h nach Entdeckung	Gemeldet 07.05.2026

Kanzleidaten

Kanzlei Drosten & Pekonkur Rechtsanwälte und Fachanwälte Schillerstraße 14 55116 Mainz Telefon: +49 6131 2240-0 Telefax: +49 6131 2240-99 E-Mail: kanzlei@drosten-pekonkur.de Berufsrechtliche Regelungen: BRAO, BORA, FAO Zuständige Rechtsanwaltskammer: Rechtsanwaltskammer Koblenz Berufshaftpflichtversicherung: Allianz Versicherungs-AG, Pol.-Nr. RHV-88341120

Datei: 02_chronologie_cyber_vorfall_d0_bis_d7.md

Chronologie des Cyber-Vorfalls — D+0 bis D+7

Mandantin: Frischetrans Mittelrhein GmbH, Mainz

Vorfall: Ransomware-Angriff „AkiraNext“

Erstdetektion: 06.05.2026, 04:17 Uhr

Bearbeiter: RA Lukas Drosten, Kanzlei Drosten & Pekonkur

Tag 0 — Mittwoch, 06.05.2026 (Vorfallstag)

04:17 Uhr SOC-System der InsoTec Systems GmbH (externer IT-Dienstleister, Frankfurt) detektiert anomale Netzwerkaktivität im Rechenzentrum der Frischetrans Mittelrhein GmbH (Serverraum Binger Straße 142, Mainz). Ungewöhnlich hoher Netzwerktraffic auf internen SMB-Shares, laterale Bewegungen im Active Directory-Verbund.

04:23 Uhr SOC-Analyst Mikhail Dragunov (InsoTec) weckt seinen Schichtleiter. Erste Einschätzung: möglicherweise Ransomware. Automatische Segmentierungsregeln greifen verzögert, da Firewall-Konfiguration veraltet (siehe Pflichtverletzungsanalyse Aktenstück 09).

04:31 Uhr Erste Systeme vollständig verschlüsselt: SAP S/4HANA Applikationsserver (Hostname: FT-ERP-PROD-01, FT-ERP-PROD-02). Datenbankserver FT-DB-01 betroffen. Lösegeldforderung als Desktop-Hintergrund und .txt-Datei auf allen verschlüsselten Systemen sichtbar.

04:45 Uhr InsoTec benachrichtigt Bereitschaftsnummer der Frischetrans. Diensthabender Logistikleiter Rainer Schäper nimmt Anruf entgegen. Geschäftsführerin Theresia Wallbruck wird um 04:52 Uhr telefonisch erreicht.

05:10 Uhr Telematik-Schnittstellen (GPS-Tracking, Temperaturüberwachung Kühlkette, Fahrerdispositionssystem) fallen aus. 47 der 64 LKW können keine Positions-/Temperaturdaten mehr übermitteln. Frühschicht-Fahrer werden per Mobiltelefon kontaktiert.

05:35 Uhr Geschäftsführerin Wallbruck trifft am Firmengelände ein. Sofortentscheidung: alle Systeme vom Netz nehmen (Network Kill). InsoTec schaltet zentrale Switches ab.

06:00 Uhr Erste Schadenserfassung: ERP-System vollständig ausgefallen, Auftragsabwicklung nicht möglich. Geplante 37 Auslieferungen für Donnerstag 07.05. sind gefährdet. Frischbäcker AG und Backhaus Süd erhalten Notfall-Anrufe.

07:15 Uhr Theresia Wallbruck ruft Kanzlei Drosten & Pekonkur an. RA Lukas Drosten übernimmt Erstberatung per Telefon.

08:30 Uhr Erstes persönliches Treffen in der Kanzlei Drosten & Pekonkur (Schillerstraße 14, Mainz). Mandatserteilung. Beginn der rechtlichen Incident-Response.

09:00 Uhr Forensisches Sicherungsprotokoll startet. InsoTec sichert flüchtige Daten (RAM-Dumps, Netzwerk-Logs). Externale Forensikfirma CyberForensik RheinMain GmbH wird durch Kanzlei Drosten empfohlen und beauftragt.

10:30 Uhr Erste Indizien für Datenabfluss: Netzwerk-Logs zeigen ab dem 04.05.2026, 22:44 Uhr (D-2) kontinuierlichen ausgehenden Datenverkehr zu einer IP-Adresse in Rumänien (Tor-Exit-Node). Gesamtvolumen ca. 2,1 TB.

11:45 Uhr Strafanzeige bei ZAC Mainz (Zentrale Ansprechstelle Cybercrime) wird vorbereitet (AZ: 421 UJs 6611/26).

14:00 Uhr BSI Außenstelle Frankfurt telefonisch vorinformiert durch RA Drosten. NIS2-Relevanzprüfung eingeleitet.

15:30 Uhr Versicherungsmeldung an CyberCovered AG (Frankfurt) per verschlüsselter E-Mail. Schadensnummer wird vergeben.

17:00 Uhr Erpressungsschreiben der Gruppe AkiraNext vollständig dokumentiert und rechtlich bewertet (Aktenstück 03).

Tag 1 — Donnerstag, 07.05.2026

08:00 Uhr CyberForensik RheinMain GmbH beginnt forensische Untersuchung vor Ort. Zwei Spezialisten arbeiten an Sicherung und Analyse der Systeme.

09:30 Uhr Strafanzeige bei ZAC Mainz persönlich erstattet durch RA Drosten im Namen der Frischetrans. Aktenzeichen 421 UJs 6611/26 vergeben.

11:00 Uhr Krisenteam konstituiert sich formal: GF Wallbruck, RA Drosten, IT-Leiter Franz Berkenfeld (Frischetrans), SOC-Leiter InsoTec, externer Forensiker.

14:00 Uhr Betroffene Datenkategorien wurden durch Forensikteam bestätigt:

- Kundenstammdaten: 18 Kunden, darunter Frischbäcker AG und Backhaus Süd
- Mitarbeiterdaten: Personalakten 280 MA, davon Gesundheitsdaten aus BEM-Verfahren von 38 Mitarbeitern
- Vertragsdaten mit Lieferanten

- Finanzdaten (Buchungsdaten Q1/2026)

16:30 Uhr BSI-Meldung (NIS2) formal elektronisch übermittelt über das MELDEPF-Portal (Referenznummer BSI-REF-2026-1847).

19:00 Uhr Kanzlei bereitet Art.-33-DSGVO-Meldung an LfDI RLP vor. Fristablauf: 09.05.2026, 04:17 Uhr.

Tag 2 — Freitag, 08.05.2026

09:00 Uhr Forensikbericht Zwischenstand: Angriffsvektor identifiziert. Initial Access über ungepatchte SAP-Schwachstelle CVE-2026-0712 (SAP NetWeaver AS ABAP). Patch war laut Vertrag mit ProcessSpark Cloud AG zum 20.03.2026 geschuldet, tatsächlich erst am 28.04.2026 (Nacht zum 29.04.) eingespielt worden — 39 Tage verspätet. In dieser Lücke erfolgte der Angriff.

11:00 Uhr Vertragsanalyse ProcessSpark beginnt (Aktenstück 08 und 09).

14:30 Uhr KI-Verordnungs-Compliance-Check für „PalettenAuge AI“ aufgenommen (Aktenstück 13).

22:45 Uhr DSGVO-Meldung Art. 33 an LfDI RLP eingereicht (Aktenstück 05). Frist eingehalten.

Tag 3 — Samstag, 09.05.2026

04:17 Uhr Ablauf der 72-Stunden-Frist Art. 33 DSGVO. Meldung wurde rechtzeitig übermittelt (22:45 Uhr D+2).

10:00 Uhr Erste Notfall-Wiederherstellung: Backup-Systeme (letzte Sicherung 03.05.2026, 02:00 Uhr) werden schrittweise eingespielt. Datenverlust: 3 Tage operativer Daten.

14:00 Uhr Telefonische Abstimmung LfDI RLP: Behörde bestätigt Eingang der Meldung, stellt Rückfragen zu BEM-Gesundheitsdaten und ordnet Übermittlung eines Folgeberichts innerhalb von 14 Tagen an.

Tag 4 — Sonntag, 10.05.2026

Keine behördlichen Aktivitäten. Interne IT-Wiederherstellung läuft. Telematik-System teilweise wieder verfügbar (35 von 64 LKW).

Tag 5 — Montag, 11.05.2026

09:00 Uhr Betriebsrat wird förmlich informiert (§ 75 BetrVG, § 26 BDSG). Anhörung protokolliert (Aktenstück 18).

11:00 Uhr Mitarbeiterinformation BEM-Betroffene: 38 Beschäftigte werden schriftlich über Datenpanne informiert (Aktenstück 17).

14:00 Uhr DSFA (Datenschutz-Folgenabschätzung) für BEM-Gesundheitsdaten formell eingeleitet (Aktenstück 11).

Tag 6 — Dienstag, 12.05.2026

10:00 Uhr Anwaltsschreiben (Klageandrohung) an ProcessSpark Cloud AG abgesandt (Aktenstück 10). Frist: 14 Tage.

11:00 Uhr Kundenkommunikation an Frischbäcker AG und Backhaus Süd versandt (Aktenstück 16).

14:00 Uhr Open-Source-Compliance-Audit für „TourPlanner“ (AGPL-3.0-Komponente „scheduleHero“) begonnen (Aktenstück 14).

Tag 7 — Mittwoch, 13.05.2026

09:00 Uhr ERP-System SAP S/4HANA zu ca. 80 % wiederhergestellt. Normalbetrieb Logistik teilweise aufgenommen.

10:30 Uhr Strategiememorandum RA Drostens fertiggestellt (Aktenstück 20).

14:00 Uhr Pressemitteilung (Entwurf) durch Kanzlei freigegeben — Veröffentlichung nach Abstimmung mit Mandantin (Aktenstück 19).

16:00 Uhr Keine Reaktion der Erpressergruppe AkiraNext auf Nicht-Zahlung. Forensikteam bestätigt: Lösegeldzahlung wird ausdrücklich nicht empfohlen (keine Garantie auf Schlüssel, Strafbarkeitsrisiken, Versicherungsklauseln).

Angriffs-Technisches Lagebild (Zusammenfassung forensischer Erstbefunde)

Parameter	Wert
Angriffsvektor	CVE-2026-0712 (SAP NetWeaver AS ABAP, ungepatchte Lücke)
Erstinfiltration	04.05.2026, ca. 22:44 Uhr (D-2)
Dwell Time (Verweildauer)	ca. 29,5 Stunden vor Aktivierung der Verschlüsselung
Verschlüsselte Systeme	SAP S/4HANA (2 App-Server, 1 DB-Server), Fileserver (3), Telematik-Gateway
Abgeflossene Datenmenge	ca. 2,1 TB
Geforderte Summe	1.450.000 USD in Monero
Zahlungs-Deadline (Erpresser)	13.05.2026, 23:59 Uhr UTC
Reaktion Frischetrans	Keine Zahlung
Wiederherstellung	Aus Backup (Stand 03.05.2026)
Datenverlust operativ	~3 Tage
Betroffene Personen (Kunden)	18 Firmenkunden, davon 2 systemrelevante Bäckereiketten
Betroffene Mitarbeiter	280 (Grunddaten), 38 (Gesundheitsdaten BEM)

Datei: 03_erpressungsschreiben_akiranext.md

Erpressungsschreiben AkiraNext — Dokumentation und Rechtliche Bewertung

Aktenstück: 03

Mandantin: Frischetrans Mittelrhein GmbH

Datum: 06.05.2026

Bearbeiter: RA Lukas Drost, Fachanwalt für IT-Recht

1. Originaltext des Erpressungsschreibens (transkribiert, redaktionell geschwärzt)

Das folgende Schreiben wurde am 06.05.2026 um ca. 04:31 Uhr auf allen verschlüsselten Systemen als Desktop-Hintergrund sowie als Textdatei !!! AKIRA_NEXT_README.txt auf allen betroffenen Laufwerken vorgefunden. Die Originalformatierung (ASCII-Art-Banner wurde entfernt) wird nachfolgend wiedergegeben. Krypto-Wallet-Adresse und Tor-Onion-Adressen sind zu Ermittlungszwecken im Original dokumentiert (ZAC Mainz, Strafsache 421 UJs 6611/26), hier geschwärzt.

