# Handlungsbedarf Frachtkriminalität in Deutschland und Europa

## Strukturelle Schutzlücken bei Mehrfachtätern, Identitätsbetrug, und Compliance Prozessen in der Logistik

Whitepaper

Version 1.0

08.05.2026

# Inhaltsverzeichnis

## Tabellenverzeichnis

## Executive Summary

Die Bedrohungslage in der Logistik eskaliert. Frachtdiebstahl nimmt nicht nur zu, sondern verändert seinen Charakter grundlegend. Nach aktuellen Branchenanalysen ist Cargo Theft in Europa innerhalb eines Jahres um 438 % gestiegen und mehr als zehnmal so hoch wie noch im Jahr 2021. Deutschland steht zugleich bei schweren Schadensfällen im europäischen Vergleich an der Spitze. Die Angriffe sind heute zunehmend strategisch vorbereitet, digital unterstützt und arbeitsteilig organisiert. An die Stelle einfacher Gelegenheitsdelikte treten Insiderbeteiligung, Fake-Carrier-Konstruktionen, Identitätsbetrug, Dokumentenfälschung und Mehrfachidentitäten.

Gerade darin liegt das zentrale Problem: Täter erscheinen nicht mehr nur als externe Angreifer, sondern als scheinbar legitime Personen innerhalb regulärer Lieferkettenprozesse. Sie greifen auf echte oder gefälschte Dokumente zurück, wechseln Identitäten, nutzen Unternehmenswechsel und Subunternehmerstrukturen und können dadurch trotz vorheriger Auffälligkeiten erneut Zugang zu sicherheitsrelevanten Positionen erhalten. Herkömmliche Kontrollmechanismen reichen dafür nicht aus. Weder klassische Dokumentenprüfungen noch isolierte Unternehmensscreenings oder punktuelle biometrische Prüfungen schließen diese Schutzlücke zuverlässig.

Gleichzeitig stehen Unternehmen unter erheblichem operativem und rechtlichem Druck, weil Führerscheine, Arbeitserlaubnisse und weitere einsatzrelevante Nachweise fortlaufend geprüft, vorgehalten und dokumentiert werden müssen. In der Praxis führt dies häufig zu hohem manuellem Aufwand, zu ineffizienten Prozessen und zu zusätzlichen Haftungs- und Datenschutzrisiken.

Dieses Whitepaper analysiert anhand reputabler Quellen die wachsende Sicherheitslücke in der Logistik, arbeitet die daraus folgenden Lösungsanforderungen heraus und vergleicht die derzeit angebotenen Lösungsansätze systematisch anhand dieser Anforderungen.

Jährlicher Schaden durch Frachtdiebstahl

**8.2 Mrd. €**

Europäische Kommission

## 1. Zunehmender Frachtdiebstahl

Frachtdiebstahl ist eine zunehmende Herausforderung. Die Schätzung der Europäischen Kommission aus dem ROADSEC-Leitfaden beziffert den Schaden durch Frachtdiebstahl in der Europäischen Union auf rund 8,2 Mrd. € jährlich (trans.info, 2025).

Der Präsident der Transport Asset Protection Association (TAPA) fasst die Lage wie folgt zusammen: „It is beyond any doubt that supply chain resilience is more at risk today than at any time in the Association's 23-year history in the EMEA region" (TAPA, 2023, S. 7). Und weiter: „Crime is spreading, losses are soaring, risks are escalating" (TAPA, 2023, S. 4). Ein besonders eindrücklicher Hinweis auf die zunehmende Bedeutung

dieses Problems findet sich in einem europäischen Branchenüberblick von trans.info. Hier wird auf Basis mehrerer Marktanalysen ein massiver Anstieg von Frachtdiebstählen in Europa dokumentiert: „in 2023 a 438% jump compared to 2022 and more than ten times higher than in 2021“ (trans.info, 2025).