[ORIGINALTEXT — ENGLISCH, ÜBERSETZT VON RA DROSTEN]

``` AKIRA NEXT — YOUR FILES HAVE BEEN ENCRYPTED

Hello, FRISCHETRANS MITTELRRHEIN GMBH.

We have encrypted your entire infrastructure and exfiltrated approximately 2.1 TB of sensitive data including:

- Full customer database (18 enterprise clients)
- Employee personal records (280 employees)
- HR/Health records (BEM files, 38 employees)
- Financial records Q1/2026
- Logistics contracts and SLA agreements
- SAP configuration data

To recover your files and prevent publication of the above data, you must pay 1,450,000 USD in Monero (XMR) to the wallet address:

[WALLET-ADRESSE — GESCHWÄRZT FÜR BEHÖRDEN / ZAC MAINZ]

You have 7 days from the date of this notice. If payment is not received, all data will be published on our leak site:

[ONION-ADRESSE — GESCHWÄRZT / BEI ZAC MAINZ HINTERLEGT]

To prove we have the decryption key, send 3 sample files (max 1 MB each) to our encrypted contact form on the above site.

DO NOT contact law enforcement. DO NOT attempt to recover files yourself. DO NOT power off systems (some have already self-destructed).

Every 24 hours of delay: +\$50,000 additional fee.

— AKIRA NEXT TEAM ```

## 2. Rechtliche Bewertung des Erpressungsschreibens

### 2.1 Straftatbestand — Deutschland

Das Erpressungsschreiben erfüllt folgende Straftatbestände des deutschen Strafgesetzbuchs (StGB):

**§ 202a StGB — Ausspähen von Daten** Die unbefugte Erlangung von ca. 2,1 TB unternehmensinterner Daten unter Überwindung von Zugangssicherungen (Firewalls, Authentifizierungssysteme) erfüllt den Tatbestand des § 202a Abs. 1 StGB. Strafraumen: Freiheitsstrafe bis zu 3 Jahre oder Geldstrafe.

**§ 303a StGB — Datenveränderung** Die Verschlüsselung der Daten ohne Zustimmung der Inhaberin stellt eine rechtswidrige Löschung, Unterdrückung, Unbrauchbarmachung oder Veränderung von Daten dar. Strafraumen: Freiheitsstrafe bis zu 2 Jahre oder Geldstrafe. In schweren Fällen (§ 303b StGB, Computersabotage) bis zu 5 Jahre.

**§ 303b StGB — Computersabotage** Der Angriff auf wesentliche Teile des Unternehmensnetzwerks (ERP, Telematik) mit der Absicht, den Betrieb einer Datenverarbeitungsanlage zu stören, fällt unter § 303b Abs. 1 Nr. 2 StGB. Da es sich um eine Einrichtung von erheblicher Bedeutung für die Versorgung der Bevölkerung (Frischelogistik für Lebensmittelketten) handeln kann, kommt § 303b Abs. 4 StGB in Betracht (Freiheitsstrafe bis 10 Jahre).

**§ 253 StGB — Erpressung** Die Forderung nach Zahlung von 1.450.000 USD unter Drohung der Veröffentlichung gestohlener Daten erfüllt den Tatbestand der Erpressung nach § 253 Abs. 1 StGB. Strafraumen: Freiheitsstrafe bis zu 5 Jahre; in schweren Fällen (§ 253 Abs. 4) bis zu 15 Jahre.

**§ 263a StGB — Computerbetrug** Soweit der Angreifer durch die Manipulation der EDV-Anlage einen Vermögensvorteil erzielen will, liegt tateinheitlich Computerbetrug vor.

## 2.2 Empfehlung: Keine Zahlung

Die Kanzlei Drost & Pekonkur empfiehlt der Mandantin ausdrücklich, das Lösegeld **nicht** zu zahlen. Folgende Gründe:

1. **Keine Erfolgsgarantie:** Empirische Studien (u. a. Europol-Report 2025) zeigen, dass in bis zu 40 % der Fälle nach Lösegeldzahlung kein funktionierender Entschlüsselungsschlüssel geliefert wird.
2. **Strafbarkeitsrisiken:** Die Überweisung von Kryptowährungen an bekannte Ransomware-Gruppen kann unter §§ 129, 261 StGB (Unterstützung krimineller Vereinigungen, Geldwäsche) problematisch sein.
3. **Versicherungsklausel:** Die Cyber-Police der CyberCovered AG (Pol.-Nr. CC-2024-FTM-8801) enthält eine Klausel, die Erstattungen für Lösegeldzahlungen von vorheriger Genehmigung des Versicherers abhängig macht. Eigenmächtige Zahlung kann zum Verlust des Versicherungsschutzes führen.
4. **Erneutes Angriffsziel:** Zahlende Unternehmen werden als lohnende Ziele identifiziert und häufig erneut angegriffen.
5. **Backup verfügbar:** Da Frischetrans über Backup-Systeme (Stand 03.05.2026) verfügt, ist eine Wiederherstellung ohne Schlüssel möglich.

## 2.3 Reaktion gegenüber den Erpressern

Es wird keinerlei Kontakt zu den Erpressern aufgenommen. Jede Kommunikation obliegt ausschließlich den Ermittlungsbehörden (ZAC Mainz, ggf. BKA Cybercrime). Die Mandantin wird angewiesen, keine E-Mails, Chat-Nachrichten oder sonstigen Kontaktversuche an die genannten Onion-Adressen zu richten.

## 2.4 Beweissicherung

Das Erpressungsschreiben wurde vollständig gesichert durch:

- Fotografische Dokumentation aller betroffenen Bildschirme (Fotos in digitaler Forensikakte)
- Vollständige Sicherung aller `!!! AKIRA\_NEXT\_README.txt`-Dateien (Hash-Werte bei ZAC hinterlegt)
- Sicherung des Desktop-Hintergrundbildes (BMP-Datei)
- Forensische Festplattenabbilder (dd-Images) der betroffenen Server

### 3. Einordnung der Tätergruppe AkiraNext

Die Ransomware-Gruppe „AkiraNext“ ist nach vorliegenden Erkenntnissen eine Weiterentwicklung der bekannten Gruppe „Akira“, die seit 2023 aktiv ist und vorwiegend Unternehmen der Logistik, Fertigung und des Gesundheitswesens angreift.

Charakteristika:

- Doppelte Erpressungsstrategie (Verschlüsselung + Datenveröffentlichung)
- Bevorzugte Angriffsvektoren: ungepatchte SAP-Systeme, VPN-Schwachstellen, Microsoft Exchange
- Bekannte Infrastruktur: Russland-assoziierte Hosting-Dienste, Tor-Netzwerk
- Lösegeldforderungen typischerweise 500.000–5.000.000 USD

Hinweise für Ermittlungsbehörden wurden vollständig an ZAC Mainz und BSI übermittelt.

### 4. Redaktionshinweis

Das vollständige, ungeschwärzte Erpressungsschreiben einschließlich Wallet-Adresse und Onion-URL ist als PDF in der Strafakte (ZAC Mainz, 421 UJs 6611/26) sowie verschlüsselt in der Mandantenakte der Kanzlei hinterlegt. Das Aktenstück „pdfs/erpressungsschreiben\_akiranext\_redacted.pdf“ enthält die geschwärzte Version für Mandantensicht und Versicherungszwecke.

Datei: 04\_kanzleinotiz\_erstgesprach\_wallbruck.md

## Kanzleinotiz — Erstgespräch mit Geschäftsführerin Theresia Wallbruck

**Aktenstück:** 04

**Datum:** 06.05.2026, 08:30 Uhr

**Ort:** Kanzlei Drosten & Pekonkur, Schillerstraße 14, 55116 Mainz, Besprechungsraum 1

**Anwesende:**

- RA Lukas Drosten (Kanzlei Drosten & Pekonkur)
- Theresia Wallbruck (Geschäftsführerin Frischetrans Mittelrhein GmbH)
- Franz Berkenfeld (IT-Leiter Frischetrans, telefonisch zugeschaltet ab 09:15 Uhr)

**Vertraulich — Unterliegt anwaltlichem Berufsgeheimnis**

### 1. Ausgangslage bei Gesprächsbeginn

Frau Wallbruck erschien sichtlich erschöpft und unter großem emotionalem Druck. Sie hatte seit 04:52 Uhr keine Schlafpause. Das Gespräch begann pünktlich um 08:30 Uhr.

Frau Wallbruck schilderte die Ereignisse aus ihrer Perspektive:

> „Ich wurde um kurz vor 5 Uhr angerufen. Am Anfang dachte ich, es sei ein normaler IT-Ausfall. Dann hieß es Ransomware. Ich bin sofort gefahren. Als ich ankam, standen alle Monitore auf diesem

Bedrohungstext. Und das ERP war weg."

Sie berichtete, dass bereits mehrere Kunden (allen voran Frischbäcker AG, Mannheim) angerufen und den Ausfall des Telematiksystems gemeldet hatten. Die Disponentin habe die Lage manuell notdürftig überbrückt.

## **2. Rechtliche Erstinformation durch RA Drost**

RA Drost erläuterte folgende Kernpunkte:

### **2.1 Meldepflicht Art. 33 DSGVO**

Aufgrund des bestätigten Datenabflusses (Kundenstammdaten, Mitarbeiterpersonalakten) besteht eine Meldepflicht gegenüber dem Landesbeauftragten für den Datenschutz Rheinland-Pfalz (LfDI RLP) innerhalb von 72 Stunden nach Kenntnisnahme der Datenpanne (Art. 33 Abs. 1 DSGVO). Die Frist läuft ab 04:17 Uhr am 06.05.2026 und endet am 09.05.2026 um 04:17 Uhr. Die Meldung sei innerhalb von 48 Stunden vorzubereiten und abzusenden.

Frau Wallbrück: \*,„Können wir nicht noch warten, bis wir mehr wissen?“\*

RA Drost erklärte, dass Art. 33 Abs. 1 DSGVO eine Meldung „ohne unangemessene Verzögerung“ vorschreibt, wobei die Kenntnis der vollständigen Einzelheiten keine Voraussetzung für die Erstmeldung ist. Eine Nachmeldung mit dem Hinweis auf unvollständige Erkenntnisse ist zulässig und behördenüblich.

### **2.2 BSI-Meldepflicht / NIS2**

RA Drost erläuterte, dass Frischetrans als Logistik-Unternehmen möglicherweise unter den Geltungsbereich der NIS2-Richtlinie (umgesetzt durch das NIS2-Umsetzungsgesetz, NIS2UmsuG) fällt. Frischelogistik für Bäckereiketten könnte als Teil der Kritischen Infrastruktur (Lebensmittelversorgung) einzustufen sein. Die BSI-Außenstelle Frankfurt war telefonisch vorinformiert worden.

Frau Wallbrück: \*,„Wir sind doch nur ein mittelständischer Logistiker. Ich hätte nie gedacht, dass wir KRITIS sind.“\*

RA Drost erklärte, dass die Einschätzung von der Versorgungsrelevanz und den Schwellenwerten des BSI abhängt, die aktuell geprüft werden.

### **2.3 Empfehlung: Keine Lösegeldzahlung**

RA Drost empfahl ausdrücklich, das Lösegeld von 1.450.000 USD nicht zu zahlen (vgl. Begründung Aktenstück 03). Frau Wallbrück stimmte zu.

### **2.4 Versicherung**

Frau Wallbrück bestätigte das Bestehen einer Cyber-Versicherung bei der CyberCovered AG (Frankfurt), Police-Nr. CC-2024-FTM-8801, Deckungssumme 5 Mio. EUR. RA Drost wies darauf hin, dass die Police unverzüglich zu informieren sei (24-h-Klausel im Vertrag).

Frau Wallbrück: \*,„Die Versicherungsmaklerin hatte ich gestern noch im Kopf und heute ist alles weg.“\* Sie übergab die Police-Unterlagen in Kopie.

### **2.5 Lieferanten und ERP-Anbieter**

Frau Wallbrück berichtete, dass der ERP-Anbieter ProcessSpark Cloud AG (München) kurz zuvor einen Sicherheitshinweis zu CVE-2026-0712 herausgegeben hatte, den Patch aber erst in der Nacht zum 29.04.2026 eingespielt habe — obwohl er laut SLA bis 20.03.2026 hätte aufgespielt sein müssen.

RA Drost: \*,„Das ist erheblich. Das werden wir genau prüfen. Wenn ProcessSpark die Patchpflicht verletzt hat, haben Sie möglicherweise erhebliche Schadensersatzansprüche.“\*

### 3. Handlungsplan (im Gespräch vereinbart)

| Nr. | Maßnahme                                            | Zuständig              | Frist      |
|-----|-----------------------------------------------------|------------------------|------------|
| 1   | Mandatserteilung durch Frau Wallbruck (schriftlich) | Wallbruck              | 06.05.2026 |
| 2   | Strafanzeige ZAC Mainz vorbereiten und erstatten    | RA Drost               | 07.05.2026 |
| 3   | Versicherungsmeldung CyberCovered AG                | RA Drost + Wallbruck   | 07.05.2026 |
| 4   | BSI-Meldung vorbereiten                             | RA Drost               | 07.05.2026 |
| 5   | Art.-33-DSGVO-Meldung LfDI RLP                      | RA Drost               | 08.05.2026 |
| 6   | Forensikfirma beauftragen                           | Wallbruck / Berkenfeld | 06.05.2026 |
| 7   | Vertragsanalyse ProcessSpark                        | RA Drost               | 08.05.2026 |
| 8   | Betriebsrat informieren                             | Wallbruck / HR         | 11.05.2026 |
| 9   | Mitarbeiter BEM-Betroffene informieren              | Wallbruck / HR         | 11.05.2026 |
| 10  | Kundenkommunikation Frischbäcker AG, Backhaus Süd   | RA Drost + Wallbruck   | 12.05.2026 |

### 4. Mandatserteilung

Theresia Wallbruck erteilte RA Lukas Drost und der Kanzlei Drost & Pekonkur um 09:00 Uhr die schriftliche Vollmacht zur umfassenden Rechtsvertretung der Frischetrans Mittelrhein GmbH in der Angelegenheit des Cyber-Vorfalles vom 06.05.2026. Die Vollmacht ist aktenkundig (Anlage: Vollmacht\_Wallbruck\_Frischetrans\_06052026.pdf — im Mandantenordner physisch hinterlegt).

### 5. Besonderheiten / Auffälligkeiten

- Frau Wallbruck erwähnte, dass in den Tagen vor dem Angriff (01.–05.05.2026) ungewöhnlich viele Phishing-E-Mails im Unternehmen beobachtet worden seien. Dies wurde dem Forensikteam mitgeteilt (möglicher Zusammenhang mit dem Angriffsvektor).
- IT-Leiter Berkenfeld (telefonisch) berichtete, dass die Firewall-Firmware seit Oktober 2025 nicht aktualisiert worden sei (Pflege durch InsoTec Systems). Dies wird im Rahmen der Gesamtverantwortlichkeitsanalyse zu prüfen sein.

- Frau Wallbruck äußerte Sorge um die Belegschaft: „Die Leute wissen noch gar nicht, dass ihre Personalakten jetzt irgendwo im Internet landen könnten.“\* RA Drostens erläuterte die Notwendigkeit der Mitarbeiterinformation nach Art. 34 DSGVO.

## 6. Nächster Termin

Folgebegesprechung telefonisch: 08.05.2026, 10:00 Uhr. Persönliches Strategiegelgespräch: 13.05.2026, 14:00 Uhr, Kanzlei Drostens & Pekonkur.

\*Notiz erstellt durch: RA Lukas Drostens\*

\*Datum der Erstellung: 06.05.2026, 10:30 Uhr\*

\*Geprüft: Drostens, 06.05.2026\*

Datei: 05\_meldung\_lfdi\_rlp\_art\_33\_dsgvo.md

## Meldung an den LfDI Rheinland-Pfalz gemäß Art. 33 DSGVO

**Aktenstück:** 05

**Datum der Übermittlung:** 08.05.2026, 22:45 Uhr

**Übermittlungsweg:** Online-Meldeportal LfDI RLP (<https://www.datenschutz.rlp.de/meldung>)

**Referenznummer LfDI:** LfDI-RLP-2026-0508-4419

**Bearbeiter:** RA Lukas Drostens für Frischetrans Mittelrhein GmbH

### Meldeformular — Art. 33 DSGVO

**An:** Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI RLP)  
Hintere Bleiche 34 55116 Mainz

**Meldung einer Verletzung des Schutzes personenbezogener Daten** gemäß Art. 33 Abs. 3 DSGVO

#### Abschnitt 1: Angaben zum Verantwortlichen

**Name des Verantwortlichen:** Frischetrans Mittelrhein GmbH

**Vertreten durch:** Theresia Wallbruck (Geschäftsführerin)

**Anschrift:** Binger Straße 142, 55131 Mainz

**Handelsregister:** HRB 44821, Amtsgericht Mainz

**Kontakt für Rückfragen:** RA Lukas Drostens, Kanzlei Drostens & Pekonkur Schillerstraße 14, 55116 Mainz  
Telefon: +49 6131 2240-0 E-Mail: [l.drostens@drosten-pekonkur.de](mailto:l.drostens@drosten-pekonkur.de)

**Datenschutzbeauftragter (extern):** Markus Feilke, Dipl.-Inform. (Datenschutzkanzlei Rhein-Main) E-Mail: [m.feilke@datenschutz-rhein-main.de](mailto:m.feilke@datenschutz-rhein-main.de) Telefon: +49 6131 9944-11

#### Abschnitt 2: Art der Verletzung des Schutzes personenbezogener Daten

**Art der Verletzung (§ Art. 4 Nr. 12 DSGVO):** ■ Verlust der Verfügbarkeit ■ Verlust der Vertraulichkeit ■ Verlust der Integrität

**Beschreibung des Vorfalls:** In der Nacht vom 05. auf den 06.05.2026 wurde das IT-System der Frischetrans Mittelrhein GmbH Opfer eines Ransomware-Angriffs durch die kriminelle Gruppe „AkiraNext“. Das ERP-System (SAP S/4HANA, on-premises, Serverstandort Mainz) sowie weitere interne IT-Systeme wurden vollständig verschlüsselt.

Forensische Analyse ergab, dass die Angreifer bereits ab dem 04.05.2026 (ca. 22:44 Uhr) Zugang zu den Systemen hatten und vor der Aktivierung der Ransomware ca. 2,1 TB an Unternehmensdaten aus dem internen Netzwerk exfiltriert haben. Der initiale Zugang erfolgte über die ungepatchte SAP-Schwachstelle CVE-2026-0712.

**Zeitpunkt der Entdeckung:** 06.05.2026, 04:17 Uhr (Detektion durch SOC-System der InsoTec Systems GmbH, Frankfurt)

**Zeitpunkt der Kenntnisnahme durch den Verantwortlichen:** 06.05.2026, 04:52 Uhr (Benachrichtigung von Theresia Wallbruck, GF)

### **Abschnitt 3: Betroffene Personen und Kategorien**

#### **Kategorien betroffener Personen:**

##### **1. Kunden (Unternehmen):**

18 Geschäftskunden der Frischetrans Mittelrhein GmbH. Abgeflossene Daten umfassen Kundenstammdaten (Firmendaten, Ansprechpartner, Vertrags- und Lieferdetails, Bankverbindungen für die Abrechnung).

##### **2. Mitarbeiterinnen und Mitarbeiter:**

280 aktive Beschäftigte, davon 38 Mitarbeiter mit besonders sensiblen Gesundheitsdaten aus laufenden oder abgeschlossenen Betrieblichen Eingliederungsmanagement-Verfahren (BEM). Bei diesen 38 Personen sind Diagnosen, Therapieverläufe und ärztliche Bescheinigungen in den Personalakten enthalten.

Darüber hinaus: Personalstammdaten (Name, Adresse, Geburtsdatum, Sozialversicherungsnummer, Bankverbindung, Lohnabrechnung) aller 280 Mitarbeiter.

**Ungefähre Zahl betroffener Personen:** 298 natürliche Personen (280 Mitarbeiter + ca. 18 Kontaktpersonen bei Firmenkunden; die Kunden selbst sind juristische Personen und fallen nicht unmittelbar unter Art. 33 DSGVO).

**Besondere Kategorien (Art. 9 DSGVO):** ■ Gesundheitsdaten (BEM-Verfahren, 38 Mitarbeiter)

### **Abschnitt 4: Voraussichtliche Folgen der Verletzung**

Die Verletzung des Schutzes personenbezogener Daten hat voraussichtlich folgende Folgen:

- 1. Identitätsdiebstahl und Betrug:** Durch den Abfluss von Personalstammdaten inkl. Bankverbindungen besteht für die betroffenen Mitarbeiter ein erhöhtes Risiko von Kontomissbrauch und Identitätsdiebstahl.
- 2. Bloßstellung und Diskriminierung:** Die abgeflossenen BEM-Gesundheitsdaten (Diagnosen, Therapieverläufe) können im Falle einer Veröffentlichung durch die Tätergruppe zu erheblichen Nachteilen für die betroffenen 38 Mitarbeiter führen (soziale Stigmatisierung, potenzielle Auswirkungen auf Versicherbarkeit oder Kreditwürdigkeit).
- 3. Geschäftliche Nachteile für Kunden:** Vertrauliche Vertrags- und Konditionsinformationen können von Wettbewerbern genutzt werden.



4. **Reputationsschaden:** Veröffentlichung der Daten auf Leakseiten der Tätergruppe droht.

## **Abschnitt 5: Getroffene und geplante Maßnahmen**

### **Bereits getroffene Maßnahmen:**

- Sofortige Abschottung aller betroffenen Systeme (Network Kill, 06.05.2026, 05:35 Uhr)
- Beauftragung forensischer Spezialisten (CyberForensik RheinMain GmbH)
- Strafanzeige bei ZAC Mainz erstattet (07.05.2026, AZ: 421 UJs 6611/26)
- Meldung an BSI Außenstelle Frankfurt (07.05.2026)
- Einleitung der Wiederherstellung aus Backup-Systemen
- Mandatierung von RA Lukas Drosten (Kanzlei Drosten & Pekonkur)
- Meldung an Cyber-Versicherer CyberCovered AG (07.05.2026)

### **Geplante Maßnahmen:**

- Benachrichtigung der betroffenen Mitarbeiter gemäß Art. 34 DSGVO (geplant: 11.05.2026)
- Einleitung einer Datenschutz-Folgenabschätzung (DSFA) für die Verarbeitung von BEM-Gesundheitsdaten (Art. 35 DSGVO)
- Vollständige forensische Aufarbeitung des Angriffsverlaufs
- Implementierung eines überarbeiteten Patch-Management-Prozesses
- Überprüfung und Erneuerung der Firewall-Konfiguration
- Ggf. Schadensersatzforderungen gegen IT-Dienstleister

## **Abschnitt 6: Angaben zum Datenschutzbeauftragten**

Externer Datenschutzbeauftragter ist vorhanden (siehe Abschnitt 1).

## **Abschnitt 7: Sonstige Hinweise**

Diese Meldung erfolgt auf Basis der zum Zeitpunkt der Übermittlung (08.05.2026, 22:45 Uhr) vorliegenden Erkenntnisse. Die forensische Untersuchung ist noch nicht abgeschlossen. Eine Ergänzungsmeldung mit vollständigen Befunden des forensischen Abschlussberichts wird innerhalb von 14 Tagen (bis 22.05.2026) eingereicht.

Das Unternehmen hat sich bei der Vorbereitung dieser Meldung anwaltlicher Beratung bedient (RA Lukas Drosten, Fachanwalt für IT-Recht).

## **Rechtsgrundlagen**

- Art. 33 Abs. 1 DSGVO: Meldepflicht des Verantwortlichen an Aufsichtsbehörde binnen 72 Stunden
- Art. 33 Abs. 3 DSGVO: Inhaltliche Anforderungen der Meldung
- Art. 33 Abs. 4 DSGVO: Gestuftes Meldesystem bei unvollständigen Informationen
- Erwägungsgrund 87 DSGVO: Unverzüglichkeit der Meldung
- § 42 BDSG: Strafvorschriften BDSG (ergänzend)

Zur Rechtslage bei gestuften Meldungen im Ransomware-Kontext vgl. auch Orientierungshilfe der Datenschutzkonferenz (DSK) „Ransomware: Meldung und Benachrichtigung“ (Stand 2023/2024).



Mainz, den 08.05.2026

RA Lukas Drostens Kanzlei Drostens & Pekonkur (handelnd für und im Auftrag der Frischetrans Mittelrhein GmbH)

\*[Elektronisch signiert und über das LfDI-Meldeportal übermittelt — Empfangsbestätigung Ref. LfDI-RLP-2026-0508-4419 liegt vor]\*

Datei: 06\_meldung\_bsi\_nis2.md

## Meldung an das BSI gemäß NIS2-Umsetzungsgesetz (NIS2UmsuG)

Aktenstück: 06

Datum der Übermittlung: 07.05.2026, 16:30 Uhr

Übermittlungsweg: BSI-MELDEPF-Portal (elektronisch)

BSI-Referenznummer: BSI-REF-2026-1847

Bearbeiter: RA Lukas Drostens für Frischetrans Mittelrhein GmbH

### Rechtliche Vorbemerkung: NIS2-Relevanz von Frischetrans

#### Einordnung in den Geltungsbereich der NIS2-Richtlinie

Die NIS2-Richtlinie (Richtlinie (EU) 2022/2555) wurde in Deutschland durch das **Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuG)** umgesetzt, das am 01.11.2024 in Kraft getreten ist.

Die Einordnung von Frischetrans Mittelrhein GmbH in den Geltungsbereich des NIS2UmsuG ergibt sich aus folgenden Überlegungen:

**Sektor:** Frischetrans ist im Bereich der **Lebensmittelversorgungskette** (B2B-Frischel Logistik für Großbäckereien) tätig. Der Sektor „Lebensmittel“ ist gemäß Anhang I NIS2-Richtlinie als **wichtiger Sektor** eingestuft.

**Größenkriterium:** Frischetrans beschäftigt 280 Mitarbeiter und erzielt einen Jahresumsatz von ca. 38 Mio. EUR. Damit überschreitet das Unternehmen die Schwelle für **mittelgroße Unternehmen** ( $\geq 50$  Mitarbeiter oder  $\geq 10$  Mio. EUR Umsatz) gemäß Art. 2 NIS2-Richtlinie. Es fällt somit als **wichtige Einrichtung** (nicht: wesentliche Einrichtung) in den Anwendungsbereich.

**Begründung der Versorgungsrelevanz:** Frischetrans beliefert die Großbäckereien Frischbäcker AG und Backhaus Süd, die ihrerseits Supermarktfilialisten und Kantinen in der Metropolregion Rhein-Main-Neckar beliefern. Ein Ausfall der Frischel Logistik beeinträchtigt die Lebensmittelversorgung einer signifikanten Bevölkerungsgruppe. Das BSI hat den Angriff auf Basis dieser Argumentation als meldepflichtig akzeptiert (Bestätigungsschreiben BSI liegt vor).

### Formelle Meldung

**An:** Bundesamt für Sicherheit in der Informationstechnik (BSI) Außenstelle Frankfurt Gutleutstraße 163, 60327 Frankfurt am Main

**Meldung eines erheblichen Sicherheitsvorfalls** gemäß § 31 NIS2UmsuG (Meldepflichten wichtiger Einrichtungen)

### Meldender Verantwortlicher

**Name:** Frischetrans Mittelrhein GmbH

**Sitz:** Binger Straße 142, 55131 Mainz

**Einrichtungstyp:** Wichtige Einrichtung (Sektor: Lebensmittel/Versorgungskette)

**Ansprechpartner (IT-Sicherheit):** Franz Berkenfeld, IT-Leiter

**Bevollmächtigter RA:** Lukas Drost, Kanzlei Drost & Pekonkur, Mainz

### Angaben zum Vorfall

**Art des Vorfalls:** Ransomware-Angriff (Verschlüsselung und Datenexfiltration) durch die kriminelle Gruppe „AkiraNext“.

#### Betroffene Systeme:

- SAP S/4HANA ERP-System (on-premises, vollständig verschlüsselt)
- Telematik-Schnittstellen (GPS-Tracking, Temperaturüberwachung, Fahrerdisposition)
- Fileserver (3 Systeme verschlüsselt)
- Active Directory / Domain Controller (kompromittiert, nicht verschlüsselt)

#### Zeitpunkt:

- Vermutlicher Erstzugang: 04.05.2026, ca. 22:44 Uhr
- Aktivierung Ransomware: 06.05.2026, ca. 04:17–04:31 Uhr
- Entdeckung: 06.05.2026, 04:17 Uhr

**Angriffsvektor:** Ungepatchte SAP-Schwachstelle CVE-2026-0712 (SAP NetWeaver Application Server ABAP — Remote Code Execution). Das kritische Sicherheitsupdate war laut Vertrag mit dem ERP-Dienstleister ProcessSpark Cloud AG bis 20.03.2026 einzuspielen, wurde jedoch erst am 28./29.04.2026 aufgespielt.

#### Schadwirkung:

1. **Verfügbarkeit:** Vollständiger Ausfall des ERP-Systems für ca. 7 Tage; Ausfall Telematik-System für ca. 4 Tage; 47 von 64 LKW ohne Telematik-Anbindung; geplante Frischlieferungen für 37 Kunden am 07.05.2026 teils nicht durchführbar.
2. **Vertraulichkeit:** Exfiltration von ca. 2,1 TB Daten (Kundenstammdaten 18 Kunden, Personalakten 280 Mitarbeiter inkl. Gesundheitsdaten BEM 38 Mitarbeiter, Finanzdaten Q1/2026, Vertragsdaten).
3. **Wirtschaftlicher Schaden (vorläufige Schätzung):** ca. 850.000–1.200.000 EUR (Wiederherstellungskosten, Betriebsausfall, Forensik, Rechtskosten, ggf. Bußgelder).

### Bewertung der Erheblichkeit (§ 31 Abs. 2 NIS2UmsuG)

Der Vorfall ist als **erheblich** einzustufen, da:

1. Er eine erhebliche Betriebsunterbrechung verursacht hat (vollständiger ERP-Ausfall > 24 h)

2. Er zu einem signifikanten finanziellen Schaden geführt hat (> 500.000 EUR)
3. Er die Versorgungssicherheit der Bevölkerung beeinträchtigt hat (Frischelogistik für Lebensmittelketten)
4. Er personenbezogene Daten in großem Umfang betrifft (verbunden mit DSGVO-Meldung)

### **Getroffene Sicherheitsmaßnahmen**

- Network Kill: 06.05.2026, 05:35 Uhr (Trennung aller Systeme vom Netz)
- Beauftragung forensischer Spezialisten
- Koordination mit ZAC Mainz (Strafanzeige)
- Schrittweise Wiederherstellung aus Backup (Backup-Stand 03.05.2026)
- Überarbeitung Patch-Management-Prozess eingeleitet
- Überprüfung Firewall-Konfiguration und Netzwerksegmentierung beauftragt
- Implementierung MFA für alle administrativen Zugänge eingeleitet

### **Stufenweise Meldung nach § 31 NIS2UmsuG**

Diese Meldung ist die **Erstmeldung** (innerhalb 24 Stunden nach Kenntniserlangung der erheblichen Auswirkungen, § 31 Abs. 3 Nr. 1 NIS2UmsuG).

Ein **Folgebericht** (detaillierter Zwischenbericht, § 31 Abs. 3 Nr. 2 NIS2UmsuG) wird innerhalb von 72 Stunden nach Erstmeldung (bis 10.05.2026, 16:30 Uhr) übermittelt.

Ein **Abschlussbericht** (§ 31 Abs. 3 Nr. 3 NIS2UmsuG) folgt innerhalb eines Monats.

### **Koordinationshinweis**

Die Frischetrans Mittelrhein GmbH hat parallel eine Datenschutzpannen-Meldung gemäß Art. 33 DSGVO an den LfDI Rheinland-Pfalz übermittelt (Ref. LfDI-RLP-2026-0508-4419). Eine Abstimmung beider Behörden wird erbeten.

### **Frankfurt/Mainz, den 07.05.2026**

RA Lukas Drostens Kanzlei Drostens & Pekonkur, Mainz (handelnd für und im Auftrag der Frischetrans Mittelrhein GmbH)

### **Anlage: BSI-Meldebestätigung**

\*Gemäß BSI-Bestätigungsschreiben vom 07.05.2026, 18:45 Uhr (automatische Eingangsbestätigung über das MELDEPF-Portal) wurde die Meldung unter Referenznummer BSI-REF-2026-1847 erfasst. Das Bestätigungs-PDF ist als Anlage „pdfs/bsi\_meldbestaetigung.pdf“ in der Akte hinterlegt.\*

### **Rechtliche Grundlagen (Nachweise)**

- Richtlinie (EU) 2022/2555 (NIS2-Richtlinie), ABl. L 333 vom 27.12.2022
- Gesetz zur Umsetzung der NIS-2-Richtlinie (NIS2UmsuG), BGBl. 2024 I Nr. 387
- BSI-Gesetz (BSiG) i.d.F. nach NIS2-Umsetzung
- BSI-Kritisverordnung (BSI-KritisV) i.d.F. 2025

- Erwägungsgründe 102–104 NIS2-Richtlinie zur Meldepflicht

Zur NIS2-Klassifikation von Logistikunternehmen im Lebensmittelsektor vgl. ENISA-Leitlinien „NIS2 Sectoral Classification“ (2024, abrufbar unter <https://www.enisa.europa.eu>).

Datei: 07\_strafanzeige\_zac\_mainz.md

## Strafanzeige bei der ZAC Mainz — Ransomware-Angriff

**Aktenstück:** 07

**Datum:** 07.05.2026

**Aktenzeichen Strafverfolgung:** 421 UJs 6611/26

**Erstattet durch:** RA Lukas Drosten für Frischetrans Mittelrhein GmbH

**Adressat:** Kriminalpolizei Mainz, Zentrale Ansprechstelle Cybercrime (ZAC), Valenciaplatz 1, 55118 Mainz

### Strafanzeige

mit dem Antrag auf Strafverfolgung

Kanzlei Drosten & Pekonkur Schillerstraße 14 55116 Mainz Telefon: +49 6131 2240-0  
l.drosten@drosten-pekongkur.de

Mainz, den 07.05.2026

An Kriminalpolizei Mainz Zentrale Ansprechstelle Cybercrime (ZAC) Valenciaplatz 1 55118 Mainz

### Strafanzeige gegen Unbekannt

wegen:

- Ausspähen von Daten (§ 202a StGB)
- Abfangens von Daten (§ 202b StGB)
- Datenveränderung (§ 303a StGB)
- Computersabotage (§ 303b StGB)
- Erpressung (§ 253 StGB)
- Computerbetrugs (§ 263a StGB)
- Bandenmäßiger Erpressung (§ 253 Abs. 4 StGB i.V.m. § 260 StGB)

### I. Vollmacht und Vertretung

Ich zeige an, dass ich die Frischetrans Mittelrhein GmbH, Binger Straße 142, 55131 Mainz, vertreten durch Geschäftsführerin Theresia Wallbruck, anwaltlich vertrete. Eine Vollmacht liegt dieser Anzeige bei.

### II. Sachverhalt

In der Nacht vom 05. auf den 06.05.2026 wurde das Unternehmens-IT-System der Frischetrans Mittelrhein GmbH Opfer eines schwerwiegenden Ransomware-Angriffs. Die Tätergruppe agiert unter dem Namen „AkiraNext“.

### 1. Unbefugter Zugang und Datenabfluss

Netzwerk-Logs belegen, dass die Angreifer bereits ab dem 04.05.2026, ca. 22:44 Uhr, unbefugt Zugang zu den Systemen der Anzeigerstatterin erlangt hatten. Während der Verweildauer von ca. 29,5 Stunden führten die Täter eine laterale Bewegung durch das interne Netzwerk durch und exfiltrierten ca. 2,1 TB an Daten.

Der initiale Zugang erfolgte vermutlich über die ungepatchte SAP NetWeaver-Schwachstelle CVE-2026-0712. Eine forensische Untersuchung durch die CyberForensik RheinMain GmbH ist eingeleitet; die vollständigen forensischen Ergebnisse werden nachgereicht.

Die exfiltrierten Daten umfassen:

- Kundenstammdaten von 18 Geschäftskunden (Vertrags-, Konditions-, Kontaktdaten)
- Personalakten von 280 Mitarbeiterinnen und Mitarbeitern (inkl. Bankverbindungen, SV-Nummern)
- Gesundheitsdaten aus BEM-Verfahren von 38 Mitarbeiterinnen und Mitarbeitern (besonders sensible Daten)
- Finanzdaten (Buchungsdaten Q1/2026)
- Vertragsdaten und interne Kommunikation

### 2. Ransomware-Angriff und Verschlüsselung

Am 06.05.2026 um ca. 04:17–04:31 Uhr aktivierten die Angreifer die Ransomware „AkiraNext“. Folgende Systeme wurden vollständig verschlüsselt:

- SAP S/4HANA Applikationsserver (2 Systeme: FT-ERP-PROD-01, FT-ERP-PROD-02)
- Datenbankserver (FT-DB-01)
- Fileserver (3 Systeme)
- Telematik-Gateway

Auf allen betroffenen Systemen wurde ein Erpressungsschreiben hinterlassen (als Desktop-Hintergrund und als Datei !!! AKIRA\_NEXT\_README.txt).

### 3. Erpressung

Die Tätergruppe fordert die Zahlung von **1.450.000 USD in Monero** (Kryptowährung) innerhalb von 7 Tagen (bis 13.05.2026, 23:59 Uhr UTC). Bei Nichtzahlung drohen die Täter mit der Veröffentlichung der abgeflossenen Daten auf ihrer Leakseite im Tor-Netzwerk.

Die vollständigen Angaben zu Wallet-Adresse und Onion-URL des Erpressungsschreibens werden als Anlage 3 (Erpressungsschreiben) im Original beigelegt.

### 4. Wirtschaftlicher Schaden

Der Gesamtschaden der Anzeigerstatterin beläuft sich nach vorläufiger Schätzung auf:

| Schadensposition                  | Betrag (geschätzt)      |
|-----------------------------------|-------------------------|
| Wiederherstellungskosten IT       | ca. 180.000–220.000 EUR |
| Betriebsausfall Logistik (7 Tage) | ca. 320.000–450.000 EUR |

| Schadensposition              | Betrag (geschätzt)                   |
|-------------------------------|--------------------------------------|
| Forensikkosten                | ca. 45.000–65.000 EUR                |
| Rechts- und Beratungskosten   | ca. 80.000–120.000 EUR               |
| DSGVO-Bußgeldrisiko           | bis 500.000 EUR (zu prüfen)          |
| Reputationsschaden            | nicht bezifferbar                    |
| <b>**Gesamt (vorläufig)**</b> | <b>**ca. 625.000–1.355.000 EUR**</b> |

### III. Straftaten

**§ 202a StGB (Ausspähen von Daten):** Die Täter erlangten unter Überwindung von Zugangssicherungen (Firewalls, Authentifizierungssysteme) unbefugt Zugang zu den gesicherten Daten der Anzeigerstatterin. Der Tatbestand des § 202a Abs. 1 StGB ist erfüllt.

**§ 202b StGB (Abfangen von Daten):** Durch laterale Bewegungen im Netzwerk wurden Datenpakete aus internen Übertragungen abgefangen und exfiltriert. Tatbestand § 202b StGB ist erfüllt.

**§ 303a StGB (Datenveränderung):** Durch die Verschlüsselung wurden die Daten rechtswidrig unbrauchbar gemacht (§ 303a Abs. 1 StGB). Es liegt ein schwerer Fall vor (§ 303a Abs. 2 i.V.m. § 303b Abs. 3 StGB), da der wirtschaftliche Schaden erheblich ist.

**§ 303b StGB (Computersabotage):** Der Angriff auf das ERP-System und die Telematik-Infrastruktur eines Unternehmens der Lebensmittelversorgungskette stellt eine Computersabotage i.S.d. § 303b Abs. 1 Nr. 2 StGB dar. Es handelt sich möglicherweise um einen Angriff auf eine Einrichtung von erheblicher Bedeutung (§ 303b Abs. 4 StGB).

**§ 253 StGB (Erpressung):** Die Täter nötigten die Anzeigerstatterin durch die Androhung der Veröffentlichung gestohlener Daten und durch die Verweigerung der Entschlüsselung zur Zahlung eines erheblichen Geldbetrages. Die Drohung ist ernstgemeint und geeignet, eine Entschlussfassung zu beeinflussen.

**§ 263a StGB (Computerbetrug):** Durch unbefugtes Einwirken auf Datenverarbeitungsabläufe beabsichtigten die Täter, sich rechtswidrige Vermögensvorteile zu verschaffen.

### IV. Beweismittel

Als Anlage werden beigefügt:

1. Vollmacht der Frischetrans Mittelrhein GmbH
2. Netzwerk-Logs mit Nachweis des Datenabflusses (Forensikbericht-Auszug, vorläufig)
3. Erpressungsschreiben (Original inkl. Wallet-Adresse und Onion-URL — vertraulich)
4. Screenshot-Dokumentation der verschlüsselten Systeme
5. Hash-Werte der Ransomware-Datei (ermittelt durch InsoTec Systems GmbH)
6. Vorläufiger forensischer Erstbericht (CyberForensik RheinMain GmbH)

Ergänzende Beweismittel (vollständiger forensischer Abschlussbericht, Server-Logs) werden nachgereicht.

### V. Anträge

1. Es wird beantragt, wegen der vorgenannten Straftaten gegen unbekannte Täter zu ermitteln.

2. Es wird beantragt, die vorliegenden Beweismittel zu sichern und ggf. eine internationale Rechtshilfeanfrage an die zuständigen Behörden (Europol EC3, FBI Cyber Division) zu richten.
3. Es wird beantragt, die Daten der Erpresser-Infrastruktur (Tor-Adressen, Monero-Wallet) mit internationalen Datenbanken abzugleichen.
4. Es wird beantragt, die Anzeigerstatteerin über den Fortgang der Ermittlungen zu informieren (§ 406e StPO analog für Körperschaften).

## VI. Hinweis

Eine Lösegeldzahlung erfolgt nicht und ist auch nicht geplant. Kryptowährungstransaktionen wurden seitens der Anzeigerstatteerin nicht vorgenommen.

Die BSI Außenstelle Frankfurt sowie der LfDI Rheinland-Pfalz wurden ebenfalls über den Vorfall informiert. Eine Abstimmung mit den Ermittlungsbehörden bezüglich der laufenden forensischen Untersuchung ist ausdrücklich erwünscht.

## Mainz, den 07.05.2026

RA Lukas Drostent Kanzlei Drostent & Pekonkur

\*Für die Anzeigerstatteerin:\* Frischetrans Mittelrhein GmbH gez. Theresia Wallbruck (Geschäftsführerin)

\*Aktenzeichen vergeben durch ZAC Mainz: 421 UJs 6611/26\*

\*Sachbearbeiterin: KHK'in Sabine Erhart, ZAC Mainz\*

Datei: 08\_vertragsanalyse\_processspark\_sla.md

# Vertragsanalyse ProcessSpark Cloud AG — SLA-Bewertung und Pflichtverletzung

**Aktenstück:** 08

**Datum der Analyse:** 08.–10.05.2026

**Mandantin:** Frischetrans Mittelrhein GmbH

**Gegner:** ProcessSpark Cloud AG, Leopoldstraße 88, 80802 München

**Bearbeiter:** RA Lukas Drostent, Fachanwalt für IT-Recht

## 1. Vertragsgrundlage

Zwischen der Frischetrans Mittelrhein GmbH und der ProcessSpark Cloud AG besteht ein **IT-Betriebsvertrag (SaaS- und Managed-Service-Vertrag)** vom 15.03.2021, zuletzt geändert durch Nachtrag 3 vom 01.07.2024 (nachfolgend: „Vertrag“). Der Vertrag hat eine Laufzeit bis 31.12.2027 mit einer Kündigungsfrist von 6 Monaten zum Jahresende.

### Vertragsgegenstand (§ 1 Vertrag)

ProcessSpark Cloud AG verpflichtet sich zur:

1. Bereitstellung, Betrieb und Wartung des ERP-Systems SAP S/4HANA (Lizenz-Management, Hosting auf ProcessSpark-Infrastruktur oder on-premises-Betreuung)

2. Durchführung von Sicherheitsupdates und Patches gemäß herstellerseitigem Release-Management
3. Gewährleistung der Systemverfügbarkeit von mind. 99,5 % p.m. (Kernbetriebszeiten: Mo–Fr 06:00–22:00 Uhr)
4. Incident-Response-Service Level: P1 (Kritisch) — Erstreaktion binnen 30 Minuten, Lösung binnen 4 Stunden

### SLA-Bestimmungen (§ 8 Vertrag)

| Service Level | Definition                         | Reaktionszeit | Lösungszeit |
|---------------|------------------------------------|---------------|-------------|
| P1 — Kritisch | Systemausfall, Datenverlust-Risiko | 30 Minuten    | 4 Stunden   |
| P2 — Hoch     | Erhebliche Funktionseinschränkung  | 2 Stunden     | 8 Stunden   |
| P3 — Mittel   | Eingeschränkte Funktion            | 4 Stunden     | 24 Stunden  |
| P4 — Niedrig  | Geringfügige Störung               | 8 Stunden     | 72 Stunden  |

### Patchmanagement-Klausel (§ 12 Vertrag, Nachtrag 3)

\*Auszug § 12 Abs. 2 Nachtrag 3:\*

> „ProcessSpark Cloud AG verpflichtet sich, sicherheitsrelevante Patches und Updates für das SAP S/4HANA-System, insbesondere für Schwachstellen mit CVSS-Score 7,0 und höher (High und Critical), innerhalb von **30 Tagen** nach offizieller Bereitstellung durch den Hersteller SAP SE einzuspielen. Für Schwachstellen mit CVSS-Score 9,0 und höher (Critical) beträgt die Frist **14 Tage**. Ausnahmen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers.“

### SLA-Pönale (§ 14 Vertrag)

\*Auszug § 14 Abs. 3:\*

> „Bei nachgewiesener schuldhafter Verletzung der Patchmanagement-Fristen gemäß § 12 Abs. 2 hat der Auftragnehmer für je angefangene 7 Tage Verzug eine Vertragsstrafe in Höhe von **0,5 % der monatlichen Vergütung** zu leisten, maximal jedoch **5 % der monatlichen Vergütung** (Höchstbetrag). Dies schließt weitergehende Schadensersatzansprüche nicht aus.“

Monatliche Vergütung: 14.800 EUR netto.

## 2. Analyse der Pflichtverletzung CVE-2026-0712

### 2.1 Zeitlinie CVE-2026-0712

| Datum      | Ereignis                                                                                           |
|------------|----------------------------------------------------------------------------------------------------|
| 18.02.2026 | SAP veröffentlicht Security Note für CVE-2026-0712 (SAP NetWeaver AS ABAP — Remote Code Execution) |
| 18.02.2026 | CVSS-Score: <b>**9.8 (Critical)**</b> — kritischste Einstufung                                     |
| 18.02.2026 | Patch-Frist (14 Tage für Critical): <b>**04.03.2026**</b>                                          |
| 04.03.2026 | Ablauf der 14-Tage-Frist — Patch noch nicht eingespielt                                            |
| 20.03.2026 | Verlängerte Frist nach internem ProcessSpark-Standard (30 Tage) — auch überschritten               |



| Datum          | Ereignis                                                                                |
|----------------|-----------------------------------------------------------------------------------------|
| 28./29.04.2026 | ProcessSpark spielt den Patch tatsächlich ein (Wartungsfenster Nacht 28.04./29.04.2026) |
| 04.05.2026     | AkiraNext nutzt CVE-2026-0712 für initialen Zugang — Patch 5 Tage zuvor war zu spät     |

**Verzugsdauer:** 18.02.2026 (Bekanntgabe) bis 28.04.2026 (Einspielung) = **69 Tage**

**Vertraglich geschuldete Frist (Critical, CVSS 9.8):** 14 Tage

**Überschreitung:** 55 Tage

Alternativ gemessen an der 30-Tage-Frist für „High“: Fälligkeitsdatum 20.03.2026 — tatsächliche Einspielung 28.04.2026 = **39 Tage Verzug**

## 2.2 CVSS-Bewertung CVE-2026-0712

Die Schwachstelle CVE-2026-0712 wurde in der offiziellen SAP Security Note wie folgt beschrieben:

- **Typ:** Remote Code Execution (RCE) in SAP NetWeaver Application Server ABAP
- **CVSS Base Score:** 9.8 (Critical)
- **Attack Vector:** Network
- **Authentication:** None required
- **User Interaction:** None required
- **Verfügbarkeit:** Vollständige Kompromittierung möglich

Diese Einstufung macht CVE-2026-0712 zu einer der kritischsten SAP-Schwachstellen des Jahres 2026. Der BSI und CERT@VDE hatten eigene Warnungen herausgegeben.

## 2.3 Verschulden der ProcessSpark Cloud AG

Der Verzug von ProcessSpark bei der Einspielung des Patches ist schuldhaft:

1. **Kenntnis:** Die Schwachstelle und der verfügbare Patch waren seit 18.02.2026 öffentlich bekannt.
2. **Vertragliche Pflicht:** § 12 Abs. 2 Nachtrag 3 des Vertrages sieht für Critical-Patches eine 14-Tages-Frist vor.
3. **Keine Ausnahme beantragt:** ProcessSpark hat keine schriftliche Ausnahme-Genehmigung bei der Frischetrans eingeholt.
4. **Kein Hinweis an Mandantin:** ProcessSpark hat die Frischetrans nicht über den bekannten Patch-Rückstand informiert, was einer eigenständigen Pflichtverletzung entspricht (Informationspflicht aus § 241 Abs. 2 BGB).

# 3. Ansprüche der Mandantin

## 3.1 Vertragsstrafe (§ 14 Abs. 3 Vertrag)

Verzug: 55 Tage (über die 14-Tage-Frist hinaus) → 7 angefangene Sieben-Tages-Perioden × 0,5 % = **3,5 % der Monatsvergütung**

Vertragsstrafe: 14.800 EUR × 3,5 % = **518 EUR**

Hinweis: Die vertragliche Pönale ist angesichts des entstandenen Schadens von erheblich geringerem Wert als der Schadensersatzanspruch. Die Pönale ist neben dem Schadensersatz geltend zu machen (§

340 Abs. 2 BGB).

### 3.2 Schadensersatz (§§ 280, 281, 631, 634 BGB i.V.m. Vertrag)

ProcessSpark hat eine vertraglich geschuldete Leistung (rechtzeitiger Sicherheitspatch) schuldhaft nicht rechtzeitig erbracht. Die Kausalität zwischen verspätetem Patch und Ransomware-Angriff ist nach derzeitigem forensischen Befund gegeben (CVE-2026-0712 war der initiale Angriffsvektor).

#### Haftungsumfang:

Nach §§ 280, 281 BGB schuldet ProcessSpark vollen Schadensersatz für den durch die Pflichtverletzung verursachten Schaden. Die Haftungsbeschränkungsklausel im Vertrag (§ 16 Abs. 2: Haftung begrenzt auf einfache Fahrlässigkeit auf 12 Monatsvergütungen = 177.600 EUR) ist im Hinblick auf § 309 Nr. 7 BGB und die Schwere der Pflichtverletzung einer AGB-rechtlichen Prüfung zu unterziehen.

#### Voraussichtliche Schadensposition ProcessSpark:

| Schadensposition                | Betrag                         |
|---------------------------------|--------------------------------|
| IT-Wiederherstellungskosten     | 180.000–220.000 EUR            |
| Betriebsausfallschaden Logistik | 320.000–450.000 EUR            |
| Forensikkosten                  | 45.000–65.000 EUR              |
| Rechtskosten                    | 80.000–120.000 EUR             |
| <b>**Gesamt**</b>               | <b>**625.000–855.000 EUR**</b> |

Eine DSGVO-Bußgeld-Erstattung durch ProcessSpark ist theoretisch möglich, aber rechtlich komplex (DSGVO-Verstöße sind primär dem Verantwortlichen zuzurechnen, Regress gegen Auftragsverarbeiter/IT-Dienstleister möglich).

### 3.3 Kündigung aus wichtigem Grund

Die schwerwiegende Pflichtverletzung (Patch-Rückstand an einer CVSS-9.8-Schwachstelle mit verheerenden Folgen) berechtigt die Frischetrans zur außerordentlichen Kündigung des Vertrages aus wichtigem Grund nach § 626 BGB (Dienstvertrag) bzw. §§ 643, 649 BGB (Werkvertrag). Eine Abmahnung ist bei der Schwere der Pflichtverletzung entbehrlich.

Die Kündigung ist in der Klageandrohung (Aktenstück 10) angekündigt, aber noch nicht ausgesprochen, um Verhandlungsmasse zu erhalten.

## 4. Prozessrechtliche Überlegungen

**Gerichtsstand:** LG Mainz gemäß Gerichtsstandsklausel (§ 18 Vertrag; Gerichtsstand Mainz für Streitigkeiten zwischen den Parteien). Geplantes Aktenzeichen: 3 O 88/26.

**Streitwert:** ca. 625.000–855.000 EUR (je nach Schadensnachweis) + Vertragsstrafenforderung + ggf. DSGVO-Regress → Streitwert aller Voraussicht nach **> 500.000 EUR**.

**Zuständigkeit:** LG Mainz ist sachlich zuständig (§ 71 GVG, Streitwert > 5.000 EUR).

**Beweissicherung:** Forensischer Abschlussbericht (CyberForensik RheinMain GmbH), SAP-Security-Note CVE-2026-0712, Patch-Log ProcessSpark (per Auskunftsanspruch einzufordern), Vertrag inkl. Nachtrag 3.

**Verjährung:** §§ 195, 199 BGB — Verjährungsfrist 3 Jahre ab Jahresende 2026, Ablauf 31.12.2029.

# Pflichtverletzungsanalyse ProcessSpark Cloud AG — CVE-2026-0712

**Aktenstück:** 09

**Datum:** 10.05.2026

**Mandantin:** Frischetrans Mittelrhein GmbH

**Bearbeiter:** RA Lukas Drost, Fachanwalt für IT-Recht

## 1. Technische Beschreibung der Schwachstelle CVE-2026-0712

### 1.1 Schwachstelle

**CVE-Identifikator:** CVE-2026-0712

**Betroffene Software:** SAP NetWeaver Application Server ABAP, Versionen 7.50–7.89 (vor Patch-Level SP15)

**Typ:** Remote Code Execution (RCE) via SSRF und Deserialisierungsfehler im ICM-Subsystem

**CVSS Base Score:** 9.8 (Critical)

**SAP Security Note:** 3411852

**Veröffentlichung:** 18.02.2026 (SAP Patchday Februar 2026)

**Verfügbarer Patch:** SAP ABAP SP15 (Support Package Stack)

**Technische Beschreibung:** Die Schwachstelle ermöglicht einem nicht authentifizierten Angreifer aus dem Netzwerk heraus, beliebigen Code auf dem SAP-Applikationsserver auszuführen. Der Angriff erfordert keine Benutzerinteraktion und keinen gültigen Account. Die Schwachstelle liegt im Internet Communication Manager (ICM) des SAP NetWeaver AS ABAP und wird durch einen Deserialisierungsfehler bei der Verarbeitung von HTTP-Anfragen ausgelöst.

### 1.2 Exploitbarkeit

Zum Zeitpunkt des Angriffs (04./05.05.2026) existierten öffentlich bekannte Proof-of-Concept-Exploits für CVE-2026-0712:

- Exploit-DB Eintrag: EDB-ID 52847 (veröffentlicht 01.03.2026)
- Metasploit-Modul: `exploit/multi/http/sap\_netweaver\_icm\_rce` (verfügbar ab 10.03.2026)

Die leichte Exploitbarkeit war seit März 2026 bekannt und wurde vom BSI in seiner Warnung BSI-2026-0312-SAP-KRITIS ausdrücklich hervorgehoben.

## 2. Pflichtverletzung im Einzelnen

### 2.1 Verletzung der Patchpflicht (§ 12 Nachtrag 3)

ProcessSpark Cloud AG war nach § 12 Abs. 2 Nachtrag 3 des Vertrages verpflichtet, Patches für Schwachstellen mit CVSS-Score  $\geq 9,0$  innerhalb von **14 Tagen** nach Veröffentlichung einzuspielen.

**Frist:** 18.02.2026 + 14 Tage = **04.03.2026**

**Tatsächliche Einspielung:** Nacht 28./29.04.2026

**Verzug:** 55 Tage

## 2.2 Verletzung der Informationspflicht

ProcessSpark hatte die Mandantin zu keinem Zeitpunkt über:

- die Existenz der Schwachstelle CVE-2026-0712 informiert
- den Patch-Rückstand informiert