Laut dem letzten Bericht der TAPA steht Deutschland auf Platz 1 der Länder, die die meisten Diebstähle mit einem Schaden von über 100.000 € an die TAPA gemeldet haben, Zitat: „Germany recorded the highest number of major losses“ (TAPA, 2023, S. 4). Täter zielen längst nicht mehr nur auf hochpreisige Ware. Allerdings ist im Falle hochpreisiger Ware der Schaden beachtlich. Hierzu schreibt der Report: „€300 million of losses recorded in just two crimes; one involving the hijacking of miscellaneous goods in Belgium, and the other a case of fraud detected within a metal supply chain by a global organisation based in Germany.“

Angriffe auf EMEA-Lieferketten in 273 Tagen

**49.366**

TAPA EMEA

Es bleibt jedoch nicht bei zwei Vorkommnissen; der TAPA wurden „49,366 criminal attacks on supply chains in EMEA in 273 days“ gemeldet und die Dunkelziffer wird als hoch eingeschätzt (TAPA, 2023, S. 3). Hierbei wurden im Jahr 2024 76 % der Warendiebstähle in der Logistik direkt aus Fahrzeugen entwendet (Logistik Heute, 2025).

Verluste durch Frachtdiebstahl in Europa

**+438%** ggü. Vorjahr

trans.info

### 1.1. Zunehmende Fähigkeiten krimineller Strukturen

Das Fachmagazin Logistik Heute titelt „Ladungsdiebstahl: „Strategischer“ Diebstahl war 2024 herausragender Wachstumstrend“ (Logistik Heute, 2025). „Die Zunahme der strategischen Kriminalität, das heißt der Kriminalität, die sich der Täuschung, des Betrugs und der Vorausplanung bedient, ist das bemerkenswerteste Ergebnis unseres Berichts“, sagt Tony Pelli, Global Practice Director for Security & Resilience bei BSI Consulting. Der Grad der Raffinesse, der eingesetzt wird, zeigt, dass das organisierte Verbrechen die Schwachstellen der Lieferkette immer besser kennt (Logistik Heute, 2025).

#### 1.1.1. Zunehmende Nutzung von Insidern innerhalb der Lieferkette

In der sicherheitsbezogenen Fachliteratur und Branchenanalyse wird zunehmend darauf hingewiesen, dass Logistikdiebstähle nicht ausschließlich von externen Tätergruppen, sondern in wachsendem Maße unter Mitwirkung von Personen innerhalb der Lieferkette erfolgen. Dabei handelt es sich um sog. Insider, demnach Personen, die entweder im Angestelltenverhältnis oder über Transportpartnerstrukturen oder über sonstige

Dienstleisterstrukturen in die Lieferkette als Fahrer, Geschäftsführer sog. Fake Carrier, Lagerarbeiter oder sonstige Arbeiter eingebunden sind. Diese Insider werden oft gezielt in Lieferketten eingeschleust, um Diebstähle zu begehen oder vorzubereiten. Sie sind entweder aktiv am Diebstahl beteiligt, oder ermöglichen diesen durch Informationsweitergabe, Zutrittverschaffung, Sabotage oder passives Dulden.

Der weltweit anerkannte Sicherheitsbericht des TT Club in Zusammenarbeit mit der BSI stellt in der 2025 veröffentlichten Ausgabe klar: „Industries ranging from food and beverage to metals, consumer goods, and apparel have all experienced the impact of strategic theft. This problem is exacerbated by insider participation, with criminals leveraging access to sensitive information to identify and intercept high-value shipments“ (TT Club, BSI, 2025, S. 6).

> “All industries have experienced the impact of strategic theft.”
>
> BSI Consulting and TT Club

Auch das Beratungs- und Versicherungsunternehmen Munich Re weist in seinem aktuellen Bericht auf die Rolle von Insider-Kollusion bei komplexen Täuschungsdelikten in der Lieferkette hin. Dort wird ‚Insider Collusion‘ als eine ‚Key Strategy‘ beschrieben, die Kriminelle nutzen, um Sicherheitsmaßnahmen zu umgehen (Munich Re, 2025). Der europäische Branchenüberblick von trans.info konstatiert auf Basis mehrerer Marktanalysen: „Fraudulent carriers, [...] identity deception and even insider collusion are also on the rise“ (trans.info, 2025). Auch der auf Risikomanagement spezialisierte Roanoke-Konzern sieht im Cargo Theft Report 2025 einen signifikanten Trend: „ Insider information is frequently leveraged to target higher-value shipments, amplifying the risks for businesses handling premium products“ (Roanoke Insurance Group Inc., 2025).