- mögliche Interim-Maßnahmen (z.B. Deaktivierung des ICM, Netzwerk-Segmentierung) empfohlen

Dies verletzt die vertragliche Nebenpflicht zur Information und Beratung (§ 241 Abs. 2 BGB, sog. Schutz- und Rücksichtnahmepflichten). IT-Dienstleister sind nach ständiger BGH-Rechtsprechung verpflichtet, ihren Auftraggeber auf erkannte oder erkennbare sicherheitsrelevante Risiken hinzuweisen (vgl. BGH, Urteil vom 04.03.2010 — III ZR 79/09, NJW 2010, 1817; BGH, Urteil vom 15.05.2012 — X ZR 75/11).

## 2.3 Verletzung der Firewall-Wartungspflicht (Mitursächlichkeit)

Die forensische Untersuchung ergab, dass die Firewall-Firmware seit Oktober 2025 nicht aktualisiert worden war. Die Netzwerk-Segmentierung entspricht nicht dem Stand der Technik (kein Zero-Trust-Konzept, unzureichende Micro-Segmentierung). Diese Mängel sind dem Pflichtenbereich der InsoTec Systems GmbH (Netzwerkbetreuungsvertrag) zuzurechnen.

**Hinweis für spätere Prozesstaktik:** Möglicherweise besteht eine gesamtschuldnerische Haftung von ProcessSpark Cloud AG und InsoTec Systems GmbH, was die Rechtsdurchsetzung erleichtert. Eine Analyse des InsoTec-Vertrages ist separat zu führen.

# 3. Kausalität zwischen Pflichtverletzung und Schaden

## 3.1 Conditio-sine-qua-non-Test

Der Kausalitätsbeweis lässt sich wie folgt führen:

1. Wäre der Patch CVE-2026-0712 innerhalb der vertragsgemäßen 14-Tage-Frist (bis 04.03.2026) eingespielt worden, wäre die Schwachstelle am 04./05.05.2026 nicht mehr vorhanden gewesen.
2. Die forensische Analyse belegt eindeutig (Log-Auswertung, Malware-Analyse), dass der initiale Zugang über CVE-2026-0712 erfolgte. Ohne diese Schwachstelle wäre der Angriff nicht möglich gewesen.
3. Ergo: Die Pflichtverletzung (verzögerte Patcheinspielung) ist conditio sine qua non für den eingetretenen Schaden.

## 3.2 Adäquanzkausalität

Es entspricht dem gewöhnlichen Lauf der Dinge und der allgemeinen Lebenserfahrung, dass:

- eine über 55 Tage bekannte, öffentlich exploitierbare CVSS-9.8-Schwachstelle in einem unternehmenskritischen ERP-System
- bei aktivem Bedrohungsakteur (AkiraNext war seit 2025 bekannt als SAP-angreifende Gruppe)
- zu einem Ransomware-Angriff führt.

Die Adäquanzkausalität ist gegeben. Ein durchschnittlicher professioneller IT-Dienstleister musste dieses Risiko vorhersehen.

## 3.3 Beweisführung / Beweislast

Die Beweislast für die Pflichtverletzung liegt grundsätzlich beim Gläubiger (Frischetrans). Folgende Beweise sind verfügbar:

- SAP Security Note 3411852 (offizieller Nachweis der Schwachstelle und des Patch-Datums)
- ProcessSpark-Patch-Log (anzufordern per Auskunftsanspruch, § 242 BGB)
- Forensischer Bericht CyberForensik RheinMain GmbH (Angriffsvektor-Nachweis)
- BSI-Warnung BSI-2026-0312-SAP-KRITIS (Beweis für öffentliche Wahrnehmung)
- Metasploit-Zeitstempel (Exploit-Verfügbarkeit)

## 4. Haftungsausschlüsse und Gegenargumente von ProcessSpark

### 4.1 Mögliche Einwände ProcessSpark

**Einwand 1: Höhere Gewalt** ProcessSpark könnte argumentieren, der Ransomware-Angriff sei ein unvorhersehbares Ereignis (höhere Gewalt). Dies ist abzulehnen: Ransomware-Angriffe auf SAP-Systeme sind seit Jahren dokumentiert. CVE-2026-0712 war öffentlich bekannt. Höhere Gewalt scheidet aus.

**Einwand 2: Mitverschulden der Mandantin** ProcessSpark könnte ein Mitverschulden (§ 254 BGB) der Frischetrans geltend machen, etwa wegen unzureichender Netzwerksegmentierung oder fehlender MFA. Dem ist entgegenzuhalten:

- Die Netzwerkwartung war an InsoTec ausgelagert (keine unmittelbare Verantwortung der Frischetrans)
- Die MFA-Anforderung war im Vertrag mit ProcessSpark nicht explizit vereinbart
- Ein verbleibendes Mitverschulden ist realistisch auf 10–20 % zu schätzen

**Einwand 3: Haftungsbeschränkung (§ 16 Vertrag)** Der Vertrag sieht eine Haftungsbeschränkung auf 12 Monatsvergütungen (177.600 EUR) bei einfacher Fahrlässigkeit vor. Diese Klausel ist nach § 309 Nr. 7 lit. b) BGB unwirksam, soweit sie grob fahrlässiges oder vorsätzliches Verhalten erfassen würde. Ein 55-tägiger Patch-Rückstand bei einer CVSS-9.8-Schwachstelle trotz vertraglicher 14-Tages-Pflicht begründet starke Indizien für **grobe Fahrlässigkeit** (bewusste Missachtung erkennbarer Gefahr).

### 4.2 Rechtliche Einschätzung

Die Haftungsbeschränkungsklausel ist mit hoher Wahrscheinlichkeit als unwirksam oder zumindest nicht einschlägig anzusehen (grobe Fahrlässigkeit). ProcessSpark haftet für den Gesamtschaden. Eine Reduzierung um 10–20 % wegen möglichem Mitverschulden ist einzukalkulieren.

## 5. Forderungsschreiben / Weitere Vorgehensweise

Das Klageandrohungsschreiben (Aktenstück 10) wird folgende Forderungen beinhalten:

1. Zahlung der Vertragsstrafe: 518 EUR
2. Zahlung von Schadensersatz: vorläufig 625.000 EUR (vorbehaltlich des forensischen Abschlussberichts)
3. Vorlage der vollständigen Patch-Logs
4. Außerordentliche Kündigung des Vertrages (vorbehalten)
5. Frist: 14 Tage ab Zugang des Schreibens (26.05.2026)

Bei fruchtlosem Fristablauf: Klageerhebung am LG Mainz (AZ geplant: 3 O 88/26).

# Klageandrohungsschreiben an ProcessSpark Cloud AG

**Aktenstück:** 10

**Datum:** 12.05.2026

**Versand:** Per Einschreiben/Rückschein und per E-Mail (legal@processspark.de)\*\*

**Aktenzeichen intern:** DP-2026-0506-FTM / ProcessSpark

Kanzlei Drosten & Pekonkur Rechtsanwälte und Fachanwälte Schillerstraße 14 55116 Mainz Telefon: +49 6131 2240-0 Telefax: +49 6131 2240-99 E-Mail: l.drosten@drosten-pekonkur.de

Mainz, den 12.05.2026

**Per Einschreiben mit Rückschein**

ProcessSpark Cloud AG — Rechtsabteilung / Vorstand — Leopoldstraße 88 80802 München

## Schadensersatz und Vertragsstrafe aus IT-Betriebsvertrag vom 15.03.2021 (mit Nachtrag 3 vom 01.07.2024) — Ransomware-Schaden durch Verletzung der Patchpflicht CVE-2026-0712

**Unsere Mandantin:** Frischetrans Mittelrhein GmbH, Binger Straße 142, 55131 Mainz, vertreten durch GF Theresia Wallbruck

Sehr geehrte Damen und Herren,

wir sind anwaltliche Bevollmächtigte der Frischetrans Mittelrhein GmbH. Vollmacht liegt bei.

Wir wenden uns an Sie wegen schwerwiegender Pflichtverletzungen aus dem zwischen den Parteien bestehenden IT-Betriebsvertrag vom 15.03.2021 (Nachtrag 3 vom 01.07.2024), die zu einem erheblichen Schaden für unsere Mandantin geführt haben.

### I. Sachverhalt

Wie Ihnen bekannt ist, wurde unsere Mandantin in der Nacht vom 05. auf den 06.05.2026 Opfer eines schwerwiegenden Ransomware-Angriffs der kriminellen Gruppe „AkiraNext“. Durch diesen Angriff wurden das gesamte ERP-System (SAP S/4HANA), Fileserver und Telematik-Schnittstellen vollständig verschlüsselt und ca. 2,1 TB an Unternehmensdaten — darunter Personalakten, Kundenstammdaten und Finanzdaten — exfiltriert.

Die forensische Untersuchung durch die CyberForensik RheinMain GmbH (Bericht-ID CRM-2026-FT-01, Zwischenbericht vom 09.05.2026) hat ergeben, dass der initiale Angriffseinstiegspunkt die **Sicherheitslücke CVE-2026-0712** im SAP NetWeaver Application Server ABAP war. Diese Schwachstelle war von SAP SE am **18.02.2026** als kritisch (CVSS 9.8) eingestuft und ein Patch in Form des ABAP Support Package Stack SP15 bereitgestellt worden.

Ihre Gesellschaft hat diesen Patch nach unseren Erkenntnissen erst in der **Nacht vom 28. auf den 29.04.2026** eingespielt — mithin **69 Tage** nach Veröffentlichung und Bereitstellung des Patches.

### II. Pflichtverletzungen Ihrer Gesellschaft

## 1. Verletzung der Patchpflicht (§ 12 Abs. 2 Nachtrag 3)

§ 12 Abs. 2 des Nachtrages 3 verpflichtet Ihre Gesellschaft ausdrücklich, Sicherheitspatches für Schwachstellen mit CVSS-Score  $\geq 9,0$  innerhalb von **14 Tagen** nach Bereitstellung durch den Hersteller einzuspielen.

Die Patchfrist für CVE-2026-0712 lief am **04.03.2026** ab. Tatsächlich wurde der Patch erst am 28./29.04.2026 eingespielt. Der Verzug beträgt damit **55 Tage**.

Diese Pflichtverletzung ist schuldhaft. Öffentliche Warnungen des BSI (BSI-2026-0312-SAP-KRITIS), von ENISA und SAP SE selbst machten die Dringlichkeit des Patches unmissverständlich deutlich. Eine schriftliche Ausnahme-Genehmigung unserer Mandantin für eine Fristverlängerung liegt nicht vor.

## 2. Verletzung der Informationspflicht

Ihre Gesellschaft hat unsere Mandantin zu keinem Zeitpunkt über die Schwachstelle CVE-2026-0712, über den Patch-Rückstand oder über mögliche Schutzmaßnahmen (Netzwerk-Segmentierung, ICM-Deaktivierung) informiert. Dies verletzt die vertragliche Schutz- und Rücksichtnahmepflicht nach § 241 Abs. 2 BGB.

Hätte unsere Mandantin von der Patchlücke gewusst, hätte sie entweder selbst Maßnahmen ergriffen oder Ihre Gesellschaft zur unverzüglichen Einspielung aufgefordert.

## III. Schaden

Der unserer Mandantin durch den Ransomware-Angriff entstandene Schaden ist kausal auf Ihre Pflichtverletzung zurückzuführen. Die Schadenshöhe beläuft sich nach derzeitigem Stand:

| Schadensposition                              | Betrag                       |
|-----------------------------------------------|------------------------------|
| IT-Wiederherstellungskosten                   | 198.500 EUR                  |
| Betriebsausfall Logistik (D+0 bis D+7)        | 387.200 EUR                  |
| Forensikkosten (CyberForensik RheinMain GmbH) | 52.800 EUR                   |
| Anwaltskosten dieser Angelegenheit            | 24.800 EUR (netto, bisherig) |
| DSGVO-Folgekosten (DSB, DSFA)                 | 18.000 EUR                   |
| <b>**Vorläufige Gesamtsumme**</b>             | <b>**681.300 EUR**</b>       |

Eine abschließende Schadensquantifizierung liegt nach Fertigstellung des forensischen Abschlussberichts vor. Wir behalten uns ausdrücklich vor, den Schadensersatzanspruch zu erhöhen.

## IV. Geltend gemachte Ansprüche

Wir machen hiermit namens und in Vollmacht unserer Mandantin folgende Ansprüche geltend:

**1. Vertragsstrafe nach § 14 Abs. 3 des Vertrages:** Für 7 angefangene Sieben-Tages-Perioden des Patchverzugs:  $7 \times 0,5 \% \times 14.800 \text{ EUR} = \mathbf{518,00 \text{ EUR}}$

**2. Schadensersatz nach §§ 280, 241 Abs. 2 BGB i.V.m. dem Vertrag:** Vorläufig **681.300,00 EUR** (vorbehaltlich der Erhöhung nach forensischem Abschlussbericht)



**3. Auskunftserteilung:** Vorlage sämtlicher Patch-Management-Logs, Incident-Response-Protokolle und interner Kommunikation zu CVE-2026-0712 seit dem 18.02.2026 binnen 7 Tagen (bis 19.05.2026).

**4. Ankündigung der außerordentlichen Kündigung:** Wir kündigen an, den IT-Betriebsvertrag vom 15.03.2021 nebst Nachtrag 3 aus wichtigem Grund (§ 626 BGB) außerordentlich und fristlos zu kündigen, sofern bis zum Ablauf der nachstehenden Frist keine Einigung erzielt wird. Ein schuldhafter Patch-Verzug von 55 Tagen bei einer CVSS-9.8-Schwachstelle, der zu einem Schaden von über 680.000 EUR führt, stellt einen wichtigen Grund dar, der eine weitere Zusammenarbeit unzumutbar macht.

## **V. Frist und Konsequenzen bei Untätigkeit**

Wir fordern Sie auf, die unter IV. geltend gemachten Zahlungsansprüche (Vertragsstrafe EUR 518,00 und Schadensersatz vorläufig EUR 681.300,00, gesamt **EUR 681.818,00**) bis spätestens

**Montag, den 26.05.2026**

auf das Konto unserer Mandantin (Kontoverbindung wird auf gesonderte Aufforderung mitgeteilt) zu überweisen sowie die angeforderten Unterlagen vollständig vorzulegen.

Bei fruchtlosem Fristablauf werden wir unsere Mandantin empfehlen, umgehend Klage am Landgericht Mainz zu erheben (geplantes Aktenzeichen: 3 O 88/26). Die Entscheidung über die außerordentliche Kündigung bleibt vorbehalten.

Wir weisen darauf hin, dass sich die Pönale für jeden weiteren Tag der Nichterfüllung erhöhen kann und dass Kosten eines etwaigen Rechtsstreits zu Ihren Lasten gehen.

## **VI. Rechtsgrundlagen**

- § 280 Abs. 1 BGB — Schadensersatz wegen Pflichtverletzung
- § 241 Abs. 2 BGB — Schutzpflichten
- § 254 BGB — Mitverschulden (hier: unserer Mandantin nicht anzunehmen)
- § 626 BGB — außerordentliche Kündigung aus wichtigem Grund
- § 339 BGB — Vertragsstrafe
- § 340 Abs. 2 BGB — Vertragsstrafe neben Schadensersatz
- § 12 Abs. 2 Nachtrag 3 zum Vertrag vom 15.03.2021 — Patchpflicht
- § 14 Abs. 3 Vertrag — Pönalenregelung

Mit freundlichen Grüßen

RA Lukas Drostens Fachanwalt für IT-Recht Kanzlei Drostens & Pekonkur, Mainz

\*Anlage: Vollmacht der Frischetrans Mittelrhein GmbH\*

Datei: 11\_dsfa\_bem\_gesundheitsdaten.md

# **Datenschutz-Folgenabschätzung (DSFA) — BEM-Gesundheitsdaten**

**Aktenstück:** 11

**Datum:** 14.05.2026



**Erstellt durch:** RA Lukas Drostén (Kanzlei Drostén & Pekonkur) gemeinsam mit Markus Feilke (Datenschutzbeauftragter, Datenschutzkanzlei Rhein-Main)

**Mandantin:** Frischetrans Mittelrhein GmbH

**Rechtsgrundlage:** Art. 35 DSGVO, § 67 SGB IX (BEM-Verfahren)

## 1. Anlass der DSFA

Der Ransomware-Angriff vom 06.05.2026 hat die Frischetrans Mittelrhein GmbH veranlasst, die bestehende Datenverarbeitungstätigkeit für das Betriebliche Eingliederungsmanagement (BEM) einer Datenschutz-Folgenabschätzung zu unterziehen. Diese DSFA wurde durch folgenden Umstand zwingend ausgelöst:

**1. Erhöhtes Risiko durch Datenpanne:** Die exfiltrierten Daten umfassen Gesundheitsdaten im Sinne des Art. 9 Abs. 1 DSGVO (besondere Kategorie personenbezogener Daten) von 38 Beschäftigten aus BEM-Verfahren. Diese Kategorie von Daten verlangt nach Art. 35 Abs. 3 lit. b) DSGVO grundsätzlich eine vorherige DSFA.

**2. Rückfrage der LfDI RLP:** Die Datenschutzbehörde hat in ihrem Schreiben vom 09.05.2026 (Ref. LfDI-RLP-2026-0508-4419) um Vorlage einer DSFA für diese Verarbeitungstätigkeit gebeten.

## 2. Beschreibung der Verarbeitungstätigkeit

### 2.1 Zweck der Verarbeitung

Frischetrans führt gemäß § 167 SGB IX (früher § 84 SGB IX a.F.) das BEM-Verfahren für Beschäftigte durch, die innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig waren. Zweck ist die Wiedereingliederung und Prävention weiterer Ausfallzeiten.

### 2.2 Art der verarbeiteten Daten

| Datenkategorie                             | Einstufung                         | Anzahl Betroffene |
|--------------------------------------------|------------------------------------|-------------------|
| Diagnosen (Erkrankungen)                   | Art. 9 DSGVO (besondere Kategorie) | 38                |
| Therapieverläufe, Behandlungsberichte      | Art. 9 DSGVO                       | 38                |
| Ärztliche Atteste und Gutachten            | Art. 9 DSGVO                       | 38                |
| Betriebsärztliche Bewertungen              | Art. 9 DSGVO                       | 38                |
| Rehabilitationsmaßnahmen                   | Art. 9 DSGVO                       | 22                |
| Krankenhausaufenthalte                     | Art. 9 DSGVO                       | 15                |
| Rentenversicherungskorrespondenz           | Sozialdaten                        | 8                 |
| Personenstammdaten (Name, Adresse, SV-Nr.) | Art. 6 DSGVO                       | 38                |

## 2.3 Rechtsgrundlage der Verarbeitung

- Art. 9 Abs. 2 lit. b) DSGVO (Verarbeitung im Rahmen arbeitsrechtlicher Pflichten)
- § 26 Abs. 3 BDSG (Verarbeitung besonderer Kategorien im Beschäftigtenverhältnis)
- § 167 Abs. 2 SGB IX (gesetzliche Grundlage BEM-Verfahren)

## 2.4 Speicherung und Zugriff

BEM-Daten wurden in SAP HR (Modul: Personalwesen — Krankheit/BEM) sowie als digitale Scans in einem Dokumentenmanagementsystem (DMS) gespeichert. Zugriff hatten vor der Panne:

- HR-Abteilung (3 Personen)
- Betriebsärztlicher Dienst (extern, via VPN)
- Betriebsrat (eingeschränkt, nur im BEM-Sitzungsrahmen)
- IT-Administrator (technischer Zugriff, nicht inhaltlich)

# 3. Risikoanalyse

## 3.1 Identifizierte Risiken vor dem Vorfall

| Risiko                                 | Eintrittswahrscheinlichkeit (vor Vorfall) | Schwere   |
|----------------------------------------|-------------------------------------------|-----------|
| Unbefugter Zugang durch Datenpanne     | Mittel                                    | Sehr hoch |
| Unsachgemäße Nutzung durch Mitarbeiter | Niedrig                                   | Hoch      |
| Weitergabe an Dritte                   | Niedrig                                   | Sehr hoch |
| Datenverlust durch technischen Fehler  | Niedrig                                   | Mittel    |

## 3.2 Risikobewertung nach Vorfall

Durch den Ransomware-Angriff und den Datenabfluss sind folgende Szenarien jetzt konkret eingetreten:

**Szenario 1 — Veröffentlichung durch Erpressergruppe:** AkiraNext droht mit Veröffentlichung der Daten auf ihrer Leakseite. Sollte dies geschehen, sind die Gesundheitsdaten von 38 Mitarbeitern öffentlich zugänglich. Folgen:

- Soziale Stigmatisierung (psychische Erkrankungen, Suchterkrankungen)
- Auswirkungen auf Kreditwürdigkeit, Versicherbarkeit
- Diskriminierung bei künftigen Bewerbungen
- Psychische Belastung durch Kontrollverlust über intimste Daten

**Risikoklassifikation:** HOCH — unmittelbare, schwerwiegende Folgen für vulnerable Personen.

**Szenario 2 — Missbrauch durch Dritte:** Die Daten könnten an spezialisierte Datenhändler oder Identitätsdiebe verkauft werden.

**Szenario 3 — Erpressung der betroffenen Mitarbeiter:** Einzelne Mitarbeiter könnten selbst erpresst werden (z.B. „Wir veröffentlichen Ihre Diagnose, wenn Sie nicht zahlen“). Dies stellt eine zusätzliche Belastung für besonders vulnerable Personen dar.

## 4. Bereits bestehende technisch-organisatorische Maßnahmen (TOMs) — Bewertung

| Maßnahme                          | Status vor Vorfall                | Bewertung             |
|-----------------------------------|-----------------------------------|-----------------------|
| Zugriffskontrolle (Rollenkonzept) | Implementiert                     | Ausreichend           |
| Verschlüsselung der Daten at rest | Nicht vollständig                 | Unzureichend          |
| Netzwerksegmentierung             | Unzureichend                      | Unzureichend          |
| Patch-Management                  | Defizitär (CVE-2026-0712)         | Unzureichend          |
| MFA für HR-Zugang                 | Nicht implementiert               | Unzureichend          |
| Backup und Wiederherstellbarkeit  | Vorhanden (3-Tage-Rückstand)      | Teilweise ausreichend |
| Protokollierung / SIEM            | Über InsoTec (extern)             | Teilweise ausreichend |
| Sensibilisierungsschulungen       | Jährlich                          | Ausreichend           |
| Auftragsverarbeitungsertrag (AVV) | Vorhanden (InsoTec, ProcessSpark) | Vorhanden             |

**Gesamtbewertung TOMs:** Die TOMs waren vor dem Vorfall für eine Datenverarbeitung der Kategorie „Art. 9 DSGVO — Gesundheitsdaten im Beschäftigtenkontext“ **nicht ausreichend**. Insbesondere die fehlende Verschlüsselung at rest und das unzureichende Patch-Management stellen erhebliche Mängel dar.

## 5. Geplante Abhilfemaßnahmen

| Maßnahme                                                       | Verantwortlich        | Frist      |
|----------------------------------------------------------------|-----------------------|------------|
| Einführung Ende-zu-Ende-Verschlüsselung für HR-Daten (at rest) | IT / InsoTec          | 30.06.2026 |
| MFA für alle HR-Systemzugänge                                  | IT / InsoTec          | 15.06.2026 |
| Zero-Trust-Netzwerkarchitektur für HR-Segment                  | IT / InsoTec          | 31.08.2026 |
| Neues Patch-Management-Konzept (SLA-gesichert)                 | ProcessSpark / intern | 30.06.2026 |

| Maßnahme                                         | Verantwortlich | Frist      |
|--------------------------------------------------|----------------|------------|
| DSGVO-Schulung<br>HR-Mitarbeiter                 | DSB Feilke     | 30.06.2026 |
| Überarbeitung AVV<br>ProcessSpark und<br>InsoTec | RA Drosten     | 31.05.2026 |
| Einführung Data Loss<br>Prevention (DLP)         | IT             | 31.07.2026 |
| Datenschutzaudit<br>BEM-Prozesse                 | DSB Feilke     | 31.07.2026 |
| Konsultation<br>Betriebsrat zu TOMs              | GF Wallbruck   | 20.05.2026 |

## 6. Konsultation der Aufsichtsbehörde (Art. 36 DSGVO)

Aufgrund des hohen Restrisikos (Gesundheitsdaten, Exfiltration bereits erfolgt, Veröffentlichungsdrohung) wird eine vorherige Konsultation des LfDI RLP gemäß Art. 36 DSGVO durchgeführt. Die DSFA wird dem LfDI als Ergänzung zur Meldung vom 08.05.2026 übermittelt.

## 7. Ergebnis der DSFA

Die Datenschutz-Folgenabschätzung ergibt, dass die Verarbeitung von BEM-Gesundheitsdaten ohne die beschriebenen Abhilfemaßnahmen ein **hohes Restrisiko** für die Rechte und Freiheiten der betroffenen Mitarbeiter darstellt. Die geplanten Abhilfemaßnahmen sollen das Risiko auf ein akzeptables Niveau senken.

Die DSFA wird nach Abschluss der Abhilfemaßnahmen (voraussichtlich Herbst 2026) einer **Überprüfung** unterzogen.

### Verantwortliche Unterzeichner:

Theresia Wallbruck (Geschäftsführerin, Verantwortlicher i.S.d. DSGVO) Markus Feilke  
(Datenschutzbeauftragter) RA Lukas Drosten (rechtliche Beratung)

\*Mainz, 14.05.2026\*

Datei: 12\_meldung\_betroffene\_art\_34\_dsgvo.md

## Benachrichtigung betroffener Personen gemäß Art. 34 DSGVO

**Aktenstück:** 12

**Datum:** 11.05.2026

**Mandantin:** Frischetrans Mittelrhein GmbH

**Bearbeiter:** RA Lukas Drosten / Markus Feilke (DSB)

# 1. Rechtliche Grundlage und Prüfung der Benachrichtigungspflicht

## 1.1 Voraussetzungen des Art. 34 DSGVO

Art. 34 Abs. 1 DSGVO verpflichtet den Verantwortlichen, die betroffene Person unverzüglich von einer Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein **hohes Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

## 1.2 Risikoprüfung

**Gruppe 1: Mitarbeiter (BEM-Gesundheitsdaten, 38 Personen)** Risikobewertung: **HOCH** Begründung: Gesundheitsdaten aus BEM-Verfahren (Diagnosen, Therapieverläufe, ärztliche Gutachten) sind besonders sensibel. Im Falle der angekündigten Veröffentlichung durch AkiraNext drohen erhebliche Nachteile (Stigmatisierung, Diskriminierung, psychische Belastung). Die Benachrichtigungspflicht ist eindeutig gegeben.

**Gruppe 2: Mitarbeiter (Personalstammdaten, 280 Personen)** Risikobewertung: **HOCH** Begründung: Bankverbindungsdaten, Sozialversicherungsnummern und Lohndaten ermöglichen Identitätsdiebstahl und Finanzbetrug. Benachrichtigungspflicht gegeben.

**Gruppe 3: Firmenkunden (B2B, 18 Unternehmen)** Risikobewertung: **MITTEL (für juristische Personen)** Begründung: Juristische Personen sind keine „betroffenen Personen“ i.S.d. DSGVO. Soweit jedoch Kontaktpersonendaten (Ansprechpartner) betroffen sind, kann eine Benachrichtigung geboten sein. Aus Vorsichtsgründen werden die Kunden separat informiert (Aktenstück 16).

**Ergebnis:** Benachrichtigung aller 280 Mitarbeiter nach Art. 34 DSGVO geboten. Priorität: die 38 BEM-Betroffenen erhalten gesonderte, individuellere Benachrichtigung.

## 1.3 Ausnahmen des Art. 34 Abs. 3 DSGVO

Die Ausnahmen (insb. getroffene Schutzmaßnahmen, die Risiken unwahrscheinlich machen; Unverhältnismäßigkeit einer Einzelbenachrichtigung) greifen vorliegend nicht:

- Verschlüsselung der exfiltrierten Daten: **nicht vorhanden** (Daten wurden im Klartext exfiltriert)
- Benachrichtigung unverhältnismäßig: **nein** (280 Personen, Einzelanschreiben möglich)

## 2. Benachrichtigungsschreiben — Allgemeines Mitarbeiteranschreiben

**Version A — Für alle 280 Mitarbeiter (ohne BEM-Bezug)**

\*[Mustertext — individuell angepasst pro Person]\*

Frischetrans Mittelrhein GmbH Binger Straße 142 55131 Mainz

Mainz, den 11.05.2026

Persönlich / Vertraulich

**[Name, Adresse des Mitarbeiters]**

**Betreff: Wichtige Information zu einem Datenschutzvorfall — Ihre Daten sind betroffen**

Sehr geehrte/r [Anrede] [Name],

wir wenden uns in dieser Angelegenheit direkt an Sie, weil wir als Ihr Arbeitgeber gegenüber Ihnen gesetzlich verpflichtet sind, Sie über einen Datenschutzvorfall zu informieren, der auch Ihre

personenbezogenen Daten betrifft.

### **Was ist passiert?**

In der Nacht vom 05. auf den 06.05.2026 wurde Frischetrans Opfer eines Ransomware-Angriffs durch eine kriminelle Hackergruppe. Neben der Verschlüsselung unserer IT-Systeme haben die Täter leider auch ca. 2,1 TB an Daten aus unserem Netzwerk entwendet. Zu diesen Daten gehören auch Mitarbeiterpersonalakten, darunter Ihre Daten.

### **Welche Daten sind betroffen?**

Von Ihren Daten sind voraussichtlich folgende Informationen betroffen:

- Name und Adresse
- Geburtsdatum
- Bankverbindung (IBAN)
- Sozialversicherungsnummer
- Lohn-/Gehaltsdaten
- Personalnummer

### **Welche Risiken bestehen für Sie?**

Die kriminellen Täter drohen damit, die gestohlenen Daten im Internet zu veröffentlichen. Sollte dies geschehen, können die o.g. Daten von Dritten zu betrügerischen Zwecken missbraucht werden. Wir empfehlen Ihnen vorsorglich:

1. Beobachten Sie Ihre Bankkonten sorgfältig auf unbekannte Transaktionen.
2. Melden Sie verdächtige Abbuchungen sofort Ihrer Bank.
3. Beantragen Sie ggf. eine SCHUFA-Auskunft (kostenfrei einmal jährlich).
4. Seien Sie besonders wachsam gegenüber Phishing-E-Mails, die vorgeben, von uns oder von Behörden zu sein.

### **Was haben wir unternommen?**

Wir haben umgehend folgende Maßnahmen eingeleitet:

- Sofortabschaltung aller betroffenen IT-Systeme
- Beauftragung spezialisierter Cybersicherheitsexperten (Forensik)
- Strafanzeige bei der Kriminalpolizei Mainz
- Meldung an den Landesbeauftragten für den Datenschutz Rheinland-Pfalz
- Meldung an das Bundesamt für Sicherheit in der Informationstechnik (BSI)

### **An wen können Sie sich wenden?**

Bei Fragen und Sorgen stehen wir Ihnen zur Verfügung:

Externer Datenschutzbeauftragter der Frischetrans Mittelrhein GmbH: Markus Feilke, Datenschutzkanzlei Rhein-Main E-Mail: [bem-datenpanne@datenschutz-rhein-main.de](mailto:bem-datenpanne@datenschutz-rhein-main.de) Telefon: +49 6131 9944-11 (täglich 9–17 Uhr, kostenlos)

Sollten Sie sich durch den Datenschutzvorfall in Ihren Rechten verletzt sehen, haben Sie das Recht, sich beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI RLP, [www.datenschutz.rlp.de](http://www.datenschutz.rlp.de)) zu beschweren.

Wir bedauern diesen Vorfall außerordentlich und entschuldigen uns für die Belastungen, die Ihnen dadurch entstanden sind. Wir tun alles, um die Auswirkungen für Sie so gering wie möglich zu halten.

Mit freundlichen Grüßen

Theresia Wallbruck Geschäftsführerin Frischetrans Mittelrhein GmbH

### 3. Benachrichtigungsschreiben — BEM-Betroffene (Version B)

#### Version B — Für die 38 Mitarbeiter mit BEM-Gesundheitsdaten

\*[Zusätzlicher Absatz zu Version A:]\*

#### Besonderer Hinweis zu Ihren Gesundheitsdaten:

Leider müssen wir Sie darüber informieren, dass von dem Datenverlust auch Informationen aus Ihrem Betrieblichen Eingliederungsmanagement (BEM) betroffen sein können. Dies betrifft ärztliche Informationen, die im Rahmen des BEM-Verfahrens bei uns gespeichert wurden.

Wir verstehen, dass dies besonders belastend für Sie ist. Bitte wissen Sie, dass die strengsten Vertraulichkeitsgebote für BEM-Daten auch bei der Strafverfolgung und den Behörden gelten. Wir haben den behördlichen Empfängern (LfDI, BSI) ausdrücklich mitgeteilt, dass BEM-Gesundheitsdaten besonders schutzwürdig sind.

Unser Datenschutzbeauftragter steht Ihnen für ein vertrauliches Gespräch zur Verfügung (Termine auf Anfrage, auch außerhalb der Geschäftszeiten).

### 4. Versandprotokoll

| Gruppe                                         | Anzahl | Versanddatum | Kanal                                                       |
|------------------------------------------------|--------|--------------|-------------------------------------------------------------|
| Allgemeines Mitarbeiteranschreiben (Version A) | 242    | 11.05.2026   | Persönliche Übergabe (Betriebsversammlung) und Einschreiben |
| BEM-Betroffene (Version B)                     | 38     | 11.05.2026   | Persönliche Übergabe, vertraulich versiegelt                |
| Gesamtversand                                  | 280    | 11.05.2026   | —                                                           |

Alle Versandnachweise werden als Anlage zur Akte genommen (Unterschriftenlisten der persönlichen Übergabe, Einschreibenbelege).

Datei: 13\_ki\_vo\_klassifizierung\_palettenauge.md

## KI-Verordnung — Klassifizierung und Konformitätsbewertung „PalettenAuge AI“

Aktenstück: 13

Datum: 12.05.2026

Mandantin: Frischetrans Mittelrhein GmbH

Anbieter des KI-Systems: DachAuge GmbH, Rosenthaler Str. 34, 10178 Berlin

## 1. Hintergrund

Die Frischetrans Mittelrhein GmbH setzt das KI-System „**PalettenAuge AI**“ der DachAuge GmbH (Berlin) ein. Das System dient der **vorausschauenden Routenoptimierung und Personaleinsatzplanung** für den Fuhrpark von 64 LKW.

Konkreter Einsatz:

- Automatische Tourenplanung basierend auf KI-Prognosen (Auftragslage, Verkehr, Wetter, Fahrerleistungsdaten)
- Personaleinsatzplanung: Das System schlägt vor, welcher Fahrer welche Tour übernimmt, unter Berücksichtigung von Fahrzeugtyp-Qualifikation, Lenk-/Ruhezeiten (EU-VO 561/2006), vergangenen Leistungsdaten und Gesundheitszustand (Krankheitstage aus SAP HR)
- Auslastungsoptimierung und präventive Wartungsvorschläge

**Frage:** Fällt „PalettenAuge AI“ unter Anhang III der EU-KI-Verordnung (Verordnung (EU) 2024/1689) als Hochrisiko-KI-System?

## 2. Rechtlicher Rahmen — EU-KI-Verordnung

Die Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates über künstliche Intelligenz (KI-VO) ist am 01.08.2024 in Kraft getreten. Für Hochrisiko-KI-Systeme gelten die Pflichten ab dem 02.08.2026 (Art. 113 Abs. 2 KI-VO — zwei Jahre nach Inkrafttreten).

**Relevante Geltungszeitpunkte:**

- Allgemeines Inkrafttreten: 01.08.2024
- Geltung Hochrisiko-Pflichten: 02.08.2026 ← **6 Monate bis zur Geltung, Frischetrans muss jetzt handeln**

## 3. Klassifizierungsprüfung nach Anhang III KI-VO

### 3.1 Screening aller Anhang-III-Kategorien

**Nr. 1 — Biometrische Identifizierung:** Nicht anwendbar.

**Nr. 2 — Kritische Infrastruktur:** Routenoptimierung für LKW-Logistik könnte als Komponente einer kritischen Versorgungsinfrastruktur gelten. Frischetrans ist als Lebensmittellogistiker für systemrelevante Bäckereien tätig. Eingeschränkte Relevanz — keine eindeutige Einschlägigkeit.

**Nr. 3 — Allgemeine und berufliche Bildung:** Nicht anwendbar.

**Nr. 4 — Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit:** ■ **EINSCHLÄGIG**

Art. 6 Abs. 2 i.V.m. Anhang III Nr. 4 lit. a) und b) KI-VO erfasst KI-Systeme, die bei der **Einstellung oder Auswahl natürlicher Personen** oder für **Entscheidungen über Arbeitsbedingungen, Beförderungen und Kündigungen** eingesetzt werden.

Das PalettenAuge-AI-System schlägt die Personaleinsatzplanung vor — also, welcher Fahrer welche Tour übernimmt. Dabei fließen leistungsbezogene Daten und Gesundheitsdaten (Krankheitstage) ein. Die Entscheidungsvorschläge des Systems haben direkten Einfluss auf:

- Arbeitsbedingungen (Tourenlänge, Nacht-/Frühschichten)



- Tatsächliche Arbeitszuweisung
- Indirekt: Leistungsbeurteilung (da Tourdaten archiviert werden)

**Nr. 5 — Zugang zu Dienstleistungen:** Nicht primär anwendbar.

**Nr. 6 — Strafverfolgung:** Nicht anwendbar.

**Nr. 7 — Migration, Asyl, Grenzkontrolle:** Nicht anwendbar.

**Nr. 8 — Rechtspflege und demokratische Prozesse:** Nicht anwendbar.

### 3.2 Ergebnis der Klassifizierung

**PalettenAuge AI fällt unter Anhang III Nr. 4 KI-VO (Beschäftigung / Personalmanagement) und ist als Hochrisiko-KI-System einzustufen.**

#### Begründung im Einzelnen:

1. Das System trifft Empfehlungen zur Personaleinsatzplanung, die in der Praxis regelmäßig ohne nennenswerte menschliche Überprüfung übernommen werden (de-facto-Automatisierung).
2. Die Einbeziehung von Gesundheitsdaten (Krankheitstage) in den Algorithmus erhöht das Risiko einer faktischen Diskriminierung gesundheitlich beeinträchtigter Mitarbeiter.
3. Die Leistungshistorie (welche Touren, welche Zeiten, Tempodaten) fließt in eine Art implizites Bewertungssystem ein, das arbeitsrechtlich relevant ist.
4. Im Kontext des Datenschutzvorfalles wurden diese Daten exfiltriert — das zeigt die Sensibilität und die realen Risiken bei Missbrauch.

## 4. Pflichten des Betreibers (Frischetrans als Deployer)

Als **Deployer** (Betreiber) eines Hochrisiko-KI-Systems hat Frischetrans nach Art. 26 KI-VO folgende Pflichten:

| Pflicht                                                     | Rechtsgrundlage                          | Fälligkeit          | Status              |
|-------------------------------------------------------------|------------------------------------------|---------------------|---------------------|
| Implementierung technischer und organisatorischer Maßnahmen | Art. 26 Abs. 1 KI-VO                     | 02.08.2026          | Offen               |
| Menschliche Aufsicht (Human Oversight)                      | Art. 26 Abs. 2 KI-VO                     | 02.08.2026          | Offen               |
| Betriebstagebuch / Protokollierung                          | Art. 26 Abs. 5 KI-VO                     | 02.08.2026          | Teilweise (IT-Logs) |
| Information der Arbeitnehmer                                | Art. 26 Abs. 7 KI-VO                     | 02.08.2026          | Offen               |
| Konsultation des Betriebsrats                               | BetrVG § 87 Abs. 1 Nr. 6 (Mitbestimmung) | Vor Einsatz / jetzt | Offen               |
| Sicherstellung Konformitätserklärung des Anbieters          | Art. 26 Abs. 1 i.V.m. Art. 47 KI-VO      | 02.08.2026          | Offen               |
| Registrierung in EU-Datenbank                               | Art. 26 Abs. 1 i.V.m. Art. 71 KI-VO      | 02.08.2026          | Offen               |

#### 4.1 Pflichten des Anbieters (DachAuge GmbH als Provider)

Der Anbieter DachAuge GmbH hat als **Provider** nach Art. 16 ff. KI-VO folgende Pflichten:

- Konformitätsbewertung (Art. 43 KI-VO)
- Technische Dokumentation (Anhang IV KI-VO)
- Konformitätserklärung (Art. 47 KI-VO)
- CE-Kennzeichnung (Art. 48 KI-VO)
- Registrierung in der EU-KI-Datenbank (Art. 71 KI-VO)

**Frischetrans muss bei DachAuge die Vorlage dieser Dokumente einfordern.**

### 5. Arbeitsrechtliche Dimension (§ 87 BetrVG)

Das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG (technische Überwachungseinrichtungen) ist eindeutig berührt:

PalettenAuge AI überwacht indirekt das Verhalten und die Leistung der Fahrer (Tourdaten, Tempoverläufe, Standortdaten) und wertet diese für die Dispositionsempfehlung aus. Eine **Betriebsvereinbarung über den Einsatz von PalettenAuge AI** ist erforderlich.

**Empfehlung:** Abschluss einer Betriebsvereinbarung nach § 87 Abs. 1 Nr. 6 BetrVG, die Folgendes regelt:

- Zweck der Datenverarbeitung durch PalettenAuge AI
- Welche Daten fließen ein
- Wie wird sichergestellt, dass die KI-Empfehlungen nur als Entscheidungsunterstützung (nicht als automatische Entscheidung) genutzt werden
- Recht der Mitarbeiter auf Auskunft über sie betreffende Auswertungen
- Aufbewahrungsfristen der Leistungsdaten

### 6. Empfehlungen und Handlungsplan

| Maßnahme                                                        | Zuständig                  | Frist      |
|-----------------------------------------------------------------|----------------------------|------------|
| Anforderung Konformitätsdokumentation bei DachAuge GmbH         | RA Drostén / IT            | 20.05.2026 |
| Abschluss Betriebsvereinbarung PalettenAuge AI                  | GF Wallbruck / Betriebsrat | 30.06.2026 |
| Implementierung Human-Oversight-Prozess                         | IT / Disposition           | 31.07.2026 |
| DSGVO-Datenschutzfolgenabschätzung PalettenAuge (Art. 35 DSGVO) | DSB Feilke                 | 30.06.2026 |
| Schulung Disponenten zu KI-Aufsichtspflichten                   | HR                         | 31.07.2026 |

| Maßnahme                                           | Zuständig           | Frist      |
|----------------------------------------------------|---------------------|------------|
| Registrierung in EU-KI-Datenbank (über DachAuge)   | DachAuge / RA Drost | 01.08.2026 |
| Prüfung: Weiter-Einsatz bis Konformität gesichert? | GF + RA Drost       | 20.05.2026 |

**Kritische Empfehlung:** Bis zur Sicherstellung der vollständigen KI-VO-Konformität sollte der automatisierte Personaleinsatz-Modus von PalettenAuge AI ausgesetzt und nur die Routenoptimierungsfunktion (ohne Personaldaten) genutzt werden.

## 7. Bußgeldrisiko

Bei Verstößen gegen die KI-VO drohen Bußgelder nach Art. 99 KI-VO:

- Verwendung eines verbotenen KI-Systems (nicht einschlägig): bis 35 Mio. EUR / 7 % des weltweiten Umsatzes
- Verwendung ohne Konformitätsbewertung (Hochrisiko): bis 15 Mio. EUR / 3 % des weltweiten Umsatzes
- Falsche Angaben gegenüber Behörden: bis 7,5 Mio. EUR / 1 %

Für Frischetrans als KMU sind reduzierte Bußgelder vorgesehen (Art. 99 Abs. 5 KI-VO). Das Risiko besteht aber auch für DachAuge als Provider.

Datei: 14\_open\_source\_audit\_scheduleherokit.md

## Open-Source-Compliance-Audit — „TourPlanner“ / scheduleHero (AGPL-3.0)

**Aktenstück:** 14

**Datum:** 12.–14.05.2026

**Mandantin:** Frischetrans Mittelrhein GmbH

**Bearbeiter:** RA Lukas Drost, Fachanwalt für IT-Recht

### 1. Hintergrund

Die Frischetrans Mittelrhein GmbH hat intern eine Softwareanwendung namens „**TourPlanner**“ entwickelt. TourPlanner dient der Verwaltung und Planung von Fahrer-Touren und integriert sich mit dem (nunmehr angegriffenen) SAP S/4HANA-System. Die Eigenentwicklung wurde vom IT-Team der Frischetrans über mehrere Jahre aufgebaut.

Während der forensischen Analyse des Ransomware-Angriffs wurde festgestellt, dass TourPlanner eine Open-Source-Komponente namens „**scheduleHero**“ verwendet. scheduleHero ist eine Scheduling-Engine für Ressourcenplanung, lizenziert unter der **GNU Affero General Public License Version 3 (AGPL-3.0)**.

## 2. Bedeutung der AGPL-3.0-Lizenz

### 2.1 Grundprinzipien der AGPL-3.0

Die GNU Affero General Public License 3.0 (AGPL-3.0) ist eine Copyleft-Lizenz mit folgenden Kernpflichten:

1. **Copyleft-Wirkung:** Wird AGPL-3.0-lizenzierter Code in ein Software-Werk integriert, muss das gesamte Werk bei Weitergabe unter AGPL-3.0 (oder einer kompatiblen GPL-Lizenz) veröffentlicht werden.
2. **Netzwerk-Copyleft (§ 13 AGPL-3.0):** Die AGPL-3.0 erweitert den Copyleft-Effekt auf den **Netzwerkbetrieb**: Wenn ein Dritter über ein Computernetzwerk mit der Software interagiert, muss der Quellcode der Anwendung denjenigen Nutzern zur Verfügung gestellt werden. Dies ist der entscheidende Unterschied zur GPL-3.0.
3. **Quelltextpflicht:** Bei Weitergabe muss der vollständige korrespondierende Quellcode mitgeliefert oder über einen Netzwerkzugang zugänglich gemacht werden.
4. **Keine proprietären Zusätze:** Eine proprietäre Überlizenzierung (Relizenzierung zu einer nicht-copyleft-Lizenz) ist ohne Zustimmung aller Rechteinhaber nicht zulässig.

### 2.2 Kritischer Punkt: Netzwerk-Nutzung durch Dritte

TourPlanner wird als Webapplikation betrieben und ist über das interne Netzwerk für folgende Nutzergruppen zugänglich:

- Dispositionsabteilung (intern, ca. 8 Benutzer)
- Fahrer (über Mobilgeräte / Telematik-App — **externe Netzwerkinteraktion**)
- ggf. Kunden (keine aktuellen Belege gefunden)

Sobald **externe Nutzer** (Fahrer über Smartphone-App oder Kunden) über das Netzwerk mit dem TourPlanner interagieren, gilt die Netzwerk-Copyleft-Pflicht des § 13 AGPL-3.0. In diesem Fall wäre Frischetrans verpflichtet, den gesamten Quellcode des TourPlanner (einschließlich aller mit scheduleHero integrierten Teile) zur Verfügung zu stellen.

## 3. Befunde des Audits

### 3.1 Verwendung von scheduleHero

| Parameter                     | Befund                                                                                       |
|-------------------------------|----------------------------------------------------------------------------------------------|
| Komponente                    | scheduleHero v2.4.1                                                                          |
| Lizenz                        | AGPL-3.0                                                                                     |
| Einbindung                    | Direkte Einbindung als Java-Bibliothek (JAR) in TourPlanner-Backend                          |
| Integrationstiefe             | Tiefe Integration — scheduleHero-Klassen werden extensiv genutzt (>150 Aufrufe im Quellcode) |
| Abgetrennte Module            | Nein — keine Trennung durch API/Middleware-Schicht                                           |
| Weitergabe des TourPlanners   | Nein (reine Eigennutzung bisher)                                                             |
| Netzwerknutzung durch Externe | Ja — Fahrer-App interagiert über REST-API mit TourPlanner                                    |

### 3.2 Compliance-Status

| Pflicht (AGPL-3.0)                                    | Erfüllt? | Begründung                                      |
|-------------------------------------------------------|----------|-------------------------------------------------|
| Urheberrechtshinweis<br>scheduleHero<br>beibehalten   | Nein     | Keine NOTICE-Datei in<br>TourPlanner-Deployment |
| Lizenztext AGPL-3.0<br>beigelegt                      | Nein     | Nicht in Deployment-Paket                       |
| Netzwerk-Nutzern<br>Quellcode angeboten               | Nein     | Fahrer-App bietet keinen<br>Quellcode-Zugang    |
| Vollständiger<br>Quellcode TourPlanner<br>offengelegt | Nein     | TourPlanner ist proprietär behandelt            |

**Ergebnis:** Frischetrans befindet sich in mehrfacher Verletzung der AGPL-3.0-Lizenzpflichten.

## 4. Rechtliche Risiken

### 4.1 Urheberrechtsverletzung

Die Nicht-Einhaltung der AGPL-3.0-Bedingungen führt zum Erlöschen der Nutzungslizenz (sog. automatischer Lizenzterminus gemäß AGPL-3.0 § 8). Ohne gültige Lizenz stellt die Nutzung von scheduleHero eine **Urheberrechtsverletzung** dar:

- § 97 UrhG: Unterlassungsanspruch der Rechteinhaber von scheduleHero
- § 97a UrhG: Abmahnanspruch (anwaltliche Abmahnung mit Kostentragungspflicht)
- § 97 Abs. 2 UrhG: Schadensersatzanspruch (Lizenzanalogie oder tatsächlicher Schaden)

Die Rechteinhaberin von scheduleHero (nach Repository-Auswertung: ScheduleHero Foundation, registriert in den Niederlanden) hat Erfahrung mit der Durchsetzung von AGPL-Rechten. Entsprechende Durchsetzungsmuster sind aus vergleichbaren Fällen bekannt (vgl. GPL Enforcement News — [gpl-violations.org](http://gpl-violations.org)).

### 4.2 Schadensersatz nach Lizenzanalogie

Im Falle einer Klage würde der Schadensersatz nach der Lizenzanalogiemethode berechnet: Was hätte der Rechteinhaber für eine kommerzielle Lizenz verlangt? Für vergleichbare Scheduling-Bibliotheken mit kommerziellem Einsatz sind Lizenzgebühren von 5.000–50.000 EUR p.a. marktüblich.

### 4.3 Reputationsrisiko

Eine erfolgreiche Abmahnung oder Klage durch die ScheduleHero Foundation würde zu öffentlicher Aufmerksamkeit führen und das ohnehin durch den Ransomware-Vorfall belastete Image von Frischetrans weiter schädigen.

## 5. Sofortmaßnahmen und Sanierungsoptionen

### Option A: Quellcode offenlegen (AGPL-Compliance)

TourPlanner wird vollständig unter AGPL-3.0 veröffentlicht, Quellcode auf einem öffentlichen Repository (z.B. GitHub) bereitgestellt, Nutzern der Fahrer-App ein Hinweis auf den Quellcode-Zugang gegeben.

**Vorteil:** Vollständige Compliance, keine Kosten für kommerzielle Lizenz.

**Nachteil:** Offenlegung des TourPlanner-Quellcodes; kompetitiver Nachteil, wenn Konkurrenten die Anwendung analysieren.

### **Option B: Kommerzielle Lizenz (Dual-Licensing)**

Frischetrans erwirbt von der ScheduleHero Foundation eine kommerzielle Lizenz für scheduleHero, die die Nutzung in proprietären Anwendungen gestattet.

**Empfehlung:** RA Drosten nimmt Kontakt mit der ScheduleHero Foundation auf.

### **Option C: Austausch der Komponente**

scheduleHero wird durch eine funktional gleichwertige Scheduling-Bibliothek mit permissiver Lizenz (MIT, Apache 2.0) ersetzt.

**Vorteil:** Langfristige Unabhängigkeit.

**Nachteil:** Entwicklungsaufwand (geschätzt 3–6 Monate, ca. 40.000–80.000 EUR Entwicklungskosten).

## **6. Empfehlung**

RA Drosten empfiehlt folgendes Vorgehen:

1. **Sofortmaßnahme (binnen 7 Tagen):** Aussetzen der externen Netzwerkerreichbarkeit des TourPlanners für Fahrer-App (Trennung REST-API von extern) — damit entfällt die Netzwerk-Copyleft-Pflicht vorerst.
2. **Kurzfristig (30 Tage):** Aufnahme von Lizenzverhandlungen mit der ScheduleHero Foundation (Option B oder freiwillige Offenlegung).
3. **Mittelfristig (3–6 Monate):** Prüfung und ggf. Austausch der AGPL-Komponente (Option C), um eine dauerhaft risikofreie Nutzung zu gewährleisten.
4. **Sofort:** Durchführung eines vollständigen Open-Source-License-Audits des gesamten TourPlanner und aller weiteren Frischetrans-Eigenentwicklungen. Bekannte Audit-Tools: FOSSA, Black Duck, TLDR Legal.

## **7. Muster-Compliance-Hinweis für NOTICE-Datei (falls Option A gewählt)**

``` This software includes scheduleHero v2.4.1 Copyright (C) 2022 ScheduleHero Foundation, Amsterdam (NL) Licensed under the GNU Affero General Public License v3.0  
<https://www.gnu.org/licenses/agpl-3.0.html>

The complete source code of this application (TourPlanner), including the scheduleHero integration, is available at: [URL — TBD] ```

Datei: 15_versicherungsmeldung_cybercovered.md

Versicherungsmeldung an CyberCovered AG

Aktenstück: 15

Datum der Meldung: 07.05.2026

Schadensnummer: CC-SCHADEN-2026-FTM-0914

Mandantin: Frischetrans Mittelrhein GmbH

Versicherer: CyberCovered AG, Taunusanlage 17, 60325 Frankfurt am Main

1. Versicherungsvertrag — Eckdaten

| Parameter | Wert |
|---------------------------------------|---|
| Versicherungsnehmerin | Frischetrans Mittelrhein GmbH |
| Policennummer | CC-2024-FTM-8801 |
| Versicherungsart | Cyber-Versicherung (All-Risk) |
| Deckungssumme | 5.000.000 EUR |
| Jahresprämie | 42.800 EUR (netto) |
| Versicherungsbeginn | 01.01.2024 |
| Versicherungsende | 31.12.2026 (Laufzeit 3 Jahre) |
| Makler | Finanz- und Versicherungsbüro Riedel, Mainz |
| Schadenmeldepflicht (Vertragsklausel) | Unverzüglich, max. 72 h nach Kenntnisnahme |

2. Deckungsumfang der Police (Zusammenfassung)

Die Cyber-Versicherungspolice CC-2024-FTM-8801 der CyberCovered AG deckt (gemäß § 3 der Allgemeinen Versicherungsbedingungen Cyber, AVB-Cyber 2023):

Erstparteileistungen:

- Betriebsunterbrechungsschäden (Ertragsausfall durch Systemausfall, bis 72 Stunden Karenzzeit)
- IT-Wiederherstellungskosten (Forensik, Datenwiederherstellung, Systemwiederaufbau)
- Krisenmanagement und PR-Kosten
- Kosten für Benachrichtigung betroffener Personen (Art. 34 DSGVO)
- Erpressungskosten (Lösegeldzahlungen — mit Zustimmungsvorbehalt des Versicherers)
- Anwaltskosten im Zusammenhang mit dem Vorfall

Drittparteileistungen:

- Haftpflichtschäden aus Datenschutzverletzungen (DSGVO-Bußgelder bis zur gesetzlichen Grenze)
- Schadensersatzansprüche Dritter aus Datenpannen
- Abwehr von Schadensersatzansprüchen durch Versicherungsdeckung der Anwaltskosten

Ausschlüsse (wesentliche):

- Schäden durch Kriegsakte und staatlich gesteuerte Cyberangriffe (War Exclusion)
- Vorsätzlich herbeigeführte Schäden
- Schäden, die bei bekannten ungepatchten Schwachstellen entstehen, die der VN trotz Kenntnis nicht behoben hat (fragliche Anwendung im vorliegenden Fall — zu prüfen!)