> “The biggest thing that stood out was the increase in insider participation in thefts.”
>
> FreightWaves

Eine besonders konkrete Einschätzung liefert das Fachportal FreightWaves. Dort heißt es im Bericht: „The biggest thing that stood out was the increase in insider participation in thefts [...] people giving details of information or details of shipments as they are coming out of warehouses or other locations, and people sort of tailing that and stealing it, or using it to facilitate theft in other ways“ (FreightWaves, 2025). Diese Aussagen aus unabhängigen und international renommierten Quellen deuten auf eine systematische Veränderung im Modus Operandi krimineller Akteure hin: Wo früher dominant physische Gewalt und klassische Einbruchsmethoden dominierten, stehen heute vermehrt Prozesswissen, Zugriffsrechte und gezielte Manipulation im Vordergrund. Insider agieren nicht nur als Informationsquelle, sondern in vielen Fällen als integraler Teil krimineller Netzwerke. Für die europäische

Logistikbranche bedeutet dies, dass präventive Sicherheitsstrategien nicht nur nach außen, sondern auch nach innen gerichtet sein müssen – mit Fokus auf Mitarbeiterüberprüfung, Zugangskontrolle und digitale Transparenz innerhalb der Lieferkette.

### 1.1.2. Fake Carrier

Fake Carrier sind ein Indikator der steigenden Professionalisierung organisierter Kriminalität im Frachtsektor. Die Methode hat sich von simplen Diebstählen zu einer digitalen, arbeitsteiligen Betrugsindustrie entwickelt, die zu signifikanten Schäden im Frachtsektor führt. Der Begriff Fake Carrier (auch Phantom- oder Schein-Frachtführer) beschreibt Kriminelle, die sich als seriöse Spediteure ausgeben, um Frachtaufträge zu erschleichen. Die Ware wird sodann offiziell abgeholt und verschwindet häufig spurlos (Transportversicherungsmakler, 2025; GDV, 2025a; DVZ, 2021; Dekeyser, 2022). Häufige Ziele sind hochwertige Güter wie Elektronik, Metalle (z. B. Kupfer), Kleidung, Fahrzeugteile (Transportversicherungsmakler, 2025; Debus, 2024). Die nächste Stufe der Professionalisierung erreichen kriminelle Strukturen im Übergang von physischen Angriffen zu digitalen Täuschungen mit gefälschten Identitäten (Schunk Group, 2025; Handelsblatt, 2025).

Die Täter entwickeln ihre Methoden sukzessive weiter. Ein Einfallstor sind digitale Plattformen. Es werden Frachtbörsen genutzt, um lukrative Aufträge zu identifizieren und dann in die direkte Kontaktaufnahme außerhalb der Plattform mit manipulierten Kontaktdaten zu gehen (z. B. URL-Fraud durch Endungsveränderung .de zu .com) (Schunk Group, 2025; GDV, 2025a). Ein weiterer Weg ist Identitätsverschleierung, bei der gestohlene oder falsche Firmenidentitäten, gefälschte Versicherungszertifikate, Handelsregisterauszüge oder gekaperte Benutzerkonten eingesetzt werden (trans.info, 2021; TrustRiskControl, 2024). Der gesamte Ablauf der offiziellen Warenannahme und Tour-Organisation ist professionell durchorganisiert. Unterwegs erfolgen Änderungen der Lieferadresse oder die vollständige Leerung des Trailers; oft mit unwissenden Subunternehmern als Tarnung (Secure Logistics, 2026).