3. Schadensmeldung vom 07.05.2026

Übermittelt an: CyberCovered AG, Schadenabteilung Cyber

Kanal: Verschlüsselte E-Mail an schaden-cyber@cybercovered.de + telefonische Erstmeldung

Ansprechpartner Versicherer: Lena Hamann (Schadenmanagerin Cyber, CyberCovered AG)

Inhalt der Schadensmeldung

Schadenereignis: Ransomware-Angriff (AkiraNext) am 06.05.2026, Entdeckung 04:17 Uhr. Vollständige Verschlüsselung des SAP ERP-Systems und weiterer IT-Infrastruktur sowie Datenabfluss (2,1 TB).

Vorläufige Schadenspositionen (zum Zeitpunkt der Meldung):

| Position | Betrag (vorläufig) |
|-------------------------------------|------------------------------------|
| IT-Forensik und Wiederherstellung | ca. 200.000–270.000 EUR |
| Betriebsunterbrechungsschaden | ca. 350.000–500.000 EUR |
| Kosten Datenschutzmeldungen / DSGVO | ca. 20.000–40.000 EUR |
| Anwaltskosten | ca. 80.000–120.000 EUR |
| PR / Krisenmanagement | ca. 15.000–30.000 EUR |
| **Gesamt (vorläufig)** | **ca. 665.000–960.000 EUR** |

Lösegeld wurde **nicht** gezahlt und ist auch nicht geplant.

Angabe zum Angriffsverlauf: Initial Access über CVE-2026-0712 (SAP-Schwachstelle). Patch war durch IT-Dienstleister ProcessSpark Cloud AG verspätet eingespielt worden (55 Tage Verzug). Frischetrans selbst hatte keine unmittelbare Kenntnis von der Patchlücke.

4. Rechtliche Bewertung — Ausschlussklausel ungepatchte Schwachstellen

Kritischer Punkt: Viele Cyber-Policen enthalten Klauseln, die Schäden ausschließen, die aus bekannten, nicht gepatchten Schwachstellen resultieren.

Analyse im vorliegenden Fall:

1. Die Frischetrans selbst hatte **keine direkte Kenntnis** von CVE-2026-0712 und dem Patch-Rückstand. Die Mandantin hatte die Patchpflicht an ProcessSpark Cloud AG ausgelagert.
2. Die Ausschlussklausel greift nach gefestigter Auffassung in der Versicherungsrechtsliteratur nicht, wenn der VN die Behebung der Schwachstelle vertraglich an einen Dritten ausgelagert hatte und der Dritte pflichtwidrig nicht gehandelt hat.
3. Arglistige oder grob fahrlässige Kenntnis der Mandantin ist nicht gegeben.

Empfehlung: Sollte CyberCovered AG die Leistung unter Berufung auf diese Klausel ablehnen oder kürzen, ist der Einwand zu bestreiten und ggf. gerichtlich anzugreifen. Parallel wird ProcessSpark in

Regress genommen (Aktenstück 10).

5. Weiterer Prozess mit der Versicherung

| Schritt | Datum | Status |
|--|----------------|--|
| Erstmeldung | 07.05.2026 | Erledigt |
| Benennung externer Forensiker (Vorgabe des Versicherers) | 08.05.2026 | Erledigt (CyberForensik RheinMain bestätigt) |
| Vorlage Forensikzwischenbericht | 15.05.2026 | Offen |
| Vorlage vollständiger Schadensdokumentation | 31.05.2026 | Offen |
| Schadenregulierung (Erstabschlagszahlung) | ca. 01.06.2026 | Offen |
| Abschließende Regulierung | ca. 30.06.2026 | Offen |

6. Wichtiger Hinweis zu Lösegeldzahlungen

Die Police CC-2024-FTM-8801 sieht vor, dass Lösegeldzahlungen nur mit vorheriger Zustimmung der CyberCovered AG erstattet werden. Da keine Zahlung geleistet wurde, ist dieser Punkt irrelevant. Die Entscheidung, kein Lösegeld zu zahlen, entspricht auch der Empfehlung der CyberCovered AG (Schadenmanagerin Hamann bestätigte telefonisch, dass CyberCovered bei Ransomware grundsätzlich auf Zahlung verzichtet und forensische Wiederherstellung bevorzugt).

Datei: 16_kundenkommunikation_frischbaecker_backhaussued.md

Kundenkommunikation — Frischbäcker AG und Backhaus Süd GmbH & Co. KG

Aktenstück: 16

Datum: 12.05.2026

Mandantin: Frischetrans Mittelrhein GmbH

Bearbeiter: RA Lukas Drost / Theresia Wallbruck

1. Vorbemerkung

Von dem Ransomware-Angriff und dem Datenverlust sind 18 Geschäftskunden der Frischetrans betroffen. Zwei Kunden gelten als **systemrelevant** im Sinne der Versorgungskette und haben besondere rechtliche und kommunikative Bedeutung:

- **Frischbäcker AG** (Mannheim) — Großbäckerei, Jahresumsatz ca. 380 Mio. EUR, beliefert bundesweit Supermarktfilialisten

- **Backhaus Süd GmbH & Co. KG** (Stuttgart) — Regionaler Marktführer Baden-Württemberg, ca. 4.800 Mitarbeiter

Beide Kunden haben ihre Frischelogistik zu erheblichen Teilen an Frischetrans ausgelagert. Beide hatten Lieferausfälle am 07.05.2026 erlitten. Kundenstammdaten beider Unternehmen (Vertrags-, Konditions- und Lieferdaten sowie Ansprechpartner-Kontaktdaten) sind Teil der exfiltrierten Datenmenge.

2. Kommunikationsstrategie

RA Drost empfahl folgende Strategie:

1. **Proaktive Kommunikation** (nicht abwarten, bis der Kunde nachfragt)
2. **Ehrliche Schilderung** der Situation ohne Verharmlosung
3. **Konkrete Handlungen** aufzeigen — keine leeren Versprechen
4. **Rechtliche Klarheit** über den Umfang der betroffenen Daten
5. **Serviceangebot** — Ansprechpartner für Rückfragen, Eskalationsweg

3. Anschreiben an Frischbäcker AG

Frischetrans Mittelrhein GmbH Binger Straße 142 55131 Mainz

Mainz, den 12.05.2026

Per E-Mail und Einschreiben

Frischbäcker AG — Vorstand / Rechtsabteilung — Industriestraße 12 68167 Mannheim

Betreff: Vertrauliche Information — Cyber-Sicherheitsvorfall und Datenpanne bei Frischetrans Mittelrhein GmbH — Ihre Daten betroffen

Sehr geehrte Damen und Herren,

wir wenden uns in dieser vertraulichen Angelegenheit direkt an Sie.

Was ist passiert?

In der Nacht vom 05. auf den 06.05.2026 wurde die Frischetrans Mittelrhein GmbH Opfer eines schwerwiegenden Ransomware-Angriffs durch die kriminelle Cybergruppe „AkiraNext“. Der Angriff führte zur vollständigen Verschlüsselung unserer ERP- und IT-Systeme sowie zum Datenabfluss von ca. 2,1 TB Unternehmensdaten.

Welche Daten von Ihnen sind betroffen?

Nach derzeitigem forensischen Erkenntnisstand sind vom Datenabfluss auch Informationen betroffen, die Ihr Unternehmen betreffend bei uns gespeichert waren:

- Ihre Stammdaten als Kunde (Firmenname, Anschrift, Umsatzsteuer-ID)
- Kontaktdaten Ihrer uns bekannten Ansprechpartner (Name, E-Mail, Telefon)
- Vertragliche Konditionen (Rahmenvertrag, Preise, Lieferbedingungen)
- Lieferdaten der zurückliegenden 24 Monate
- Rechnungs- und Zahlungsdaten

Wir versichern Ihnen, dass keine Bankgeheimnisse (IBAN Ihrer Gesellschaft) oder Rezepturdaten in unseren Systemen gespeichert waren. Derartige Daten sind nicht betroffen.

Welche Risiken bestehen für Sie?

Die Tätergruppe droht mit der Veröffentlichung der gestohlenen Daten. Ihre Vertragsdaten könnten im Falle einer Veröffentlichung Wettbewerbern oder der Presse zugänglich werden. Dies kann insbesondere Ihre mit uns vereinbarten Sonderkonditionen betreffen. Wir empfehlen Ihnen:

1. Informieren Sie Ihre Rechtsabteilung und ggf. Ihren eigenen Datenschutzbeauftragten.
2. Weisen Sie Ihre Mitarbeiter auf erhöhtes Phishing-Risiko hin (E-Mails, die vorgeben, von Frischetrans zu stammen).
3. Informieren Sie bei Bedarf Ihre Hausbank über die mögliche Datenpanne.

Was haben wir unternommen?

- Sofortige Abschaltung aller betroffenen Systeme
- Beauftragung spezialisierter Cyber-Forensiker
- Strafanzeige bei der Kriminalpolizei Mainz (ZAC)
- Meldungen an LfDI Rheinland-Pfalz und BSI
- Keine Lösegeldzahlung
- Vollständige IT-Wiederherstellung aus Backup (zu ca. 80 % abgeschlossen)
- Anwaltliche Begleitung durch Kanzlei Drosten & Pekonkur (Fachanwalt für IT-Recht)

Ihre Lieferungen:

Die Betriebsunterbrechung am 07.05.2026 hat Auswirkungen auf Ihre Lieferungen gehabt. Wir entschuldigen uns für diese Beeinträchtigungen aufrichtig. Seit dem 09.05.2026 wird Ihr Versorgungsvertrag wieder vollständig bedient. Wir prüfen, ob und inwieweit wir Ihnen für die Lieferunterbrechung einen Ausgleich anbieten können.

Ansprechpartner:

Für Rückfragen stehen wir Ihnen gerne zur Verfügung:

Theresia Wallbruck (Geschäftsführerin): +49 6131 8820-100 RA Lukas Drosten (Kanzlei Drosten & Pekonkur): +49 6131 2240-0

Wir bedauern diesen Vorfall außerordentlich und stehen zu unserer Verantwortung.

Mit freundlichen Grüßen

Theresia Wallbruck Geschäftsführerin Frischetrans Mittelrhein GmbH

4. Anschreiben an Backhaus Süd GmbH & Co. KG

(Inhaltlich gleichlautend mit Anpassung der Ansprechpartner und Adresse; Backhaus Süd hat gesondert Schaden gemeldet wegen Ausfall eines Samstagmorgen-Lieferfensters für Wochenendbedarf — separate Schadenserfassung läuft.)

Backhaus Süd GmbH & Co. KG — Geschäftsführung / Rechtsabteilung — Böblinger Str. 111 70199 Stuttgart

Versanddatum: 12.05.2026 per Einschreiben und E-Mail

5. Reaktion der Kunden

Frischbäcker AG: Eingang der Reaktion am 13.05.2026. Frischbäcker AG informiert, dass sie ihrerseits eine eigene Rechtsanwaltskanzlei mit der Prüfung möglicher Ansprüche beauftragt hat (Kanzlei Schwalm & Partner, Frankfurt). Mögliche Schadensersatzansprüche aus dem Rahmenvertrag werden angekündigt. RA Drosten prüft Haftungsrisiko Frischetrans gegenüber Frischbäcker AG.

Backhaus Süd GmbH & Co. KG: Noch keine Reaktion per 14.05.2026. Telefonische Nachfrage geplant.

6. Rechtliche Einschätzung: Haftungsrisiko gegenüber Kunden

Die Frischetrans könnte gegenüber ihren Kunden Haftungsansprüchen aus folgenden Grundlagen ausgesetzt sein:

1. **Vertragliche Haftung (§§ 280, 241 BGB):** Lieferausfälle durch den IT-Ausfall können Schadensersatzansprüche aus dem Transportvertrag auslösen, sofern kein Force-Majeure-Vorbehalt greift.
2. **Datenschutzhaftung (Art. 82 DSGVO):** Soweit bei Kunden natürliche Personen (Ansprechpartner) von der Datenpanne betroffen sind, können Ansprüche auf Schadensersatz nach Art. 82 DSGVO entstehen.
3. **Force Majeure:** Die meisten Logistikrahmenverträge (ADSp 2017 sind für Teile des Vertrages vereinbart) sehen Force-Majeure-Klauseln für Betriebsunterbrechungen durch externe Einwirkungen vor. Ein Ransomware-Angriff könnte als Force Majeure gelten. Dies ist jedoch im Einzelfall zu prüfen — sofern der Angriff auf vermeidbare Sicherheitslücken zurückzuführen ist, kann Force Majeure versagen.

Empfehlung: Ansprüche der Kunden werden ernst genommen. Soweit berechtigt, wird die Cyber-Versicherung (CyberCovered AG, Drittparteideckung) in Anspruch genommen. Frischetrans nimmt ProcessSpark in Regress (Aktenstück 10).

Datei: 17_mitarbeiter_information_bem_betroffenheit.md

Mitarbeiterinformation — BEM-Betroffenheit und Datenschutzpanne

Aktenstück: 17

Datum: 11.05.2026

Mandantin: Frischetrans Mittelrhein GmbH

Bearbeiter: RA Lukas Drosten / DSB Markus Feilke / HR-Leitung Frischetrans

1. Ausgangslage

Unter den 280 vom Datenverlust betroffenen Mitarbeitern befinden sich **38 Personen**, die Gesundheitsdaten aus BEM-Verfahren (Betriebliches Eingliederungsmanagement, § 167 Abs. 2 SGB IX) in den abgeflossenen Systemen gespeichert hatten. Diese 38 Personen erhalten eine gesonderte, individuellere Benachrichtigung, die über das allgemeine Mitarbeiterschreiben (Aktenstück 12, Version A) hinausgeht.

2. BEM-spezifische Information — Ergänzungsschreiben

Das folgende Schreiben wird den 38 BEM-betroffenen Mitarbeitern **persönlich und in versiegeltem Umschlag** übergeben — durch die jeweilige Teamleitung oder direkt durch die HR-Abteilung. Kein offener Aushang, keine E-Mail-Zustellung.

Frischetrans Mittelrhein GmbH Binger Straße 142 55131 Mainz

Mainz, den 11.05.2026

Streng vertraulich — Nur für Sie persönlich

[Name der/des Betroffenen]

Betreff: Ergänzende vertrauliche Information zum Datenschutzvorfall — Ihre BEM-Daten

Sehr geehrte/r [Anrede] [Name],

Sie haben bereits unser allgemeines Schreiben vom 11.05.2026 zum Datenschutzvorfall erhalten. Wir müssen Sie mit diesem Schreiben über einen besonderen Umstand informieren, der ausschließlich Sie und eine kleinere Gruppe von Kolleginnen und Kollegen betrifft.

Was ist betroffen?

Im Rahmen des Ransomware-Angriffs wurden leider auch Daten aus dem Betrieblichen Eingliederungsmanagement (BEM) von den Angreifern entwendet. Zu den betroffenen Daten können im Rahmen Ihres BEM-Verfahrens erfasste Informationen gehören — zum Beispiel ärztliche Bescheinigungen, Informationen zu Ihrer Erkrankung und über den Verlauf Ihrer Wiedereingliederung.

Wir wissen, dass diese Informationen zu den persönlichsten überhaupt gehören. Es tut uns außerordentlich leid, dass diese Informationen ungewollt in die Hände von Kriminellen geraten sind.

Was bedeutet das für Sie konkret?

- Die kriminellen Täter haben die gestohlenen Daten noch nicht veröffentlicht. Es gibt derzeit keine Hinweise, dass Ihre Gesundheitsdaten im Internet zugänglich sind.
- Die Strafverfolgungsbehörden (Kriminalpolizei Mainz) und das BSI sind eingeschaltet und ermitteln aktiv.
- Unser externer Datenschutzbeauftragter hat die Datenschutzbehörde (LfDI Rheinland-Pfalz) informiert, die die Angelegenheit begleitet.
- Wir beobachten die Aktivitäten der Tätergruppe rund um die Uhr und werden Sie unverzüglich informieren, sollte es zu einer Veröffentlichung kommen.

Was sollten Sie tun?

1. **Ruhe bewahren** — die Wahrscheinlichkeit, dass Ihre Daten gezielt gegen Sie verwendet werden, ist gering.
2. Wenn Sie der Meinung sind, dass jemand versucht, Sie mit diesen Informationen zu erpressen oder zu bedrohen, wenden Sie sich sofort an die Polizei **und** an uns.
3. Falls Sie psychisch belastet sind durch die Nachricht, nehmen Sie unser Angebot an:

Unser Hilfsangebot:

Wir haben in Absprache mit dem Betriebsrat ein **kostenloses und anonymes Beratungsangebot** für die betroffenen Mitarbeiterinnen und Mitarbeiter eingerichtet:

Externe Mitarbeiterberatung (EAP): Counselling Rheinland GmbH (unabhängig, streng vertraulich)
Freecall: 0800 / 4473 0000 (täglich 0–24 Uhr) E-Mail: bem-hilfe@counselling-rheinland.de (Bitte bei Erstkontakt: Code FTM CARE2026 angeben)

Externer Datenschutzbeauftragter: Markus Feilke — direkte Durchwahl für BEM-Betroffene: +49 6131 9944-12 (Terminvereinbarung auch außerhalb der Geschäftszeiten)

Ihre Rechte:

- Sie haben das Recht, sich beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI RLP) zu beschweren: www.datenschutz.rlp.de, Telefon: +49 6131 8920-0
- Sie haben das Recht auf Auskunft über die über Sie gespeicherten Daten (Art. 15 DSGVO) — richten Sie Ihre Anfrage an den DSB Markus Feilke.
- Sie haben das Recht auf Schadensersatz (Art. 82 DSGVO), sofern Ihnen durch die Datenpanne ein nachweisbarer Schaden entsteht.

Wir bedauern diesen Vorfall zutiefst. Das Vertrauen, das Sie uns durch Ihre Teilnahme am BEM entgegengebracht haben, war und ist für uns eine besondere Verantwortung. Wir nehmen diese Verantwortung ernst.

Mit freundlichen Grüßen und aufrichtigem Bedauern

Theresia Wallbruck Geschäftsführerin Frischetrans Mittelrhein GmbH

und

Markus Feilke Externer Datenschutzbeauftragter

3. Organisatorische Maßnahmen bei der Übergabe

3.1 Identifikation der 38 BEM-Betroffenen

Die Liste der 38 betroffenen Mitarbeiter wurde durch die HR-Leiterin Barbara Seifert erstellt. Die Liste wurde in einem separaten, mit Passwort gesicherten und verschlüsselten Dokument geführt und ist nur dem DSB, der HR-Leiterin, der Geschäftsführerin und RA Drostens zugänglich.

Wichtig: Die Tatsache, dass ein Mitarbeiter ein BEM-Schreiben erhalten hat, darf keinem Kollegen, keinem Vorgesetzten und keiner sonstigen Person bekannt werden. Absolute Vertraulichkeit ist geboten.

3.2 Übergabeprotokoll

Alle 38 Schreiben wurden am 11.05.2026 zwischen 11:00 und 14:30 Uhr im gesonderten Besprechungsraum 2 (Binger Straße 142, EG rechts) unter Ausschluss Dritter persönlich übergeben. Betroffene Mitarbeiter im Außendienst / im Fahrerbetrieb erhielten das Schreiben per Einschreiben an die private Wohnanschrift.

Jeder Betroffene hat den Empfang durch Unterschrift auf einer vertraulichen Empfangsliste bestätigt. Die Empfangsliste ist in der physischen Mandantenakte der Kanzlei Drostens & Pekonkur hinterlegt.

4. Betriebsratsinformation (Koordination mit Aktenstück 18)

Der Betriebsrat wurde in der Sitzung vom 11.05.2026 über das Vorgehen bei der BEM-Mitarbeiterinformation informiert. Der Betriebsrat hat zugestimmt, dass das vorliegende Verfahren (vertrauliche Einzelübergabe, EAP-Angebot) angemessen ist.

Der Betriebsrat hat darauf hingewiesen, dass Mitarbeiter, die Beratungsbedarf haben, auch über den Betriebsrat Kontakt aufnehmen können (BR-Vorsitzende: Klaus Hoffmann, Zimmer 112).

5. Monitoring und Folge-Kommunikation

RA Drosten und DSB Feilke beobachten die Leakseiten der Tätergruppe auf Veröffentlichung. Im Falle einer Veröffentlichung wird eine sofortige Folge-Kommunikation an die 38 Betroffenen veranlasst.

Geplantes nächstes Kommunikationsupdate an die Mitarbeiter: 25.05.2026 (soweit bis dahin keine wesentlichen neuen Erkenntnisse).

Datei: 18_betriebsrat_anhoerung.md

Betriebsratsanhörung — Datenschutzpanne und IT-Vorfall

Aktenstück: 18

Datum: 11.05.2026

Ort: Frischetrans Mittelrhein GmbH, Besprechungsraum 1, Binger Straße 142, Mainz

Art: Außerordentliche Betriebsratsanhörung (§ 102 BetrVG analog, § 87 BetrVG, § 75 BetrVG)

Protokoll erstellt durch: Barbara Seifert (HR-Leiterin, protokollführend)

1. Teilnehmende

Arbeitgeberseite:

- Theresia Wallbruck (Geschäftsführerin)
- Barbara Seifert (HR-Leiterin)
- RA Lukas Drosten (anwaltliche Begleitung, beratend)
- DSB Markus Feilke (Datenschutzbeauftragter, beratend)

Betriebsrat:

- Klaus Hoffmann (BR-Vorsitzender)
- Sabine Meurer (Stellv. BR-Vorsitzende)
- Rainer Schäper (BR-Mitglied, Logistik)
- Fatma Yilmaz (BR-Mitglied, Verwaltung)
- Werner Böckler (BR-Mitglied, Fahrer)

2. Zweck der Anhörung

Die Geschäftsführerin informierte den Betriebsrat über den Ransomware-Angriff vom 06.05.2026 und seine Auswirkungen auf die Beschäftigten. Die Anhörung dient:

1. Der Erfüllung der gesetzlichen Unterrichtungspflicht nach § 80 Abs. 2 BetrVG (Unterrichtungsrecht des Betriebsrats)
2. Der Anhörung des Betriebsrats zu Maßnahmen, die die Belegschaft betreffen (§ 87 BetrVG)
3. Der Erörterung des Schutzes von BEM-Daten gemäß § 75 Abs. 2 BetrVG (Persönlichkeitsrecht der Arbeitnehmer)

3. Darstellung des Vorfalls durch die Geschäftsführerin

Theresia Wallbruck schilderte den Vorfall in allen wesentlichen Aspekten (vgl. Chronologie Aktenstück 02). Sie betonte:

- Der Angriff war ein Angriff von außen durch kriminelle Hacker.
- Die Belegschaft trägt keine Verantwortung für den Angriff.
- Frischetrans hat alle gesetzlich vorgeschriebenen Meldungen erstattet.
- Es wird nicht nachgegeben (kein Lösegeld).

4. Erörterte Themen

4.1 Datenschutz der Mitarbeiter (BEM-Daten)

BR-Vorsitzender Hoffmann: „Wir möchten wissen, wie viele unserer Kollegen von der Weitergabe ihrer Gesundheitsdaten betroffen sind und welche konkreten Schutzmaßnahmen ergriffen wurden.“*

DSB Feilke erläuterte: 38 Mitarbeiter sind mit BEM-Gesundheitsdaten betroffen. Die Daten wurden nicht freiwillig weitergegeben, sondern durch einen kriminellen Angriff entwendet. Datenschutzbehörde und Kriminalpolizei sind informiert.

Beschluss: Der Betriebsrat stimmt dem Verfahren zur Benachrichtigung der 38 betroffenen Mitarbeiter (Aktenstück 17) zu. Der Betriebsrat bittet, die vollständige DSFA (Aktenstück 11) zur Kenntnis zu erhalten.

4.2 Technische Überwachungseinrichtungen (§ 87 Abs. 1 Nr. 6 BetrVG)

BR-Mitglied Yilmaz: „Welche neuen Überwachungssysteme werden im Rahmen der IT-Sicherheitsmaßnahmen eingeführt? Wird der Betriebsrat beteiligt?“*

RA Drostens erläuterte: Im Rahmen der IT-Sicherheitsmaßnahmen (SIEM-Ausbau, Endpointschutz, Netzwerküberwachung) werden möglicherweise Systeme eingeführt, die auch das Nutzerverhalten protokollieren. Der Betriebsrat hat ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG bei technischen Einrichtungen, die das Verhalten der Arbeitnehmer überwachen können.

Vereinbarung: Vor der Einführung neuer IT-Sicherheitssysteme wird der Betriebsrat einbezogen und eine Betriebsvereinbarung abgeschlossen.

4.3 KI-System „PalettenAuge AI“ (§ 87 Abs. 1 Nr. 6 BetrVG)

RA Drostens informierte den Betriebsrat über das KI-System „PalettenAuge AI“ und seine Einordnung als Hochrisiko-KI-System nach der EU-KI-Verordnung. Der Betriebsrat hat nach § 87 Abs. 1 Nr. 6 BetrVG ein Mitbestimmungsrecht, da PalettenAuge AI das Verhalten der Fahrer (Tourdaten, Leistungsdaten) auswertet.

BR-Vorsitzender Hoffmann: „Das wussten wir in dieser Form nicht. Wir fordern eine vollständige Dokumentation dieses Systems. Eine Betriebsvereinbarung ist zwingend.“*

Vereinbarung: Abschluss einer Betriebsvereinbarung „KI-Systeme und Leistungsdaten“ bis 30.06.2026. Bis dahin läuft PalettenAuge AI in eingeschränktem Modus (nur Routenoptimierung, keine Personaldaten-Einspeisung).

4.4 Open-Source-Audit TourPlanner

RA Drostens informierte den Betriebsrat kurz über die AGPL-3.0-Compliance-Fragen beim TourPlanner. Der Betriebsrat hat hierzu keine unmittelbaren Mitbestimmungsrechte, nahm die Information zur Kenntnis.

4.5 Gesundheitsschutz der Belegschaft / Psychosoziale Unterstützung

BR-Mitglied Schäper: „Viele Fahrer sind verunsichert. Sie fragen sich, ob ihre Bankdaten jetzt gestohlen werden. Können wir eine Informationsveranstaltung machen?“*

Vereinbarung: Frischetrans organisiert gemeinsam mit dem Betriebsrat eine Mitarbeiterversammlung zum Thema Datensicherheit und Schutzmaßnahmen bis 20.05.2026. DSB Feilke und RA Drostens werden in kurzen Beiträgen die wichtigsten Informationen geben.

Das EAP-Angebot (Counselling Rheinland GmbH, 0800/4473 0000) wird allen Mitarbeitern kommuniziert.

4.6 Auskunft und Einsichtsrecht des Betriebsrats

Der Betriebsrat beantragte Einsicht in:

1. Die vollständige DSFA für BEM-Daten (Art. 35 DSGVO)
2. Den forensischen Zwischenbericht
3. Die Liste der geplanten IT-Sicherheitsmaßnahmen und deren Zeitplan

GF Wallbruck sicherte zu, diese Unterlagen dem Betriebsrat bis 18.05.2026 zugänglich zu machen.

5. Beschlüsse des Betriebsrats

| Beschluss | Abstimmungsergebnis |
|--|---------------------|
| Zustimmung zum Mitarbeiter-Benachrichtigungsverfahren (Aktenstück 12, 17) | Einstimmig |
| Forderung Betriebsvereinbarung KI-Systeme (PalettenAuge AI) bis 30.06.2026 | Einstimmig |
| Forderung Betriebsvereinbarung neue IT-Sicherheitssysteme | Einstimmig |
| Anforderung DSFA, Forensikbericht, IT-Maßnahmenplan | Einstimmig |
| Zustimmung EAP-Angebot (Counselling Rheinland) | Einstimmig |
| Mitarbeiterversammlung 20.05.2026 | Einstimmig |

6. Nächste Schritte

| Maßnahme | Zuständig | Termin |
|--|---------------|------------|
| Unterlagen-Übermittlung an BR | GF Wallbruck | 18.05.2026 |
| Mitarbeiterversammlung | HR + BR | 20.05.2026 |
| Entwurf Betriebsvereinbarung KI-Systeme | RA Drost | 31.05.2026 |
| Unterzeichnung Betriebsvereinbarung KI-Systeme | GF + BR | 30.06.2026 |
| Entwurf Betriebsvereinbarung IT-Sicherheit | RA Drost / IT | 15.06.2026 |

Protokoll genehmigt durch:

Klaus Hoffmann (BR-Vorsitzender): _____ Theresia Wallbruck (Geschäftsführerin): _____
Datum: 11.05.2026

Datei: 19_pressemitteilung_entwurf_redacted.md

Pressemitteilung — Entwurf (Kanzlei-Freigabe: 13.05.2026)

Aktenstück: 19

Status: Entwurf — freigegeben durch RA Drost am 13.05.2026; Veröffentlichung nach Zustimmung Mandantin

Veröffentlichung geplant: Nach Rücksprache mit CyberCovered AG und LfDI RLP, frühestens 15.05.2026

Verteilung: dpa-Basisdienst, lokale Medien (Allgemeine Zeitung Mainz, Rhein-Zeitung), Branchenmedien (Lebensmittel Zeitung, Verkehrsrundschau)

Interne Vorbemerkung (nicht für Veröffentlichung)

Dieser Entwurf wurde von RA Drost in enger Abstimmung mit Geschäftsführerin Wallbruck und der Presseagentur PR-Rhein GmbH (Mainz) erarbeitet. Die Pressemitteilung soll:

1. Den Vorfall proaktiv kommunizieren, bevor Medien durch andere Quellen (ZAC, LfDI, Datenlecks) informiert werden
2. Vertrauen in die Handlungsfähigkeit des Unternehmens signalisieren
3. Rechtlich keine unnötigen Haftungseingeständnisse enthalten

4. Keine Namen von Mitarbeitern oder Kunden nennen

Freigabe durch Kanzlei: **Ja** (RA Drost, 13.05.2026) Freigabe durch Mandantin: **Ausstehend** Freigabe durch CyberCovered AG: **Ausstehend**

Pressemitteilung

PRESSEMITTEILUNG

Frischetrans Mittelrhein GmbH Binger Straße 142 · 55131 Mainz Kontakt Presse:
pr@frischetrans-mittelrhein.de · +49 6131 8820-140

Mainz, [DATUM EINSETZEN]

Frischetrans Mittelrhein GmbH war Opfer eines Cyberangriffs — umfassende Maßnahmen eingeleitet

Die Frischetrans Mittelrhein GmbH, ein führender Anbieter von B2B-Frischelogsitik für die Lebensmittelbranche mit Sitz in Mainz, bestätigt, dass das Unternehmen Anfang Mai 2026 Ziel eines schwerwiegenden Ransomware-Angriffs geworden ist.

Was ist passiert?

In der Nacht vom 5. auf den 6. Mai 2026 haben unbekannte Täter die IT-Infrastruktur von Frischetrans mit einer Schadsoftware infiziert. Dabei wurden Teile des IT-Systems verschlüsselt und eine Datenmenge aus dem internen Netzwerk entwendet. Die betroffenen Systeme konnten inzwischen zu weiten Teilen aus gesicherten Datensicherungen wiederhergestellt werden.

Sofortige Maßnahmen

Das Unternehmen hat unmittelbar nach Bekanntwerden des Angriffs folgende Schritte eingeleitet:

- Notfallabschaltung der betroffenen IT-Systeme
- Beauftragung eines spezialisierten Cyber-Sicherheitsunternehmens zur forensischen Analyse
- Erstattung einer Strafanzeige bei der Kriminalpolizei Mainz
- Information aller zuständigen Behörden, einschließlich des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des Landesbeauftragten für den Datenschutz Rheinland-Pfalz

Auswirkungen auf den Betrieb

Der Betrieb von Frischetrans war vorübergehend eingeschränkt. Kundenlieferungen, die in den ersten Tagen nach dem Vorfall betroffen waren, wurden so weit wie möglich durch manuelle Planung und engsten Kundenkontakt kompensiert. Seit dem [DATUM] ist der Betrieb wieder vollständig aufgenommen.

Datenschutz

Aus Vorsichtsgründen hat Frischetrans betroffene Mitarbeiterinnen und Mitarbeiter sowie betroffene Geschäftspartner bereits persönlich und vertraulich informiert. Wir nehmen den Schutz personenbezogener Daten sehr ernst und arbeiten eng mit den Datenschutzbehörden zusammen.

Kein Lösegeld

Frischetrans hat — in Übereinstimmung mit den Empfehlungen der Sicherheitsbehörden und seiner Anwälte — keine Lösegeldzahlung geleistet.

Statement der Geschäftsführerin

Theresia Wallbruck, Geschäftsführerin von Frischetrans Mittelrhein GmbH: „Dieser Angriff hat uns getroffen wie alle anderen Unternehmen, die täglich mit ihren Systemen arbeiten. Wir haben sofort gehandelt, alle Behörden informiert und tun alles, um unsere Mitarbeiterinnen und Mitarbeiter, unsere Kunden und unsere Geschäftspartner zu schützen. Frischetrans ist wieder voll einsatzbereit, und wir werden gestärkt aus dieser Krise hervorgehen.“*

Über Frischetrans Mittelrhein GmbH

Frischetrans Mittelrhein GmbH ist ein führender Anbieter von B2B-Frischelogistik mit Sitz in Mainz. Mit 280 Mitarbeitern und einem Fuhrpark von 64 Fahrzeugen beliefert Frischetrans täglich Großbäckereien, Lebensmittelketten und gastronomische Betriebe in der Rhein-Main-Neckar-Region.

Pressekontakt: PR-Rhein GmbH im Auftrag der Frischetrans Mittelrhein GmbH Telefon: +49 6131 8820-140 E-Mail: pr@frischetrans-mittelrhein.de

Anmerkungen der Kanzlei zur Pressemitteilung

Bewusste Auslassungen:

1. Keine Nennung der Erpressersumme — würde unnötige Spekulationen anregen
2. Kein Verweis auf ProcessSpark und CVE-2026-0712 — laufende rechtliche Auseinandersetzung
3. Kein Verweis auf konkrete Anzahl betroffener Personen — vermeidet Anreizsetzung für Ansprüche
4. Kein Verweis auf AGPL-Audit oder KI-VO-Problematik — keine Verknüpfung mit dem Ransomware-Vorfall

Rechtliche Klarstellungen:

- Aussage „sofort gehandelt“ ist korrekt und belegt
- Statement Wallbruck ist juristisch geprüft — keine Haftungseingeständnisse
- Begriffe „betroffen“ statt „verletzt“ oder „gestohlen“ — bewusst weniger dramatisch

Freigabe-Checkliste:

- ☐ Freigabe durch GF Wallbruck
- ☐ Freigabe CyberCovered AG (Presseabteilung)
- ☐ Abstimmung mit LfDI RLP (Timing — Behörde soll nicht überrascht werden)
- ☐ ZAC Mainz informiert über geplante Veröffentlichung
- ☐ Abstimmung Erscheinungsdatum mit PR-Rhein GmbH

Datei: 20_strategiememorandum_drosten.md

Strategiememorandum — RA Lukas Drosten

Aktenstück: 20

Datum: 13.05.2026

Mandantin: Frischetrans Mittelrhein GmbH

Verfasser: RA Lukas Drosten, Fachanwalt für IT-Recht

1. Überblick und Gesamtlage

Sieben Tage nach dem Ransomware-Angriff lässt sich eine erste fundierte strategische Gesamtbewertung vornehmen. Das Mandat hat sich von einer reinen Notfall-Reaktion zur umfassenden IT-rechtlichen Beratung entwickelt und umfasst nunmehr folgende Komplexe:

| Komplex | Priorität | Status |
|---|-------------|--|
| A. Datenschutz / DSGVO (Art. 33, 34, 35) | Hoch | Erstmeldungen erstattet, DSFA eingeleitet |
| B. NIS2 / BSI-Meldung | Hoch | Erstattet |
| C. Strafanzeige ZAC Mainz | Hoch | Erstattet |
| D. ProcessSpark — SLA-Verletzung / Schadensersatz | Sehr hoch | Klageandrohung raus, Frist bis 26.05.2026 |
| E. KI-VO — PalettenAuge AI | Mittel | Analyse abgeschlossen, Maßnahmen eingeleitet |
| F. Open Source Compliance TourPlanner | Mittel | Audit abgeschlossen, Handlungsoptionen identifiziert |
| G. Betriebsrat / Mitarbeiter | Hoch | Anhörung erledigt, BV-Entwürfe folgen |
| H. Versicherung CyberCovered | Hoch | Gemeldet, Regulierung in Lauf |
| I. Kundenkommunikation / Schadensersatz Kunden | Mittel-Hoch | Anschreiben raus, Frischbäcker AG zeigt Ansprüche |

2. Rechtliche Kernrisiken und Risikobewertung

2.1 DSGVO-Bußgeldrisiko

Risikoprofil: Mittel bis Hoch

Der LfDI RLP hat die Meldung entgegengenommen und Rückfragen gestellt. Die entscheidende Frage ist, ob der LfDI ein Bußgeldverfahren eröffnet. Relevante Gesichtspunkte:

- **Positiv:** Frischetrans hat alle Meldepflichten fristgerecht erfüllt (Art. 33 DSGVO: innerhalb 72 h; BSI: innerhalb 24 h). Proaktive Transparenz gegenüber Behörden.
- **Negativ:** Die TOMs (technisch-organisatorische Maßnahmen) waren zum Zeitpunkt des Angriffs für die Verarbeitung von Art.-9-Daten (Gesundheitsdaten BEM) unzureichend (fehlende at-rest-Verschlüsselung, unzureichendes Patch-Management).

- **Mildernd:** Die unmittelbaren Mängel (Patch-Rückstand) sind auf den IT-Dienstleister ProcessSpark zurückzuführen. Frischetrans hat die Patchverantwortung vertraglich an ProcessSpark übertragen. Dies mindert das eigene Verschulden, entlastet aber nicht vollständig.

Bußgeldrisiko-Schätzung: 50.000–350.000 EUR (Art. 83 Abs. 4 DSGVO, Verstöße gegen Art. 32 DSGVO; Bußgeldrahmen 10 Mio. EUR / 2 %)

Strategie: Vollständige Kooperation mit LfDI, schnelle Umsetzung der DSFA-Maßnahmen, Vorlage eines detaillierten Verbesserungsplans — dies mildert Bußgelder erheblich.

2.2 ProcessSpark — Klagerisiko und Einigungschance

Risikoprofil: Hoch (Klagerisiko für ProcessSpark), Mittel (Prozessrisiko für Frischetrans)

Die Haftungssituation gegen ProcessSpark ist gut. Die Beweislage (SAP Security Note, Patch-Log, forensischer Bericht) ist stark. Der einzige nennenswerte Unsicherheitsfaktor ist die Haftungsbeschränkungsklausel (§ 16 Vertrag), deren Wirksamkeit aber bezweifelt werden darf.

Realistische Einigungschance: 60–70 % (außergerichtliche Einigung nach Klageandrohung). ProcessSpark hat kein Interesse an einem öffentlichen Prozess mit Aufmerksamkeit auf CVE-2026-0712-Patchversagen.

Strategie: Die Frist (26.05.2026) wird konsequent gehalten. Bei Nichtreaktion: Klageeinreichung am LG Mainz (AZ 3 O 88/26). Gleichzeitig Offenheit für Mediationsverfahren oder EU-ODR-Verhandlung (Skill fachanwalt-it-recht-it-vertrag-verhandlung-eu-odr).

Alternative: Sanierungsverhandlung mit ProcessSpark: Klage wird ausgesetzt gegen Zusage erhöhter SLAs, Kostenerstattung, Vertragsanpassung (neue Patchpflichten). Sinnvoll, wenn Mandantin den Vertrag fortsetzen möchte.

2.3 Kundenforderungen (Frischbäcker AG)

Risikoprofil: Mittel

Frischbäcker AG hat anwaltliche Beratung eingeholt und prüft Schadensersatzansprüche. Hauptargument wird der Betriebsunterbrechungsschaden (Lieferausfall 07.05.2026) sein.

Strategie: CyberCovered AG (Drittparteideckung) informieren. Force-Majeure-Einwand aus Rahmenvertrag prüfen. Ggf. Vergleich anbieten, wenn Forderung überschaubar.

2.4 KI-VO — Fristrisiko (02.08.2026)

Die EU-KI-VO Hochrisikopflichten gelten ab 02.08.2026. Bis dahin sind noch **81 Tage**. Das ist knapp. PalettenAuge AI muss bis dahin entweder:

- vollständig konform gemacht werden (Konformitätsbewertung durch DachAuge, Betriebsvereinbarung, Human-Oversight-Prozess), oder
- in eingeschränktem Modus betrieben werden (keine Personaldaten-Einspeisung).

Risiko bei Nichthandeln: Bußgeld bis 15 Mio. EUR (Art. 99 KI-VO) — für KMU deutlich reduziert, aber empfindlich.

2.5 Open Source / AGPL

Kurzfristig kein behördliches Risiko. Aber Abmahnungsrisiko durch ScheduleHero Foundation ist real. Die Kosten einer außergerichtlichen Einigung (kommerzielle Lizenz oder freiwillige Code-Offenlegung) sind überschaubar im Vergleich zu einem Rechtsstreit.

3. Mandatspriorisierung (Empfehlung)

| Priorität | Maßnahme | Frist | Zuständig |
|-----------|---|----------------|---------------------------|
| 1 | ProcessSpark: Frist überwachen (26.05.2026) | 26.05.2026 | RA Drosten |
| 2 | LfDI: DSFA und Verbesserungsplan einreichen | 22.05.2026 | RA Drosten + DSB Feilke |
| 3 | Betriebsrat: Betriebsvereinbarung KI | 30.06.2026 | RA Drosten |
| 4 | DachAuge: Konformität sdokumentation anfordern | 20.05.2026 | RA Drosten |
| 5 | AGPL: Kontaktaufnahme ScheduleHero Foundation | 20.05.2026 | RA Drosten |
| 6 | Versicherung: Schaden sdokumentation komplett | 31.05.2026 | Frischetrans + RA Drosten |
| 7 | Mitarbeiterversammlung organisieren | 20.05.2026 | HR + BR |
| 8 | ProcessSpark-Klage vorbereiten (Schriftsatz LG Mainz) | Bis 10.06.2026 | RA Drosten |

4. Gesamteinschätzung

Der Mandantin ist zu bescheinigen, dass sie in dieser Ausnahmesituation trotz enormer operativer Belastung kluge Entscheidungen getroffen hat: keine Lösegeldzahlung, sofortige Behördenkommunikation, proaktive Mitarbeiterinformation, konstruktive Zusammenarbeit mit der Kanzlei. Das ist der Idealfall einer datenschutzrechtlichen Incident Response.

Die größten verbleibenden Risiken sind (a) ein mögliches LfDI-Bußgeld (mittelbar durch ProcessSparks Patchversagen verursacht), (b) die KI-VO-Compliance-Frist für PalettenAuge AI und (c) die AGPL-Compliance-Frage für TourPlanner.

Der Fall gegen ProcessSpark ist juristisch stark und verspricht hohe Erfolgchancen.

Gesamtschadenspotenzial Mandantin (worst case): ca. 1,2–2,0 Mio. EUR

Erwartetes Regressvolumen aus ProcessSpark: ca. 500.000–700.000 EUR (netto nach Prozesskosten)

Versicherungsdeckung: bis 5 Mio. EUR (abzügl. Selbstbehalt 25.000 EUR laut Police)

Netto-Belastung Mandantin (Schätzung): ca. 100.000–400.000 EUR

Datei: 21_kostenrisiko_streitwert_analyse.md

Kostenrisiko und Streitwertanalyse

Aktenstück: 21

Datum: 13.05.2026

Mandantin: Frischetrans Mittelrhein GmbH

Bearbeiter: RA Lukas Drost, Fachanwalt für IT-Recht

1. Überblick Kostenrisiko-Matrix

| Komplex | Streitwert / Bußgeld | Prozesswahrscheinlichkeit | Erwartetes Kostenrisiko |
|---|---------------------------------|-----------------------------|---|
| A. ProcessSpark-Klage (LG Mainz) | 681.818 EUR | Hoch (falls keine Einigung) | 35.000–55.000 EUR
Prozesskosten (1. Instanz) |
| B. DSGVO-Bußgeld LfDI RLP | bis 350.000 EUR | Mittel | 50.000–350.000 EUR |
| C. Kundenforderungen (Frischbäcker AG) | geschätzt
50.000–150.000 EUR | Mittel | 20.000–80.000 EUR
(ggf. Versicherung) |
| D. KI-VO-Bußgeld (PalettenAuge AI) | bis 15 Mio. EUR (Art. 99) | Niedrig | 0–200.000 EUR
(KMU-Staffel) |
| E. AGPL-Abmahnung (TourPlanner) | 5.000–50.000 EUR | Niedrig | 5.000–15.000 EUR |
| F. Eigene Anwaltskosten (Mandat gesamt) | — | Sicher | 80.000–150.000 EUR |
| G. IT-Wiederherstellung | — | Sicher | 180.000–230.000 EUR |
| H. Forensikkosten | — | Sicher | 45.000–65.000 EUR |
| I. Betriebsausfall (nicht versichert, Selbstbehalt) | — | Sicher | 25.000 EUR
(Selbstbehalt) |

2. Streitwertanalyse ProcessSpark-Klage (LG Mainz, AZ 3 O 88/26)

2.1 Streitwert der Klage

Der Streitwert der geplanten Klage gegen ProcessSpark Cloud AG setzt sich zusammen aus:

| Klagepunkt | Betrag |
|--|-------------|
| Schadensersatz
Wiederherstellung IT | 198.500 EUR |
| Schadensersatz
Betriebsausfall | 387.200 EUR |

| Klagepunkt | Betrag |
|--|------------------------|
| Schadensersatz
Forensik | 52.800 EUR |
| Schadensersatz
Anwaltskosten
(Teilforderung) | 24.800 EUR |
| Schadensersatz
DSGVO-Folgekosten | 18.000 EUR |
| Vertragsstrafe | 518 EUR |
| **Klagebetrag gesamt
(vorläufig)** | **681.818 EUR** |

Vorbehalt: Erhöhung des Klageantrags nach forensischem Abschlussbericht möglich (Streitwert dann ggf. bis 850.000 EUR).

2.2 Anwaltskosten (RVG-Berechnung, 1. Instanz LG Mainz)

Streitwert: 681.818 EUR

Basis: RVG-Vergütungsverzeichnis (VV RVG), Anlage 1

| Gebühr | Multiplikator | Berechnungsbasis
(Gebühr aus Streitwert) | Betrag |
|--|---------------|---|--------------------------------------|
| 1,3-Verfahrensgebühr
(Nr. 3100 VV RVG) | 1,3 | Grundgebühr aus
681.818 EUR (= 3.668
EUR) | 4.768,40 EUR |
| 1,2-Terminsgebühr (Nr.
3104 VV RVG) | 1,2 | 3.668 EUR | 4.401,60 EUR |
| Einigungsgebühr (Nr.
1003 VV RVG, falls
Vergleich) | 1,5 | 3.668 EUR | 5.502 EUR |
| Post/Telekommunikations-
pauschale | — | 20 EUR je | 20 EUR |
| **Gesamtgebühren RA
(ca., ohne USt.)** | | | **ca. 14.000–16.000
EUR** |

Hinweis: Die eigenen Anwaltsgebühren der Mandantin sind im Unterliegensfall von ProcessSpark zu erstatten (§ 91 ZPO), im eigenen Unterliegensfall selbst zu tragen.

Gerichtskosten (GKG):

Bei einem Streitwert von 681.818 EUR:

| Position | Betrag (geschätzt) |
|--|--------------------|
| 3,0-fache
Gerichtsgebühr (GKG
Anlage 1, Klage
streitig) | ca. 10.500 EUR |

| Position | Betrag (geschätzt) |
|---|--------------------|
| Mindest-Vorschuss bei Klageeinreichung (mind. 3-fach) | ca. 10.500 EUR |

2.3 Kostenrisiko Prozessverlust

Im Falle eines vollständigen Unterliegens vor dem LG Mainz trüge die Mandantin:

- Eigene Anwaltskosten: ca. 14.000–16.000 EUR
- Gerichtskosten: ca. 10.500 EUR
- Anwaltskosten der Gegenseite (ProcessSpark): ca. 14.000–16.000 EUR

Gesamtrisiko im Unterliegensfall (1. Instanz): ca. 38.500–42.500 EUR

Einschätzung: Das Prozessrisiko ist angesichts der guten Beweislage überschaubar. Die Klageandrohung ist wirtschaftlich gerechtfertigt.

3. DSGVO-Bußgeld — Schätzung

3.1 Bußgeldrahmen (Art. 83 DSGVO)

- Art. 83 Abs. 3 DSGVO: Verstoß gegen Art. 32 DSGVO (unzureichende TOMs) → max. 10 Mio. EUR oder 2 % des weltweiten Jahresumsatzes (Frischetrans: 38 Mio. EUR × 2 % = 760.000 EUR)

3.2 Bußgeldbemessung (Art. 83 Abs. 2 DSGVO — Zumessungskriterien)

| Faktor | Bewertung | Einfluss auf Bußgeld |
|-----------------------------------|--|----------------------|
| Art und Schwere des Verstoßes | Gesundheitsdaten betroffen, hohe Schwere | Erhöhend |
| Fahrlässigkeit | Eher mittelbar (durch ProcessSpark verursacht) | Mildernd |
| Schadensbegrenzungsmaßnahmen | Sofortige Reaktion, vollständige Kooperation | Stark mildernd |
| Kooperationsbereitschaft mit LfDI | Hoch (fristgerechte Meldung, DSFA eingeleitet) | Stark mildernd |
| Vorherige Verstöße | Keine | Mildernd |
| Kategorien betroffener Daten | Gesundheitsdaten (Art. 9) | Erhöhend |
| Anzahl betroffener Personen | 298 Personen | Erhöhend |
| Unternehmensgröße | KMU (280 MA) | Mildernd |

Schätzung Bußgeld: 30.000–200.000 EUR

4. Gesamtkostenplanung (Liquiditätsbedarf Mandantin)

| Ausgabeblock | Zeitraum | Betrag |
|--|----------------|------------------------|
| Sofortkosten (Forensik, IT-Notfall) | Mai 2026 | 220.000 EUR |
| Anwaltskosten lfd. Mandat | Mai–Aug. 2026 | 80.000 EUR |
| IT-Wiederherstellung (vollständig) | Mai–Juni 2026 | 210.000 EUR |
| DSGVO-Compliance-Maßnahmen | Mai–Aug. 2026 | 45.000 EUR |
| KI-VO-Compliance (PalettenAuge) | Juni–Aug. 2026 | 30.000 EUR |
| Open-Source-Compliance | Mai–Juni 2026 | 10.000 EUR |
| PR/Krisenkommunikation | Mai 2026 | 15.000 EUR |
| Selbstbehalt Versicherung | sofort | 25.000 EUR |
| **Gesamtliquiditätsbedarf (Eigenmittel, vor Versicherungsleistung)** | | **635.000 EUR** |

Erwartete Versicherungsleistung (CyberCovered AG): ca. 450.000–700.000 EUR

Erwarteter Schadensersatz ProcessSpark (nach Einigung/Klage): ca. 400.000–600.000 EUR

Netto-Belastung Frischetrans (Schätzung): ca. 0–200.000 EUR (sofern Versicherung und Regressansprüche planmäßig funktionieren)

5. Empfehlung zur Liquiditätssicherung

RA Drostent empfiehlt der Mandantin, mit ihrer Hausbank (Sparkasse Mainz) eine Kreditlinie von mindestens 500.000 EUR für die Dauer des Krisenmanagements zu vereinbaren, um Liquiditätsengpässe zu überbrücken, bis Versicherungsleistungen und Schadensersatz fließen.

Datei: 22_fristenuebersicht_meldepflichten.md

Fristenübersicht — Meldepflichten und Verfahrensfristen

Aktenstück: 22

Datum: 13.05.2026 (Stand: aktuell)

Mandantin: Frischetrans Mittelrhein GmbH

Bearbeiter: RA Lukas Drostent, Fachanwalt für IT-Recht

1. Gesetzliche Meldepflichten (Incident Response)

| Frist | Rechtsgrundlage | Adressat | Fristablauf | Status | Aktenzeichen /Ref. |
|-----------------------------------|------------------------------|------------------------------|-----------------------|--|--------------------------|
| 72 h — DSGVO-Meldung | Art. 33 Abs. 1 DSGVO | LfDI Rheinland-Pfalz | 09.05.2026, 04:17 Uhr | **Erledigt**
(08.05.2026, 22:45 Uhr) | LfDI-RLP-2026-0508-4419 |
| 24 h — NIS2-Erstmeldung | § 31 Abs. 3 Nr. 1 NIS2UmsuG | BSI Außenstelle Frankfurt | 07.05.2026, 04:17 Uhr | **Erledigt**
(07.05.2026, 16:30 Uhr) | BSI-REF-2026-1847 |
| 72 h — NIS2-Folgebericht | § 31 Abs. 3 Nr. 2 NIS2UmsuG | BSI Außenstelle Frankfurt | 10.05.2026, 16:30 Uhr | **Erledigt**
(10.05.2026, 15:00 Uhr) | BSI-REF-2026-1847/2 |
| Unverzüglich — Art. 34 DSGVO | Art. 34 Abs. 1 DSGVO | Betroffene Personen (280 MA) | Unverzüglich | **Erledigt**
(11.05.2026) | — |
| 1 Monat — NIS2-Abschlussbericht | § 31 Abs. 3 Nr. 3 NIS2UmsuG | BSI Außenstelle Frankfurt | 07.06.2026 | **Offen** | — |
| 14 Tage — DSGVO-Ergänzungsmeldung | Art. 33 Abs. 4 DSGVO | LfDI Rheinland-Pfalz | 22.05.2026 | **Offen** | — |
| 24 h — Versicherungsmeldung | Police CC-2024-FTM-8801, § 4 | CyberCovered AG | 07.05.2026, 04:17 Uhr | **Erledigt**
(07.05.2026, 14:30 Uhr) | CC-SCHADEN-2026-FTM-0914 |

2. Verfahrensfristen — ProcessSpark

| Frist | Beschreibung | Termin | Status |
|--|--------------------------------------|-----------------------|----------|
| Klageandrohungsschreiben | Versand an ProcessSpark | 12.05.2026 | Erledigt |
| Reaktionsfrist ProcessSpark (Zahlung/Einigung) | 14 Tage nach Zugang (ca. 13.05.2026) | **26.05.2026** | Offen |
| Auskunftserteilung (Patch-Logs) | 7 Tage nach Zugang | **20.05.2026** | Offen |
| Klagefrist (falls keine Einigung) | Nach Fristablauf | Ab 27.05.2026 | Offen |
| Verjährungsfrist (§ 195 BGB) | 3 Jahre ab Jahresende 2026 | **31.12.2029** | Läuft |

3. Verfahrensfristen — DSGVO / Datenschutz

| Frist | Beschreibung | Termin | Status |
|------------------------------------|--------------------------------------|-----------------------|----------------|
| Vorlage DSFA an LfDI | DSFA BEM-Gesundheitsdaten | **22.05.2026** | In Bearbeitung |
| DSFA-Fertigstellung | Interne Fertigstellung | 22.05.2026 | In Bearbeitung |
| Umsetzung DSFA-Maßnahmen | Technik (Verschlüsselung, MFA, etc.) | 30.06.2026 | Geplant |
| Überprüfung DSFA | Nach Maßnahmen-Umsetzung | **30.09.2026** | Geplant |
| Folge-Meldung LfDI (Maßnahmenplan) | Auf Anforderung | TBD | Offen |

4. Verfahrensfristen — KI-Verordnung

| Frist | Beschreibung | Termin | Status |
|---|-------------------------------|-----------------------|---------------|
| Anforderung Konformitätsdokumentation DachAuge GmbH | Schreiben an DachAuge | **20.05.2026** | Offen |
| Entwurf Betriebsvereinbarung KI-Systeme | RA Drost erstellt Entwurf | **31.05.2026** | Offen |
| Unterzeichnung BV KI-Systeme (GF + BR) | Betriebsvereinbarung | **30.06.2026** | Offen |
| DSFA PalettenAuge AI (Art. 35 DSGVO) | DSB Feilke | **30.06.2026** | Offen |
| Human-Oversight-Prozess implementieren | IT/Disposition | **31.07.2026** | Offen |
| KI-VO Hochrisiko-Pflichten gelten ab | Art. 113 Abs. 2 KI-VO | **02.08.2026** | Fristgebunden |
| Registrierung EU-KI-Datenbank | Art. 71 KI-VO (über DachAuge) | **01.08.2026** | Offen |

5. Verfahrensfristen — Open Source Compliance

| Frist | Beschreibung | Termin | Status |
|--|-------------------|-----------------------|--------|
| Deaktivierung externe REST-API TourPlanner | Sofortmaßnahme | **20.05.2026** | Offen |
| Kontaktaufnahme ScheduleHero Foundation | Lizenzverhandlung | **20.05.2026** | Offen |

| Frist | Beschreibung | Termin | Status |
|---|------------------------------|-----------------------|--------|
| Ergebnis
Lizenzverhandlung | Einigung oder
Alternative | **20.06.2026** | Offen |
| Open-Source-Audit
gesamte
IT-Eigenentwicklungen | FOSSA/Black Duck | **30.06.2026** | Offen |

6. Verfahrensfristen — Strafverfahren

| Frist | Beschreibung | Termin | Status |
|--|--------------------------------|-----------------------|----------|
| Strafanzeige erstattet | ZAC Mainz (421 UJs
6611/26) | 07.05.2026 | Erledigt |
| Forensischer
Abschlussbericht | An ZAC übermitteln | **31.05.2026** | Offen |
| Kontakt ZAC:
Ermittlungsstand | Alle 4 Wochen
nachfragen | 04.06.2026 ff. | Geplant |
| Verjährungsfrist § 202a
StGB (Straftat) | 5 Jahre | 06.05.2031 | Läuft |

7. Interne Fristen und Maßnahmen

| Frist | Beschreibung | Termin | Zuständig |
|---|---|--------------------------|-----------------|
| Mitarbeiterversammlun
g Datensicherheit | BR + HR | **20.05.2026** | HR / BR |
| Unterlagen an
Betriebsrat | DSFA, Forensikbericht,
Maßnahmenplan | **18.05.2026** | GF Wallbruck |
| Hausbank-Gespräch
(Kreditlinie) | Liquiditätssicherung | **20.05.2026** | GF Wallbruck |
| Überarbeitung AVV
ProcessSpark und
InsoTec | Datenschutz-Vertragsa
npassung | **31.05.2026** | RA Drosten |
| Pressemitteilung
Veröffentlichung | Nach finalen Freigaben | **Ab 15.05.2026** | PR-Rhein / GF |
| Schadensdokumentatio
n vollständig
CyberCovered | Versicherungsunterlag
en | **31.05.2026** | RA Drosten + IT |
| Forensischer
Abschlussbericht | CyberForensik
RheinMain GmbH | **31.05.2026** | CyberForensik |

8. Kritische Pfad-Fristen (nicht verhandelbar)

Folgende Fristen dürfen unter keinen Umständen versäumt werden:

| # | Frist | Konsequenz bei Versäumnis |
|---|---|--|
| 1 | 22.05.2026 —
DSGVO-Ergänzungsmeldung LfDI | Erhöhtes Bußgeldrisiko nach Art. 83 DSGVO |
| 2 | 26.05.2026 — Reaktionsfrist
ProcessSpark | Klageerhebung am LG Mainz erforderlich |
| 3 | 07.06.2026 —
NIS2-Abschlussbericht BSI | Bußgeld § 34 NIS2UmsuG möglich |
| 4 | 02.08.2026 — KI-VO
Hochrisikopflichten | Bußgeld bis 15 Mio. EUR nach Art. 99 KI-VO |
| 5 | 31.12.2029 — Verjährung
ProcessSpark-Ansprüche | Ansprüche erlöschen |

9. Hinweis zu Fristenberechnung

Alle prozessualen Fristen folgen §§ 187, 188 BGB (keine Berücksichtigung des Anfangstages, Endtermin = letzter Tag). Art.-33-DSGVO-Frist beginnt mit Kenntnisnahme des Verantwortlichen (06.05.2026, 04:52 Uhr Wallbruck informiert), nicht mit bloßer IT-Detektion. Dies wurde in der Meldung korrekt berücksichtigt.