Schaden durch Fake Carrier allein in Benelux

**350 Mio. €**

Secure Logistics

Der durch Fake Carrier verursachte Schaden in Deutschland kennt daher nur einen Trend: stark steigend. Die Anzahl der Fälle hat sich von 2024 auf 2025 nahezu verdoppelt und auch die Schadenshöhe pro Fall steigt rasant: von 130.000 € (2024) auf 200.000 € (2025), was einem monatlichen Schaden von ca. 1,5 Mio. € entspricht (GDV, 2025a). Für die Benelux-Region wird der jährliche Schaden 2025 sogar auf mehr als 350 Mio. € geschätzt (Secure Logistics, 2026).

Um diesem Trend entgegenzuwirken, hat die TAPA eine spezialisierte „Fake-Carrier-Intelligence-Gruppe“ auf europäischer Ebene mit 38 Mitgliedern ins Leben gerufen, die seit 2021 an Maßnahmen

arbeitet (trans.info, 2021).

Bisher gibt es allerdings keine Entwarnung: die kriminellen Strukturen professionalisieren sich weiter, betreiben Arbeitsteilung (IT-Spezialisten und Logistikkenner) und internationalisieren ihre Netzwerke. Der GDV warnt daher vor einem exponentiellen Anstieg und Branchenverbände organisieren Expertengremien und Fachveranstaltungen mit Fokus Fake Carrier (SVG, 2026; GDV, 2025b; TrustRiskControl, 2024; Börse Global, 2026).

Fake-Carrier-Betrug ist wesentlich durch Identitätsbetrug natürlicher Personen geprägt. An der Frachtübergabe tritt die abholende Person als vermeintlich berechtigter Fahrer auf und nutzt gefälschte, verfälschte oder betrügerisch erlangte echte Unterlagen. IUMI und TAPA EMEA beschreiben dieses Muster mit „counterfeit driver credentials" und halten zugleich fest, dass „at the point of collection, everything appears to be a normal transport" (IUMI & TAPA, 2026).

Für die Person am Übergabepunkt ist diese Täuschung regelmäßig nicht belastbar erkennbar. Die Bundesdruckerei erklärt, dass eine Prüfung häufig „mit bloßem Auge" erfolgt und selbst bei geschulten Mitarbeitern „eine umfassende Prüfung aller Fälschungsmerkmale schlichtweg nicht möglich" sei (Bundesdruckerei, 2019).

Bei Fraudulently Obtained Genuine Documents (FOGD) verschärft sich dieses Erkennungsproblem qualitativ: Nicht die äußere Echtheit des Dokuments ist das Problem, sondern die betrügerische Grundlage seiner Erlangung. FOGD können daher auch nicht mit den besten Dokumentenprüfungsapparaten der Bundesdruckerei erkannt werden, da der Betrug nicht auf Ebene des Dokuments erfolgt, sondern auf einer vorgelagerten Ebene durch sog. „Breeder Documents" wie bspw. gefälschte Geburtsurkunden oder Herkunftsnachweise (siehe Kapitel 1.1.3.3).
Ohne die zur Erkennung von FOGD notwendigen Voraussetzungen (siehe Kapitel 1.3.2), sind Fahreranmeldungen schutzlos Kriminellen ausgeliefert, die diese weitverbreiteten Täuschungsmechanismen anwenden.

> "...criminal groups in particular tend to use multiple identities in an attempt to cover their illegal activities and avoid detection."
>
> Europol

Auch die handelnden Personen hinter dem Fake Carrier nutzen Identitätsbetrug, FOGD und Mehrfachidentitäten nicht nur zur Tatbegehung, sondern auch zur Verschleierung ihrer späteren Zuordnung. Wer mit gefälschten Dokumenten, betrügerisch erlangten echten Dokumenten oder unter wechselnden Identitäten auftritt, kann nach einer Tat erneut unter anderer Identität handeln und so Wiederholungstaten erleichtern. Europol beschreibt diesen Mechanismus für mobile kriminelle Gruppen ausdrücklich: „Members of itinerant or mobile criminal groups in particular tend to use multiple identities in an attempt to cover their illegal activities and avoid detection" (Europol, 2011). Interpol bestätigt ergänzend, dass Identitäts- und

Reisedokumentenbetrug von Kriminellen genutzt wird, „in order to carry out their illegal activities," und nennt dabei ausdrücklich auch „fraudulently obtained genuine documents" sowie „genuine documents misused by an impostor" (Interpol, 2026). Im Kontext von Fake-Carrier-Betrug verschärft dies das Risiko erheblich: Die Identität der tatsächlich handelnden Person wird zum zentralen Schwachpunkt, weil falsche oder wechselnde Identitäten Rückverfolgung, Täterzuordnung, zivilrechtliche Inanspruchnahme sowie Ermittlung und Strafverfolgung gezielt erschweren.