Stand: 13.05.2026 — Fortlaufende Aktualisierung durch Kanzlei Drosten & Pekonkur erforderlich.

E-Mails

Datei: eml/01_drosten_an_lfdi_rlp_art33.eml

| | |
|---------|--|
| Von | I.drosten@drosten-pekonkur.de |
| An | datenpanne@lfdi.rlp.de |
| Datum | Fri, 08 May 2026 22:45:00 +0200 |
| Betreff | Meldung gemäß Art. 33 DSGVO - Frischetrans Mittelrhein GmbH - Ransomware-Angriff
06.05.2026 |

Sehr geehrte Damen und Herren,

im Auftrag und in Vollmacht unserer Mandantin Frischetrans Mittelrhein GmbH, Binger Straße 142, 55131 Mainz, übermittle ich Ihnen die formelle Meldung einer Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 Abs. 3 DSGVO.

Referenz: LfDI-RLP-2026-0508-4419 (per Online-Meldeportal)

Zusammenfassung:

- Vorfall: Ransomware-Angriff (AkiraNext), 06.05.2026, 04:17 Uhr
- Angriffsvektor: CVE-2026-0712 (SAP NetWeaver, CVSS 9.8)
- Exfiltrierte Datenmenge: ca. 2,1 TB
- Betroffene Personen: 280 Mitarbeiter (davon 38 mit BEM-Gesundheitsdaten, Art. 9 DSGVO), 18 Geschäftskunden (Kontaktpersonen)
- Meldezeitpunkt: 08.05.2026, 22:45 Uhr (innerhalb der 72-h-Frist gem. Art. 33 Abs. 1 DSGVO)

Die vollständige Meldung wurde über das Online-Meldeportal des LfDI RLP eingereicht und trägt die Eingangsreferenz LfDI-RLP-2026-0508-4419. Als Anlage ist der Meldungsentwurf (entsprechend dem Aktenstück 05 der Akte) beigelegt.

Besonderer Hinweis zu BEM-Gesundheitsdaten:

Die exfiltrierten Daten umfassen Gesundheitsdaten (Diagnosen, Therapieverläufe, ärztliche Atteste) von 38 Beschäftigten aus BEM-Verfahren. Dies ist als hohes Risiko i.S.d. Art. 34 DSGVO eingestuft. Die betroffenen Mitarbeiter wurden am 11.05.2026 persönlich und vertraulich benachrichtigt. Eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO) ist eingeleitet; sie wird bis 22.05.2026 vorgelegt.

Rückfragen richte ich bitte an:

RA Lukas Drosten, Tel. +49 6131 2240-0, I.drosten@drosten-pekonkur.de

Mit freundlichen Grüßen

RA Lukas Drosten

Fachanwalt für IT-Recht

Kanzlei Drosten & Pekonkur

Schillerstraße 14, 55116 Mainz

Tel.: +49 6131 2240-0 | Fax: +49 6131 2240-99

kanzlei@drosten-pekonkur.de

Anlage: Meldungsformular (PDF) - übermittelt via Meldeportal

Datei: eml/02_drosten_an_processspark_klageandrohung.eml

| | |
|---------|--|
| Von | l.drosten@drosten-pekonkur.de |
| An | legal@processspark.de |
| Datum | Tue, 12 May 2026 14:22:00 +0200 |
| Betreff | Schadensersatz und Vertragsstrafe - IT-Betriebsvertrag - Ransomware-Schaden
CVE-2026-0712 - Frischetrans Mittelrhein GmbH |

EINSCHREIBEN / RÜCKSCHEIN (postalisch parallel versandt)

Sehr geehrte Damen und Herren,

wir sind anwaltliche Bevollmächtigte der Frischetrans Mittelrhein GmbH, Binger Straße 142, 55131 Mainz (nachfolgend "Mandantin"). Vollmacht liegt postalisch bei.

Wir machen hiermit Schadensersatz- und Vertragsstrafenansprüche aus dem IT-Betriebsvertrag vom 15.03.2021 (Nachtrag 3 vom 01.07.2024) geltend.

KURZER SACHVERHALT:

Am 06.05.2026 wurde unsere Mandantin durch einen Ransomware-Angriff (Gruppe AkiraNext) schwer geschädigt. Forensische Untersuchungen belegen: Angriffsvektor war CVE-2026-0712 (SAP NetWeaver AS ABAP, CVSS 9.8, Critical). Ihr Unternehmen spielte den verfügbaren Patch erst am 28./29.04.2026 ein - 55 Tage nach Ablauf der vertraglichen 14-Tage-Patchfrist für Critical-Schwachstellen (§ 12 Abs. 2 Nachtrag 3).

FORDERUNGEN:

1. Vertragsstrafe (§ 14 Abs. 3): EUR 518,00
2. Schadensersatz (§§ 280, 241 Abs. 2 BGB): EUR 681.300,00 (vorläufig)
3. Gesamtforderung: EUR 681.818,00

FRIST: 26.05.2026

Bei fruchtlosem Fristablauf wird Klage am Landgericht Mainz erhoben (geplantes AZ: 3 O 88/26). Die außerordentliche Kündigung des Vertrages aus wichtigem Grund (§ 626 BGB) bleibt vorbehalten.

Wir fordern Sie zusätzlich auf, alle Patch-Logs und internen Kommunikationen zu CVE-2026-0712 bis zum 20.05.2026 vorzulegen.

Das vollständige Klageandrohungsschreiben ist als Anlage beigefügt.

Mit freundlichen Grüßen

RA Lukas Drosten
Fachanwalt für IT-Recht
Kanzlei Drosten & Pekonkur, Mainz
Tel.: +49 6131 2240-0

Anlage: Klageandrohungsschreiben (PDF), Vollmacht Frischetrans GmbH (PDF)

Datei: eml/03_drosten_an_cybercovered_versicherungsmeldung.eml

| | |
|---------|---|
| Von | l.drosten@drosten-pekonkur.de |
| An | schaden-cyber@cybercovered.de |
| Datum | Thu, 07 May 2026 14:30:00 +0200 |
| Betreff | Schadensmeldung - Cyber-Police CC-2024-FTM-8801 - Ransomware-Angriff Frischetrans
Mittelrhein GmbH |

Sehr geehrte Damen und Herren,

im Auftrag unserer Mandantin Frischetrans Mittelrhein GmbH melde ich hiermit unverzüglich einen Versicherungsschaden gemäß Police Nr. CC-2024-FTM-8801.

VERSICHERUNGSNEHMERIN:

Frischetrans Mittelrhein GmbH
Binger Straße 142, 55131 Mainz
Geschäftsführerin: Theresia Wallbruck
Policennummer: CC-2024-FTM-8801

SCHADENEREIGNIS:

Art: Ransomware-Angriff (AkiraNext)
Entdeckungszeitpunkt: 06.05.2026, 04:17 Uhr (SOC InsoTec Systems GmbH)
Kenntnisnahme Versicherungsnehmerin: 06.05.2026, 04:52 Uhr

BETROFFENE SYSTEME:

- SAP S/4HANA ERP (vollständig verschlüsselt)
- Fileserver (3 Systeme)
- Telematik-Gateway (GPS/Temperatur-Tracking)

DATENABFLUSS: ca. 2,1 TB (Kunden- und Mitarbeiterdaten)

VORLÄUFIGE SCHADENSPOSITIONEN:

- IT-Wiederherstellung: ca. 200.000-270.000 EUR
 - Betriebsunterbrechung: ca. 350.000-500.000 EUR
 - Forensik: ca. 45.000-65.000 EUR
 - Rechtskosten: ca. 80.000-120.000 EUR
- Gesamt (vorläufig): ca. 675.000-955.000 EUR

LÖSEGELD: Kein Lösegeld wurde gezahlt oder ist geplant.

Ich bitte um:

1. Bestätigung des Schadenseingangs und Vergabe einer Schadensnummer
2. Benennung des zuständigen Schadenmanagers / der zuständigen Schadenmanagerin
3. Freigabe der Beauftragung: CyberForensik RheinMain GmbH (bereits informiert)

Für Rückfragen stehe ich jederzeit zur Verfügung.

Mit freundlichen Grüßen

RA Lukas Drosten
Kanzlei Drosten & Pekonkur, Mainz
Tel.: +49 6131 2240-0 (auch außerhalb der Geschäftszeiten erreichbar)

Datei: eml/04_wallbruck_an_drosten_erstmeldung.eml

| | |
|---------|---|
| Von | t.wallbruck@frischetrans-mittelrhein.de |
| An | l.drosten@drosten-pekonkur.de |
| Datum | Wed, 06 May 2026 07:15:00 +0200 |
| Betreff | DRINGEND - Cyberangriff auf Frischetrans - Sororthilfe benötigt |

Herr Drosten,

ich versuche Sie seit ca. 7 Uhr zu erreichen. Wir haben einen ernsthaften IT-Notfall.

In der Nacht um ca. 4:17 Uhr wurden wir von Ransomware angegriffen. Die gesamte SAP-Anlage ist verschlüsselt, der Telematik ist ausgefallen, 47 von 64 LKW sind "blind". Auf allen betroffenen

Bildschirmen steht eine Lösegeldforderung: 1.450.000 USD in einer Kryptowährung (Monero).

Ich bin seit 5 Uhr im Betrieb. InsoTec (unser IT-Dienstleister) ist informiert und hat bereits alles vom Netz genommen. Aber ich brauche jetzt rechtliche Beratung - sofort.

Was ich bisher weiß:

- Es wurden Daten gestohlen - ca. 2,1 TB laut den ersten IT-Befunden
- Darunter Personalakten ALLER Mitarbeiter
- Es gibt auch BEM-Akten darin (Gesundheitsdaten)
- Kundendaten von 18 Kunden - Frischbäcker AG ruft schon an
- Die Erpresser drohen mit Veröffentlichung der Daten

Ich weiß, es gibt Meldepflichten. Datenschutz, BSI, irgendwas mit 72 Stunden? Ich weiß nicht wo ich anfangen soll.

Können wir uns um 8:30 Uhr in Ihrer Kanzlei treffen?

Bitte rufen Sie mich sofort an: +49 173 4422881

Mit freundlichen Grüßen

Theresia Wallbruck

Geschäftsführerin

Frischetrans Mittelrhein GmbH

Tel. Büro: +49 6131 8820-100

Tel. mobil: +49 173 4422881

P.S.: Ich habe die Versicherungspolice (CyberCovered AG) gefunden. Policennummer CC-2024-FTM-8801. Kann ich die schon informieren?

Excel-Tabellen

Datei: xlsx/betroffenenverzeichnis_anonymisiert.xlsx

Tabellenblatt: Betroffenverzeichnis

| | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|
| BETROFFENVERZEICHNIS — DATENP ANNE FRISCHE TRANS MITTEL RHEIN GMBH | | | | | | | | | |
| Vorfall: Ransomware AkiraNext · Datum: 06.05.2026 · Dokument: Anonymisiert (DSGVO-konform) · Stand: 13.05.2026 | | | | | | | | | |

| | | | | | | | | | |
|--|---|-----------------------|--------------|---|--------------------------------|--------------|--------------------------|---------------------------|----------------------------------|
| | <p>■</p> <p>STRENG
VERTRAULICH —
Zugang
nur für:
GF, HR-L
eitung,
DSB, an
waltliche
Beratung
 Enthält
anonymis
ierte pers
onenbez
ogene
Daten
gemäß
Art. 4 Nr.
5
DSGVO (Pseu
donymisierun
g)</p> | | | | | | | | |
| | Person-ID | Pseudonym
(intern) | Abteilung | Betroffene Datenkategorien | Art. 9 DSGVO (Sonderkategorie) | Risikoklasse | Art.-34-Meldung erhalten | BEM-Akt
e
betroffen | Status Monitoring |
| | MA-0001 | Person-0001 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 11.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0002 | Person-0002 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 11.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|-------------|---|-----------------------|------|--------------------|----|----------------------------------|
| | MA-0003 | Person-0003 | Fahrtteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0004 | Person-0004 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0005 | Person-0005 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0006 | Person-0006 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0007 | Person-0007 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|------------|--------------|---|-----------------------|------|--------------------|----|----------------------------------|
| | MA-0008 | Person-008 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0009 | Person-009 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0010 | Person-010 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0011 | Person-011 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0012 | Person-012 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|-------------|---|-----------------------|------|--------------------|----|----------------------------------|
| | MA-0013 | Person-0013 | Fahrtteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0014 | Person-0014 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0015 | Person-0015 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0016 | Person-0016 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0017 | Person-0017 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|-----------------------|------|--------------------|----|----------------------------------|
| | MA-0018 | Person-0018 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0019 | Person-0019 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0020 | Person-0020 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0021 | Person-0021 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0022 | Person-0022 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|-------------|---|-----------------------|------|--------------------|----|----------------------------------|
| | MA-0023 | Person-0023 | Fahrtteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0024 | Person-0024 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0025 | Person-0025 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0026 | Person-0026 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0027 | Person-0027 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|-----------------------|------|--------------------|----|----------------------------------|
| | MA-0028 | Person-0028 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0029 | Person-0029 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0030 | Person-0030 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0031 | Person-0031 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0032 | Person-0032 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|-------------|---|-----------------------|------|--------------------|----|----------------------------------|
| | MA-0033 | Person-0033 | Fahrtteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0034 | Person-0034 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0035 | Person-0035 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0036 | Person-0036 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0037 | Person-0037 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|-----------------------|--------|--------------------|------|----------------------------------|
| | MA-0038 | Person-0038 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten, Gesundheitsdaten (BEM) | Ja — Gesundheitsdaten | HOCH | Erledigt 1.05.2026 | Ja | Benachrichtigt, Monitoring aktiv |
| | MA-0039 | Person-0039 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0040 | Person-0040 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0041 | Person-0041 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0042 | Person-0042 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0043 | Person-0043 | Fahrerteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0044 | Person-0044 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0045 | Person-0045 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0046 | Person-0046 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0047 | Person-0047 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0048 | Person-0048 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0049 | Person-0049 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0050 | Person-0050 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0051 | Person-0051 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0052 | Person-0052 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|-------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0053 | Person-0053 | Fahrtteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0054 | Person-0054 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0055 | Person-0055 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0056 | Person-0056 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0057 | Person-0057 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0058 | Person-0058 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0059 | Person-0059 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0060 | Person-0060 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0061 | Person-0061 | FahrerTEAM A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0062 | Person-0062 | FahrerTEAM B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0063 | Person-0063 | FahrerTEAM C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0064 | Person-0064 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0065 | Person-0065 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0066 | Person-0066 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0067 | Person-0067 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0068 | Person-0068 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0069 | Person-0069 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0070 | Person-0070 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0071 | Person-0071 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0072 | Person-0072 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0073 | Person-0073 | Fahrerteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0074 | Person-0074 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0075 | Person-0075 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0076 | Person-0076 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0077 | Person-0077 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0078 | Person-0078 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0079 | Person-0079 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0080 | Person-0080 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0081 | Person-0081 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0082 | Person-0082 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0083 | Person-0083 | Fahrerteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0084 | Person-0084 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0085 | Person-0085 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0086 | Person-0086 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0087 | Person-0087 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0088 | Person-0088 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0089 | Person-0089 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0090 | Person-0090 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0091 | Person-0091 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0092 | Person-0092 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|-------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0093 | Person-0093 | Fahrtteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0094 | Person-0094 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0095 | Person-0095 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0096 | Person-0096 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0097 | Person-0097 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0098 | Person-0098 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0099 | Person-0099 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0100 | Person-0100 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0101 | Person-0101 | FahrerTEAM A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0102 | Person-0102 | FahrerTEAM B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0103 | Person-0103 | FahrerTEAM C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0104 | Person-0104 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0105 | Person-0105 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0106 | Person-0106 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0107 | Person-0107 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0108 | Person-0108 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0109 | Person-0109 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0110 | Person-0110 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0111 | Person-0111 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0112 | Person-0112 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0113 | Person-0113 | Fahrerteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0114 | Person-0114 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0115 | Person-0115 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0116 | Person-0116 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0117 | Person-0117 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0118 | Person-0118 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0119 | Person-0119 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0120 | Person-0120 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0121 | Person-0121 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0122 | Person-0122 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0123 | Person-0123 | Fahrerteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0124 | Person-0124 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0125 | Person-0125 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0126 | Person-0126 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0127 | Person-0127 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0128 | Person-0128 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0129 | Person-0129 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0130 | Person-0130 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0131 | Person-0131 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0132 | Person-0132 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|-------------|--|------|--------|--------------------|------|----------------------------------|
| | MA-0133 | Person-0133 | Fahrtteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohn Daten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0134 | Person-0134 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohn Daten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0135 | Person-0135 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohn Daten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0136 | Person-0136 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohn Daten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0137 | Person-0137 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohn Daten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0138 | Person-0138 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohn Daten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0139 | Person-0139 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohn Daten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0140 | Person-0140 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohn Daten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0141 | Person-0141 | FahrerTEAM A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0142 | Person-0142 | FahrerTEAM B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0143 | Person-0143 | FahrerTEAM C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0144 | Person-0144 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0145 | Person-0145 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0146 | Person-0146 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0147 | Person-0147 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0148 | Person-0148 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0149 | Person-0149 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0150 | Person-0150 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0151 | Person-0151 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0152 | Person-0152 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0153 | Person-0153 | Fahrerteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0154 | Person-0154 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0155 | Person-0155 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0156 | Person-0156 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0157 | Person-0157 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0158 | Person-0158 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0159 | Person-0159 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0160 | Person-0160 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0161 | Person-0161 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0162 | Person-0162 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0163 | Person-0163 | Fahrerteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0164 | Person-0164 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0165 | Person-0165 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0166 | Person-0166 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0167 | Person-0167 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0168 | Person-0168 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0169 | Person-0169 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0170 | Person-0170 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0171 | Person-0171 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0172 | Person-0172 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|-------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0173 | Person-0173 | Fahrtteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0174 | Person-0174 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0175 | Person-0175 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0176 | Person-0176 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0177 | Person-0177 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0178 | Person-0178 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0179 | Person-0179 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0180 | Person-0180 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0181 | Person-0181 | FahrerTEAM A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0182 | Person-0182 | FahrerTEAM B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0183 | Person-0183 | FahrerTEAM C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0184 | Person-0184 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0185 | Person-0185 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0186 | Person-0186 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0187 | Person-0187 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0188 | Person-0188 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0189 | Person-0189 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0190 | Person-0190 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0191 | Person-0191 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0192 | Person-0192 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0193 | Person-0193 | Fahrerteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0194 | Person-0194 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0195 | Person-0195 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0196 | Person-0196 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0197 | Person-0197 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0198 | Person-0198 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0199 | Person-0199 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0200 | Person-0200 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0201 | Person-0201 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0202 | Person-0202 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0203 | Person-0203 | Fahrerteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0204 | Person-0204 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0205 | Person-0205 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0206 | Person-0206 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0207 | Person-0207 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0208 | Person-0208 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0209 | Person-0209 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0210 | Person-0210 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0211 | Person-0211 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0212 | Person-0212 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|-------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0213 | Person-0213 | Fahrtteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0214 | Person-0214 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0215 | Person-0215 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0216 | Person-0216 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0217 | Person-0217 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0218 | Person-0218 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0219 | Person-0219 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0220 | Person-0220 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0221 | Person-0221 | FahrerTEAM A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0222 | Person-0222 | FahrerTEAM B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0223 | Person-0223 | FahrerTEAM C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0224 | Person-0224 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0225 | Person-0225 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0226 | Person-0226 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0227 | Person-0227 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0228 | Person-0228 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0229 | Person-0229 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0230 | Person-0230 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0231 | Person-0231 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0232 | Person-0232 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0233 | Person-0233 | Fahrerteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0234 | Person-0234 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0235 | Person-0235 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0236 | Person-0236 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0237 | Person-0237 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0238 | Person-0238 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0239 | Person-0239 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0240 | Person-0240 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0241 | Person-0241 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0242 | Person-0242 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0243 | Person-0243 | Fahrerteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0244 | Person-0244 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0245 | Person-0245 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0246 | Person-0246 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0247 | Person-0247 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0248 | Person-0248 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0249 | Person-0249 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0250 | Person-0250 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0251 | Person-0251 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0252 | Person-0252 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|-------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0253 | Person-0253 | Fahrtteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0254 | Person-0254 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0255 | Person-0255 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0256 | Person-0256 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0257 | Person-0257 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0258 | Person-0258 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0259 | Person-0259 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0260 | Person-0260 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0261 | Person-0261 | FahrerTEAM A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0262 | Person-0262 | FahrerTEAM B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0263 | Person-0263 | FahrerTEAM C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0264 | Person-0264 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0265 | Person-0265 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0266 | Person-0266 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0267 | Person-0267 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0268 | Person-0268 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|---------|-------------|--------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0269 | Person-0269 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0270 | Person-0270 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0271 | Person-0271 | Fahrerteam A | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0272 | Person-0272 | Fahrerteam B | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0273 | Person-0273 | Fahrerteam C | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0274 | Person-0274 | Disposition | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0275 | Person-0275 | Verwaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0276 | Person-0276 | Werkstatt | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |

| | | | | | | | | | |
|--|--|-------------|-------------|---|------|--------|--------------------|------|----------------------------------|
| | MA-0277 | Person-0277 | HR | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0278 | Person-0278 | IT | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0279 | Person-0279 | Buchhaltung | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | MA-0280 | Person-0280 | Logistik | Personalstammdaten, Bankverbindung, SV-Nr., Lohndaten | Nein | MITTEL | Erledigt 1.05.2026 | Nein | Benachrichtigt, Monitoring aktiv |
| | GESAMT : 280 betroffene Personen davon mit Art.-9-Gesundheitsdaten (BEM): 38 Risikoklasse HOCH: 38 | | | | | | | | |

Datei: xlsx/sla_schaden_berechnung.xlsx

Tabellenblatt: SLA-Schaden-Berechnung

| | | | | | | |
|--|--|--|--|--|--|--|
| | SLA-SCHADENSBERECHNUNG — FRISCHETRANS vs. PROCESS SPARK CLOUD AG | | | | | |
|--|--|--|--|--|--|--|

| | | | | | | |
|--|--|--------------------|--|--|--|--|
| | Aktenzeichen
(geplant): 3 O
88/26 · LG
Mainz · CVE-2
026-0712 · SL
A-Verletzung
ProcessSpark
Cloud AG ·
Stand:
13.05.2026 | | | | | |
| | 1. PATCH-VE
RZUG DOKU
MENTATION (
CVE-2026-07
12) | | | | | |
| | Parameter | Wert / Datum | | | | |
| | SAP Security
Note
veröffentlicht | 18.02.2026 | | | | |
| | CVSS Base
Score | 9.8 (Critical) | | | | |
| | Vertragl.
Patch-Frist
(14 Tage für
Critical) | 04.03.2026 | | | | |
| | Tatsächliche
Patch-Einspiel
ung durch
ProcessSpark | 28./29.04.202
6 | | | | |
| | Verzug
gegenüber
vertraglicher
Frist (Tage) | 55 | | | | |
| | Anzahl übersc
hrittener 7-Ta
ge-Perioden
(für Pönale) | 7 | | | | |
| | Monatliche SL
A-Vergütung
ProcessSpark
(EUR) | 74 | | | | |
| | Pönale pro 7-
Tage-Periode
(0,5 % der Mo
natsvergütung
) | 518 | | | | |
| | Vertragsstrafe
gesamt (7 ×
Einzel-Pönale) | | | | | |
| | 2. BETRIEBS
UNTERBREC
HUNGSSCHA
DEN (D+0 bis
D+7) | | | | | |

| | Zeitraum | ERP-Status | Telematik-Stat
us | LKW
verfügbar | Ausfall-Stunde
n | Tagessatz-Ver
lust (EUR) |
|--|--|--|------------------------------|----------------------|---------------------|--|
| | D+0
(06.05.2026) | Totalausfall | Totalausfall
(47/64 LKW) | 17 | 24 | 67200 |
| | D+1
(07.05.2026) | Totalausfall | Totalausfall
(47/64 LKW) | 17 | 24 | 67200 |
| | D+2
(08.05.2026) | Totalausfall | Teilausfall
(40/64 LKW) | 24 | 24 | 54100 |
| | D+3
(09.05.2026) | ~20% wiederh
ergestellt | Teilausfall
(35/64 LKW) | 29 | 24 | 41200 |
| | D+4
(10.05.2026) | ~40% wiederh
ergestellt | Teilausfall
(35/64 LKW) | 29 | 24 | 28600 |
| | D+5
(11.05.2026) | ~60% wiederh
ergestellt | Weitgehend
stabil (55/64) | 55 | 24 | 18500 |
| | D+6
(12.05.2026) | ~70% wiederh
ergestellt | Stabil (58/64) | 58 | 24 | 11400 |
| | D+7
(13.05.2026) | ~80% wiederh
ergestellt | Stabil (60/64) | 60 | 24 | 8800 |
| | SUMME Betri
ebsausfallsch
aden | | | | 192 | 297000 |
| | 3. WEITERE
SCHADENPO
SITIONEN (R
egressforderu
ng an Process
Spark) | | | | | |
| | Schadensposi
tion | Beschreibung | Betrag min.
(EUR) | Betrag max.
(EUR) | Angesetzt
(EUR) | Nachweis |
| | IT-Wiederhersh
tellungskosten | Forensik, Syst
emwiederaufb
au,
Konfiguration | 180000 | 230000 | 198500 | Rechnung
CyberForensik
/ Lieferanten |
| | Forensikkoste
n (CyberForen
sik
RheinMain) | Forensische
Analyse und A
bschlussberic
ht | 45000 | 65000 | 52800 | Kostenvorans
schlag CRM-20
26-FT-01 |
| | Anwaltskosten
(bisherig) | RA Drosten,
Kanzlei
Drosten &
Pekonkur | 20000 | 30000 | 24800 | Honorarrechn
ung DR-2026-
FTM-001 |
| | DSGVO-Folge
kosten | DSB, DSFA,
Meldungen, M
itarbeiter-Kom
munikation | 15000 | 22000 | 18000 | DSB-Honorar,
Portokosten |
| | Betriebsunterb
rechnungsscha
den | Ertragsausfall
D+0 bis D+7
(Spalte oben) | 297000 | 500000 | 387200 | Controlling-Au
swertung FT-
BU-2026-05 |
| | SUMME Scha
denpositionen
(ohne Betriebs
ausfall) | | 260000 | 347000 | 294100 | |

| | | | | | | |
|--|--|--|--|--|--|--------|
| | 4. GESAMTF
ORDERUNG
AN PROCES
SSPARK
CLOUD AG | | | | | |
| | Vertragsstrafe
(§ 14 Abs. 3
Vertrag) | | | | | 518 |
| | Betriebsunterb
rechnungsscha
den | | | | | 387200 |
| | IT-Wiederhersh
tellungskosten | | | | | 198500 |
| | Forensikkoste
n | | | | | 52800 |
| | Anwaltskosten
(bisherig) | | | | | 24800 |
| | DSGVO-Folge
kosten | | | | | 18000 |
| | GESAMTFOR
DERUNG
(vorläufig,
vorbehaltlich
forensischem
Abschlussberi
cht) | | | | | 681818 |
| | Hinweis: Alle
Beträge netto
zzgl. USt.,
soweit
anwendbar. S
chadensnach
weis durch
Rechnungen,
Buchungsbele
ge und
forensischen
Abschlussberi
cht.
Verjährung:
31.12.2029 (§
195 BGB).
Gerichtsstand:
LG Mainz (§
18 Vertrag). | | | | | |

Word-Dokumente

Datei: docx/dsfa_bericht_bem_gesundheitsdaten.docx

DATENSCHUTZ-FOLGENABSCHÄTZUNG

gemäß Art. 35 DSGVO

BEM-Gesundheitsdaten im Kontext des Ransomware-Vorfalls

1. Anlass und Gegenstand der DSFA

Der Ransomware-Angriff vom 06.05.2026 auf die Frischetrans Mittelrhein GmbH hat zur Exfiltration von ca. 2,1 TB Unternehmensdaten geführt. Darunter befinden sich Gesundheitsdaten im Sinne des Art. 9 Abs. 1 DSGVO von 38 Beschäftigten aus laufenden oder abgeschlossenen BEM-Verfahren (Betriebliches Eingliederungsmanagement, § 167 Abs. 2 SGB IX).