### 1.1.3. Identitätsbetrug und Mehrfachidentitäten

#### 1.1.3.1. Umfang der Herausforderung

In der sicherheitsbezogenen Analyse moderner Lieferketten wird zunehmend deutlich, dass Identitätsbetrug in vielfältiger Form eine Schlüsselrolle bei strategischen Diebstählen spielt. Aktuelle Branchenberichte und Sicherheitsanalysen zeigen, dass Kriminelle zunehmend auf gefälschte Dokumente und Mehrfachidentitäten setzen, um Frachtdiebstähle in Europa zu begehen. In einer umfassenden Untersuchung von Munich Re wird der strategische Wandel hin zu nicht-gewaltsamen, aber hochkomplexen Betrugsformen beschrieben. Dort heißt es: „Identity deception [...] and insider collusion are all emerging as key strategies used by cargo criminals to bypass security measures" (Munich Re, 2025). Diese Einschätzung findet auch in der Berichterstattung deutscher Fachmedien Widerhall. So berichtet das Fachportal Logistik Heute unter Verweis auf den BSI/TT-Club-Cargo-Theft-Report: „Diese Waffe [strategische Kriminalität] [...] umfasst nun auch die Nachahmung und Fälschung von Dokumenten" (Logistik Heute, 2025). Europäische Behörden beziffern die Dimension: „In 2023 alone [...] 17,424 fraudsters [...] using or possessing 22,395 fraudulent documents" (Frontex, 2024).

**17,424**
fraudsters using or possessing
**22,395**
fraudulent documents in 2023.
Frontex

Kriminelle nutzen dabei sowohl gefälschte als auch echte Identitäts- und Reisedokumente in betrügerischer Weise, um ihre illegalen Aktivitäten durchzuführen (Interpol, 2026). Der belgische Versicherer AJG unterstreicht diese Entwicklung aus Sicht der Risikoabsicherung ebenfalls: „Gangs are using impersonation and document forgery to carry out heists" (Gallagher, 2025). Moderne Frachtdiebe nutzen Identitätswechsel und Imitation gezielt dort, wo die Fahrerrolle operative Schlüsselbefugnisse bündelt (Abholung, Zugang, Übergabe). TAPA beschreibt dieses Täuschungsmuster unmissverständlich: „Thieves will impersonate [...] drivers to get the cargo" (TAPA EMEA, 2024a, S. 8).

Am Beispiel eines Falls in den Niederlanden wird deutlich, wie ein Modus Operandi an der Fahrerschnittstelle praktisch funktioniert: „€1.7 million worth of iPhones stolen [...] he presented false papers at the freight company, had the shipment [...] loaded into the truck, and left"; der

Täter „posed as a truck driver“, während „the actual trucker with the correct papers“ erst am Folgetag eintraf.

> „1.7 million worth of iPhones stolen [...] he presented false papers at the freight company, had the shipment [...] loaded into the truck, and left.“
>
> NL Times

Klassische Fälschungen von Ausweisen oder Führerscheinen sind längst nicht mehr die einzige Bedrohung – moderne Täter nutzen technisch hochentwickelte Manipulationen (NL Times, 2023). Auch Breeder Documents werden gezielt eingesetzt, um damit weitere authentische Identitätsdokumente zu erschleichen (Europol, 2026). Schlussendlich lassen sich zwei Hauptkategorien von Identitätsbetrug unterscheiden (Interpol, 2026):

**Falsche Dokumente:**

- Pseudo-Dokumente – Dokumente, die nicht offiziell anerkannt sind
- Totalfälschungen (Counterfeits) – unbefugte Reproduktion eines echten Dokuments
- Verfälschungen (Forgeries) – Veränderung eines echten Dokuments

**Echte Dokumente:**

- Echte Dokumente, die von einem Identitätsvortäuscher (Impostor) missbraucht werden
- Betrügerisch erlangte echte Dokumente - (Fraudulently Obtained Genuine Documents FOGD) = Betrug mit formaler Korrektheit

Kriminelle nutzen also sowohl den Identitätsbetrug mit formaler Unkorrektheit als auch den Identitätsbetrug mit formaler Korrektheit, den FOGD.

#### 1.1.3.2. Identitätsbetrug mit formaler Unkorrektheit

Identitätsbetrug mit formaler Unkorrektheit ist dadurch gekennzeichnet, dass entweder das Dokument selbst formal mangelhaft ist oder die formale Zuordnung zwischen Dokument und vorlegender Person nicht zutrifft. Interpol ordnet in diese Systematik zunächst die falschen Dokumente ein. Dazu gehören „Counterfeits“, also „an unauthorized reproduction of a genuine document“, ferner „Forgeries“, also die „alteration of a genuine document“, sowie „Pseudo documents“, also „documents which are not officially recognized“ (Interpol, 2026). In all diesen Fällen liegt die formale Unkorrektheit bereits auf Dokumentenebene. Das Dokument ist entweder nicht echt, inhaltlich unzulässig verändert und/oder von vornherein nicht amtlich anerkannt.

Daneben gibt es Konstellationen, in denen zwar ein echtes Dokument vorliegt, die formale Identitätszuordnung im Verwendungsvorgang aber falsch ist. Interpol bezeichnet dies als „Genuine documents misused by an impostor“ (Interpol, 2026). Auch in dieser Fallgruppe liegt daher formale Unkorrektheit vor, jedoch nicht in der Dokumentengestalt, sondern in der Zuordnung zwischen Dokument und vorlegender Person. Das Dokument ist echt, aber der Identitätsnachweis ist im Kontrollmoment formal nicht korrekt, weil die vorlegende Person nicht mit der dokumentierten Person übereinstimmt.

Gemeinsam ist diesen Formen des Identitätsbetrugs somit, dass die Unkorrektheit bei einer Prüfung der formalen Dokumentenlage oder der formalen Personenidentität grundsätzlich erkennbar werden kann. Entweder zeigt sich der Mangel am Dokument selbst oder an seiner unmittelbaren Verwendung.

#### 1.1.3.3. FOGD: Identitätsbetrug mit formaler Korrektheit

Interpol klassifiziert neben klassischen Fälschungen und Missbrauch echter Dokumente insbesondere FOGD („Fraudulently obtained genuine documents“) als Standardkategorien der Täuschung (Interpol, 2026).

FOGD ist die am schwersten zu erkennende Ausprägung des Identitätsbetrugs, bei der alle bisher flächendeckend eingesetzten Prüfmechanismen versagen. Es handelt sich um amtlich ausgestellte, formal echte Ausweise (z. B. EU-Reisepässe), die jedoch auf Basis betrügerisch formulierter Identitäten ausgestellt wurden. Ein solcher Pass enthält alle originären Sicherheitsmerkmale (z. B. Hologramme, Chips, Wasserzeichen) und durchläuft jede Kontrolle regulärer Sicherheitsprüfungen, zeigt jedoch nicht die korrekte Identität des einsetzenden Betrügers (Interpol, 2026).

FOGD hat sich zu einer erheblichen und wachsenden Erscheinungsform des Dokumenten- und Identitätsbetrugs entwickelt. Die Europäische Kommission beschreibt Reisedokumentenbetrug als „increasingly significant problem“ und stellt fest, dass dieses Problem durch terroristische Angriffe und Migrationsbewegungen zusätzlich an sicherheitspolitischer Relevanz gewonnen hat (European Commission, 2018). Zudem beschreibt die Europäische Kommission eine methodische Verschiebung der Betrugsformen: „increasingly shifting from ‘traditional’ fraud“ zu „fraudulent obtaining of genuine documents“. In Europa stieg im Referenzjahr 2015-2016 die Nutzung von FOGD um 76 %, während die Nutzung klassischer Fälschungen um 4 % zurückgeht (European Commission, 2016).