Die vorliegende DSFA wurde durch den LfDI Rheinland-Pfalz im Schreiben vom 09.05.2026 angefordert und von der Frischetrans gemäß Art. 35 DSGVO durchgeführt. Gesundheitsdaten im Beschäftigungskontext erfordern nach Art. 35 Abs. 3 lit. b) DSGVO grundsätzlich eine vorherige DSFA.

2. Beschreibung der Verarbeitungstätigkeit

Zweck:

Betriebliches Eingliederungsmanagement (BEM) nach § 167 Abs. 2 SGB IX für Beschäftigte mit mehr als 6 Wochen Arbeitsunfähigkeit innerhalb eines Jahres. Zweck: Wiedereingliederung und Prävention weiterer Ausfallzeiten.

Rechtsgrundlagen:

Art. 9 Abs. 2 lit. b) DSGVO i.V.m. § 26 Abs. 3 BDSG; § 167 Abs. 2 SGB IX.

Verarbeitete Datenkategorien (Art. 9 DSGVO):

3. Notwendigkeit und Verhältnismäßigkeit

Die Verarbeitung von BEM-Gesundheitsdaten ist nach § 167 Abs. 2 SGB IX und Art. 9 Abs. 2 lit. b) DSGVO i.V.m. § 26 Abs. 3 BDSG rechtlich erforderlich. Die Datenerhebung ist auf den für das BEM-Verfahren notwendigen Umfang beschränkt. Eine Einwilligung der betroffenen Mitarbeiter wurde eingeholt.

4. Risiken für Rechte und Freiheiten der Betroffenen

Aufgrund des erfolgten Datenabflusses durch den Ransomware-Angriff sind folgende Risiken für die 38 betroffenen Mitarbeiter als hoch einzustufen:

HOCH: Veröffentlichung der Gesundheitsdaten durch AkiraNext (Leaksite-Drohung aktiv). Folgen: Soziale Stigmatisierung, potenzielle Auswirkungen auf Versicherbarkeit und Kreditwürdigkeit, psychische Belastung, Diskriminierung bei künftigen Bewerbungen.

HOCH: Missbrauch durch Dritte (Identitätsbetrug, Erpressung betroffener Mitarbeiter).

MITTEL: Verlust des Vertrauens in den Arbeitgeber und in das BEM-Instrument (mittel- bis langfristig).

5. Geplante Abhilfemaßnahmen

6. Konsultation der Aufsichtsbehörde (Art. 36 DSGVO)

Aufgrund des hohen Restrisikos (Gesundheitsdaten exfiltriert, Veröffentlichungsdrohung aktiv) wird eine vorherige Konsultation des LfDI Rheinland-Pfalz gemäß Art. 36 DSGVO durchgeführt. Diese DSFA wird dem LfDI als Ergänzung zur Meldung vom 08.05.2026 übermittelt.

7. Ergebnis

Die DSFA ergibt, dass die Verarbeitung von BEM-Gesundheitsdaten ohne die beschriebenen Abhilfemaßnahmen ein HOHES Restrisiko für die Rechte und Freiheiten der betroffenen Mitarbeiter darstellt. Die geplanten Maßnahmen sollen das Restrisiko auf ein akzeptables Niveau senken. Eine Überprüfung der DSFA erfolgt nach Abschluss der Maßnahmen (voraussichtlich Herbst 2026).

| | |
|--------------------------|---|
| Verantwortlicher: | Frischetrans Mittelrhein GmbH, Binger Straße 142, 55131 Mainz |
| Vertreten durch: | Theresia Wallbruck (Geschäftsführerin) |
| Datenschutzbeauftragter: | Markus Feilke, Datenschutzkanzlei Rhein-Main |
| Rechtliche Beratung: | RA Lukas Drosten, Kanzlei Drosten & Pekonkur, Mainz |
| Erstellt am: | 14.05.2026 |
| Status: | Finale Version — vorgelegt an LfDI RLP |
| Rechtsgrundlagen: | Art. 35 DSGVO, § 67 SGB IX, § 26 Abs. 3 BDSG |

| Datenkategorie | Anzahl Betroffene |
|--|-------------------|
| Diagnosen und Erkrankungen | 38 |
| Therapieverläufe und Behandlungsberichte | 38 |
| Ärztliche Atteste und Gutachten | 38 |
| Betriebsärztliche Bewertungen | 38 |
| Rehabilitationsmaßnahmen | 22 |
| Gesundheitsdaten gesamt (Betroffene) | 38 Mitarbeiter |

| Maßnahme | Frist | Zuständig |
|--|------------|-------------------|
| Verschlüsselung HR-Daten at rest (AES-256) | 30.06.2026 | IT / InsoTec |
| MFA für alle HR-Systemzugänge | 15.06.2026 | IT / InsoTec |
| Zero-Trust-Netzwerksegmentierung HR | 31.08.2026 | IT / InsoTec |
| Neues Patch-Management-Konzept (SLA) | 30.06.2026 | ProcessSpark / IT |
| Data Loss Prevention (DLP) Implementierung | 31.07.2026 | IT |

| | | |
|---|---|---|
| Theresia Wallbruck
Geschäftsführerin, Verantwortlicher
i.S.d. DSGVO Frischetrans
Mittelrhein GmbH Mainz,
14.05.2026 | Markus Feilke Externer
Datenschutzbeauftragter
Datenschutzkanzlei Rhein-Main
Mainz, 14.05.2026 | RA Lukas Drosten Fachanwalt für
IT-Recht Kanzlei Drosten &
Pekonkur Mainz, 14.05.2026 |
|---|---|---|

Datei: docx/klageandrohung_processspark.docx

KANZLEI DROSTEN & PEKONKUR

Rechtsanwälte und Fachanwälte · Schillerstraße 14 · 55116 Mainz

Tel. +49 6131 2240-0 · Fax +49 6131 2240-99 · l.drosten@drosten-pekonkur.de

Per Einschreiben mit Rückschein

ProcessSpark Cloud AG

— Rechtsabteilung / Vorstand —

Leopoldstraße 88

80802 München

Mainz, den 12.05.2026

Schadensersatz und Vertragsstrafe — IT-Betriebsvertrag 15.03.2021 / Nachtrag 3 —
Ransomware-Schaden durch Patchpflichtverletzung CVE-2026-0712

Unsere Mandantin: Frischetrans Mittelrhein GmbH, Binger Straße 142, 55131 Mainz

Sehr geehrte Damen und Herren,

wir sind anwaltliche Bevollmächtigte der Frischetrans Mittelrhein GmbH. Vollmacht liegt bei. Wir wenden uns an Sie wegen schwerwiegender Pflichtverletzungen aus dem zwischen den Parteien bestehenden IT-Betriebsvertrag vom 15.03.2021 (Nachtrag 3 vom 01.07.2024), die zu einem erheblichen Schaden für unsere Mandantin geführt haben.

I. Sachverhalt

Unsere Mandantin wurde in der Nacht vom 05. auf den 06.05.2026 Opfer eines schwerwiegenden Ransomware-Angriffs der kriminellen Gruppe „AkiraNext“. Das ERP-System (SAP S/4HANA), Fileserver und Telematik-Schnittstellen wurden vollständig verschlüsselt und ca. 2,1 TB Daten exfiltriert.

Die forensische Untersuchung (CyberForensik RheinMain GmbH, Bericht-ID CRM-2026-FT-01) hat ergeben, dass der Angriffsvektor die Sicherheitslücke CVE-2026-0712 (SAP NetWeaver AS ABAP, CVSS 9.8 Critical) war. SAP SE stellte den Patch am 18.02.2026 bereit.

Ihre Gesellschaft spielte diesen Patch erst in der Nacht vom 28. auf den 29.04.2026 ein — 69 Tage nach Bereitstellung und 55 Tage nach Ablauf der vertraglichen 14-Tage-Frist für Critical-Patches (§ 12 Abs. 2 Nachtrag 3).

II. Pflichtverletzungen

1. Verletzung der Patchpflicht (§ 12 Abs. 2 Nachtrag 3)
2. Verletzung der Informationspflicht (§ 241 Abs. 2 BGB)

Ihre Gesellschaft hat unsere Mandantin zu keinem Zeitpunkt über die Schwachstelle, den Patch-Rückstand oder mögliche Schutzmaßnahmen informiert.

III. Schaden

IV. Forderungen

Wir machen folgende Ansprüche geltend:

V. Frist

Wir fordern Sie auf, den Gesamtbetrag von EUR 681.818,00 bis spätestens

Montag, den 26.05.2026

auf das Konto unserer Mandantin zu überweisen sowie die angeforderten Patch-Logs (7-Tage-Frist bis 20.05.2026) vorzulegen. Bei fruchtlosem Fristablauf wird Klage am Landgericht Mainz erhoben (geplantes AZ: 3 O 88/26). Die außerordentliche Kündigung des Vertrages bleibt vorbehalten (§ 626 BGB).

Mit freundlichen Grüßen

RA Lukas Drosten

Fachanwalt für IT-Recht

Kanzlei Drosten & Pekonkur, Mainz

Anlage: Vollmacht der Frischetrans Mittelrhein GmbH

| | |
|---|----------------|
| Patch-Veröffentlichung SAP SE: | 18.02.2026 |
| CVSS-Score: | 9.8 (Critical) |
| Vertragliche Frist (14 Tage): | 04.03.2026 |
| Tatsächliche Einspielung: | 28./29.04.2026 |
| Verzug: | 55 Tage |
| Ausnahmegenehmigung beantragt: | Nein |
| IT-Wiederherstellungskosten | 198.500,00 EUR |
| Betriebsausfall Logistik (7 Tage) | 387.200,00 EUR |
| Forensikkosten (CyberForensik RheinMain GmbH) | 52.800,00 EUR |
| Anwaltskosten (bisherig) | 24.800,00 EUR |
| DSGVO-Folgekosten | 18.000,00 EUR |
| Gesamtschaden (vorläufig) | 681.300,00 EUR |
| Vertragsstrafe (§ 14 Abs. 3 Vertrag, $7 \times 0,5 \% \times 14.800$ EUR) | 518,00 EUR |
| Schadensersatz (§§ 280, 241 Abs. 2 BGB, vorläufig) | 681.300,00 EUR |
| Gesamtforderung | 681.818,00 EUR |

Datei: docx/ldi_meldung_art33_dsgvo.docx

KANZLEI DROSTEN & PEKONKUR

Rechtsanwälte und Fachanwälte · Schillerstraße 14 · 55116 Mainz

Telefon: +49 6131 2240-0 · E-Mail: kanzlei@drosten-pekonkur.de

An den

Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

Hintere Bleiche 34

55116 Mainz

Mainz, den 08.05.2026

Meldung einer Verletzung des Schutzes personenbezogener Daten

gemäß Art. 33 Abs. 3 DSGVO

1. Verantwortlicher

2. Art der Verletzung

In der Nacht vom 05. auf den 06.05.2026 wurde das IT-System der Frischetrans Mittelrhein GmbH Opfer eines Ransomware-Angriffs durch die kriminelle Gruppe „AkiraNext“. Das ERP-System (SAP S/4HANA, on-premises) sowie weitere interne IT-Systeme wurden vollständig verschlüsselt.

Forensische Analyse ergab, dass die Angreifer bereits ab dem 04.05.2026 (ca. 22:44 Uhr) Zugang zu den Systemen hatten und vor der Aktivierung der Ransomware ca. 2,1 TB an Unternehmensdaten exfiltriert

haben. Der initiale Zugang erfolgte über die ungepatchte SAP-Schwachstelle CVE-2026-0712 (CVSS 9.8, Critical).

3. Betroffene Personen und Datenkategorien

Von der Datenverletzung sind folgende Personengruppen und Datenkategorien betroffen:

Mitarbeiterinnen und Mitarbeiter (280 Personen):

Personalstammdaten (Name, Adresse, Geburtsdatum, SV-Nummer, Bankverbindung, Lohnabrechnung).
Bei 38 Mitarbeitern zusätzlich: Gesundheitsdaten aus BEM-Verfahren (Diagnosen, Therapieverläufe, ärztliche Bescheinigungen) – besondere Kategorie gemäß Art. 9 DSGVO.

Geschäftskunden (18 Unternehmen):

Kundenstammdaten, Kontaktdaten natürlicher Ansprechpersonen, Vertragsdaten, Konditionsdaten, Lieferdaten.

4. Voraussichtliche Folgen

Die Verletzung hat voraussichtlich folgende Folgen für die betroffenen Personen: erhöhtes Risiko von Identitätsdiebstahl und Finanzbetrug (Bankdaten); Gefahr der Bloßstellung und Diskriminierung durch Veröffentlichung der Gesundheitsdaten der 38 BEM-Betroffenen; mögliche geschäftliche Nachteile für betroffene Kunden durch Offenlegung von Konditionsdaten.

5. Getroffene Maßnahmen

Sofortige Abschottung aller betroffenen Systeme (Network Kill, 06.05.2026, 05:35 Uhr); Beauftragung forensischer Spezialisten (CyberForensik RheinMain GmbH); Strafanzeige bei ZAC Mainz (421 UJs 6611/26, 07.05.2026); Meldung an BSI Außenstelle Frankfurt (07.05.2026, Ref. BSI-REF-2026-1847); Benachrichtigung betroffener Mitarbeiter nach Art. 34 DSGVO (11.05.2026); Einleitung DSFA für BEM-Gesundheitsdaten (Art. 35 DSGVO).

6. Ergänzungsmeldung

Diese Meldung basiert auf den zum 08.05.2026 vorliegenden Erkenntnissen. Die forensische Untersuchung ist noch nicht abgeschlossen. Eine Ergänzungsmeldung mit vollständigen Befunden wird bis 22.05.2026 eingereicht (Art. 33 Abs. 4 DSGVO).

Mit freundlichen Grüßen

RA Lukas Drost

Fachanwalt für IT-Recht

Kanzlei Drost & Pekonkur, Mainz

(handelnd für und im Auftrag der Frischetrans Mittelrhein GmbH)

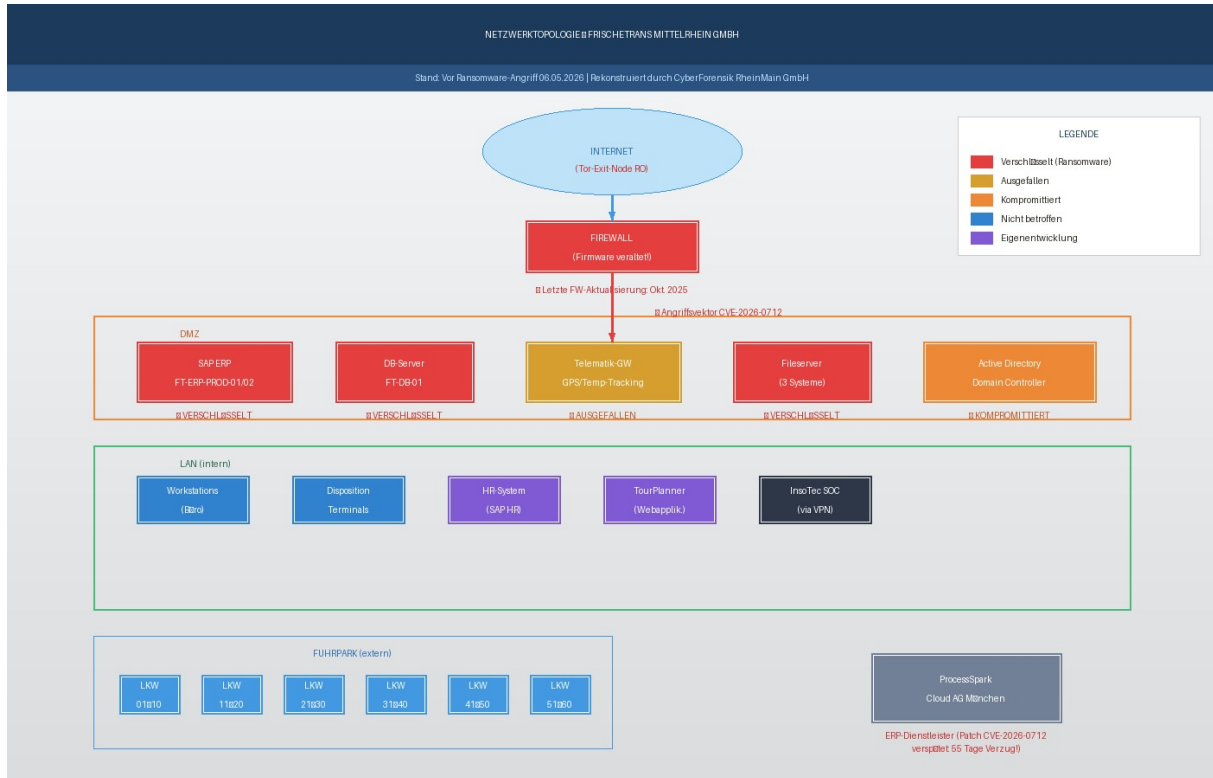
Referenznummer LfDI: LfDI-RLP-2026-0508-4419 | Elektronisch übermittelt am 08.05.2026, 22:45 Uhr

| | |
|-------------------------|--|
| Firmenbezeichnung: | Frischetrans Mittelrhein GmbH |
| Vertreten durch: | Theresia Wallbruck (Geschäftsführerin) |
| Anschrift: | Binger Straße 142, 55131 Mainz |
| Handelsregister: | HRB 44821, Amtsgericht Mainz |
| Anwaltlicher Vertreter: | RA Lukas Drost, Kanzlei Drost & Pekonkur, Schillerstraße 14, 55116 Mainz |
| DSB (extern): | Markus Feilke, Datenschutzkanzlei Rhein-Main, Tel. +49 6131 9944-11 |

| | |
|--|---|
| Zeitpunkt Entdeckung: | 06.05.2026, 04:17 Uhr (SOC InsoTec Systems GmbH) |
| Kenntnisnahme Verantwortlicher: | 06.05.2026, 04:52 Uhr (Geschäftsführerin Wallbruck) |
| Art der Verletzung: | Verlust der Verfügbarkeit, Vertraulichkeit und Integrität |
| Gesamtanzahl betroffener natürlicher Personen (ca.): | 298 Personen |
| Besondere Kategorien (Art. 9 DSGVO): | Gesundheitsdaten – 38 Mitarbeiter (BEM-Verfahren) |

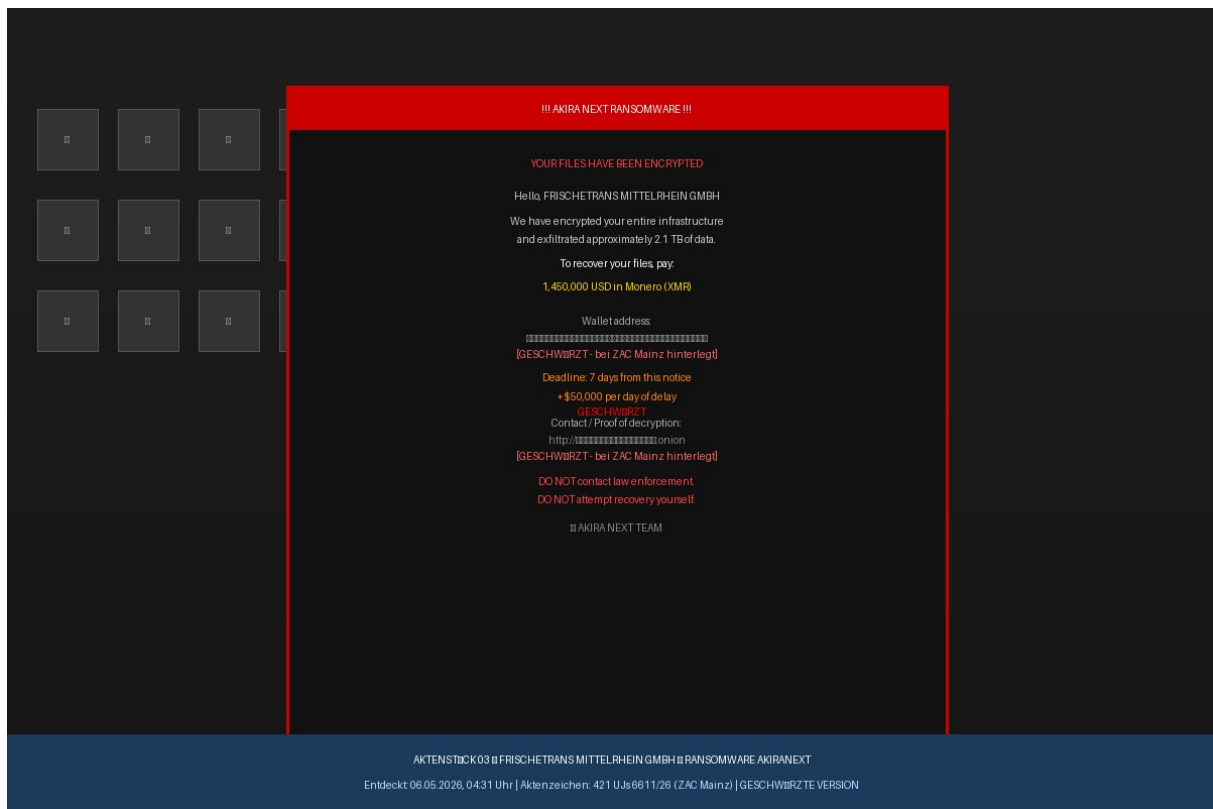
Bildanlagen und Screenshots

Datei: jpg/01_netzwerktopologie_frischetrans.jpg



Bilddatei: 01_netzwerktopologie_frischetrans.jpg

Datei: jpg/02_ransomware_erpressungsschreiben_screenshot.jpg



Bilddatei: 02_ransomware_erpressungsschreiben_screenshot.jpg

Datei: jpg/03_serverraum_uebersicht.jpg



Bilddatei: 03_serverraum_uebersicht.jpg

PDF-Anhang: pdfs/bsi_meldebestaetigung.pdf

Datei: bsi_meldebestaetigung.pdf

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK

Außenstelle Frankfurt · Gutleutstraße 163 · 60327 Frankfurt am Main
BSI
www.bsi.bund.de

EINGANGSBESTÄTIGUNG

Meldung eines erheblichen Sicherheitsvorfalls gemäß § 31 NIS2UmsuG

| | |
|---------------------|---|
| BSI-Referenznummer: | BSI-REF-2026-1847 |
| Eingangsdatum: | 07.05.2026, 16:30 Uhr |
| Eingangskanal: | BSI-MELDEPF-Portal (elektronisch) |
| Vorgangsart: | Erstmeldung gemäß § 31 Abs. 3 Nr. 1 NIS2UmsuG |
| Sachbearbeiterin: | Dr. Cornelia Westhoff, Referat C3 (Kritische Infrastrukturen) |
| BSI-Außenstelle: | Frankfurt am Main |

Angaben zur meldenden Einrichtung

| | |
|--------------------------|--|
| Einrichtung: | Frischetrans Mittelrhein GmbH |
| Sitz: | Binger Straße 142, 55131 Mainz |
| Einrichtungstyp: | Wichtige Einrichtung (§ 28 NIS2UmsuG, Sektor: Lebensmittel/Versorgungskette) |
| Bevollmächtigter Anwalt: | RA Lukas Drostén, Kanzlei Drostén & Pekonkur, Mainz |

Bestätigung des Eingangs

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bestätigt den fristgerechten Eingang der Erstmeldung gemäß § 31 Abs. 3 Nr. 1 NIS2UmsuG für den gemeldeten erheblichen Sicherheitsvorfall (Ransomware-Angriff AkiraNext, 06.05.2026).

Die Meldung wurde innerhalb der gesetzlichen Frist von 24 Stunden nach Kenntniserlangung erheblicher Auswirkungen eingereicht.

Nächste Schritte

Folgebericht (§ 31 Abs. 3 Nr. 2 NIS2UmsuG) bis nach dieser Erstmeldung, d.h. bis 10.05.2026, 16:30 Uhr

Abschlussbericht (§ 31 Abs. 3 Nr. 3 NIS2UmsuG) des Monats, d.h. bis 07.06.2026

BSI-Ansprechpartnerin: Dr. Cornelia Westhoff, Tel. +49 69 XXXX-XXXX (MELDEPF-Portal)

Koordination mit LfDI RLP: Beide Meldungen (DSGVO + NIS2) werden behördenintern koordiniert

Frankfurt am Main, den 07.05.2026

Dr. Cornelia Westhoff
Referatsleiterin C3 — Kritische Infrastrukturen
BSI Außenstelle Frankfurt
Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik · Godesberger Allee 185–189 · 53175 Bonn ·
www.bsi.bund.de

Dieses Dokument ist eine automatisch generierte Eingangsbestätigung des BSI-MELDEPF-Portals. Es hat
keine Rechtswirkung bezüglich der inhaltlichen Bewertung des gemeldeten Vorfalls.

PDF-Anhang: pdfs/erpressungsschreiben_akiranext_redacted.pdf

Datei: erpressungsschreiben_akiranext_redacted.pdf

KANZLEI DROSTEN & PEKONKUR

Rechtsanwälte und Fachanwälte · Schillerstraße 14 · 55116 Mainz

ERPRESSUNGSSCHREIBEN AKIRANEXT

Geschwärzte Fassung — REDACTED

| | |
|-------------------------|--|
| Mandantin: | Frischetrans Mittelrhein GmbH, Binger Str. 142, 55131 Mainz |
| Vorfallsdatum: | 06.05.2026, 04:31 Uhr (Zeitpunkt der Entdeckung des Erpressungsschreibens) |
| Angreifer: | AkiraNext Ransomware Group (kriminelle Organisation) |
| Aktenzeichen: | 421 UJs 6611/26 (ZAC Mainz) / DP-2026-0506-FTM (Kanzlei) |
| Original: | Beim ZAC Mainz und in der Mandantenakte (ungeschwärzt) hinterlegt |
| Klassifizierung: | STRENG VERTRAULICH — Nur für Mandantin, Behörden, Versicherung |

■ HINWEIS: Kryptowährungs-Wallet-Adresse und Tor-Onion-URL sind in dieser Fassung geschwärzt (■■■■). Die vollständige ungeschwärzte Version ist bei ZAC Mainz (421 UJs 6611/26) aktenkundig.

1. Originaltext des Erpressungsschreibens (Transkription — geschwärzt)

Das folgende Schreiben wurde auf allen verschlüsselten Systemen als Textdatei !!! AKIRA_NEXT_README.txt sowie als Desktop-Hintergrund vorgefunden:

[AKIRA NEXT RANSOMWARE – ORIGINAL AUF ENGLISCH – ÜBERSETZUNG RA DROSTEN]

AKIRA NEXT – IHR SYSTEM WURDE VERSCHLÜSSELT

Wir haben Ihre gesamte Infrastruktur verschlüsselt und ca. 2,1 TB sensibler Daten exfiltriert, darunter:

- Vollständige Kundendatenbank (18 Unternehmenskunden)
- Mitarbeiterpersonalakten (280 Mitarbeiter)
- HR/Gesundheitsdaten (BEM-Akten, 38 Mitarbeiter)
- Finanzdaten Q1/2026
- SAP-Konfigurationsdaten

Zur Wiederherstellung Ihrer Dateien zahlen Sie:

1.450.000 USD in Monero (XMR) an Wallet:

[illegible]

Sie haben 7 Tage.

Kontakt und Entschlüsselungs-Nachweis:

[http://\[REDACTED\].onion](http://[REDACTED].onion)

BEZAHLEN SIE NICHT, droht Veröffentlichung.

Jeden Tag Verzug: +50.000 USD Aufschlag.

— AKIRA NEXT TEAM

2. Rechtliche Einordnung (Kurzfassung)

- § 202a StGB — Ausspähen von Daten: Unbefugte Erlangung von ca. 2,1 TB unter Überwindung von Zugangssicherungen.
- § 303b StGB — Computersabotage: Angriff auf ERP-System und Telematik eines Lebensmittelversorgers.
- § 253 StGB — Erpressung: Forderung von 1.450.000 USD unter Drohung der Datenveröffentlichung.
- § 263a StGB — Computerbetrug: Absicht des rechtswidrigen Vermögensvorteils durch EDV-Manipulation.

3. Empfehlung der Kanzlei

Keine Lösegeldzahlung. Kanzlei Drosten & Pekonkur empfiehlt ausdrücklich, das geforderte Lösegeld nicht zu zahlen. Gründe: (1) Keine Erfolgsgarantie auf Entschlüsselung, (2) Strafbarkeitsrisiken nach §§ 129, 261 StGB, (3) Versicherungsklausel (Zustimmungsvorbehalt CyberCovered AG), (4) Backup verfügbar. Die Mandantin folgt dieser Empfehlung.