Während Fälschungen um 4% abnahmen, stieg FOGD-Nutzung in der EU um

**76 %** p.a.

Europäische Kommission

Frankreich ist nur ein Beispiel für das Ausmaß dieses Problems: Hier werden 500.000 bis 1.000.000 (von insgesamt 7.000.000) biometrische Pässe als auf Basis falscher Breeder Documents erlangt geschätzt (Le Parisien, 2011).

Politico zitiert wiederum einen griechischen Beamten in Bezug auf das Ausmaß des Problems mit “between five and seven percent of all Greek passports stem from fake ID cards or birth certificates” (Politico, 2016).

> “between five and seven percent of all Greek passports stem from fake ID cards or birth certificates.”
>
> Politico

Auch Frontex bestätigt die erhebliche operative Dimension von Dokumenten- und Identitätsbetrug an den EU-Außengrenzen. Frontex bezeichnet diese

Betrugsformen als „instrumental for a broad range of criminal activities“ (Frontex, 2024). Und Interpol stellt fest: „Criminals and terrorists often make fraudulent use of both fake and genuine identity and travel documents“ (Interpol, 2026).

Europol beschreibt den zugrundeliegenden Mechanismus der Breeder Documents wie folgt: Administrative Dokumente wie Geburtsurkunden, Heiratsurkunden, Arbeits- und Aufenthaltserlaubnisse können als „Breeder Documents“ genutzt werden, „to obtain other identification documents fraudulently“ (Europol, 2026).

Die wissenschaftliche Literatur beschreibt FOGD als gezielt genutzte Betrugsform. Eine Studie zu manipulierten Passbildern zeigt auf: „fraudsters are now known to be focusing on obtaining FOG (fraudulently obtained but genuine) passports“, eine Form von FOGD. FOG-Pässe werden dort als „real documents“ beschrieben, die irrtümlich an betrügerische Antragsteller ausgestellt werden (Robertson, et al., 2018).

> „the number of FOG documents in existence is believed to be greater than that of falsified or counterfeit documents“
>
> ITW Security Division

In der Gesamtschau zeigen diese Quellen, dass FOGD eine zunehmende und hochrelevante Erscheinungsform des Dokumenten- und Identitätsbetrugs ist. Besonders schwer wiegt, dass Fachkreise die Zahl betrügerisch erlangter echter Dokumente bzw. FOGD mittlerweile als höher einschätzen als die Zahl klassisch gefälschter oder nachgemachter Dokumente (ITW Security Division, 2017)

Ein exemplarischer Fall eines solchen Vorgehens ereignete sich in Bulgarien: Dort wurden staatliche Beamte beschuldigt, gegen Bestechung „certificates saying they had Bulgarian origins“ ausgestellt zu haben. Diese ermöglichten es Antragstellern, sich unter falscher Identität als bulgarische Staatsbürger auszugeben, um anschließend echte bulgarische Reisepässe zu erhalten – vollständig mit allen Sicherheitsmerkmalen, jedoch auf Grundlage gefälschter Angaben (Euractiv, AFP, 2018; OCCRP, 2018).

Auch Europol dokumentierte 2024 erneut, dass Reise- und Ausweisdokumente häufig betrügerisch beantragt und von Behörden auf Grundlage manipulierten Datenmaterials ausgestellt werden – etwa durch Netzwerke, die als Reisebüros getarnt sind (Europol, 2025).

Die ICAO formuliert für die sichere Ausstellung von Reisedokumenten drei notwendige Elemente. Dazu gehört insbesondere „evidence of the applicant’s identity, i.e. this is a real identity, and the applicant is in fact the claimed individual“ (ICAO, 2016).

Gerade an dieser Stelle setzt FOGD an. Wenn die Behörde aufgrund manipulierter Ausgangsinformationen, bspw. durch eine gefälschte Geburtsurkunde (Breeder Document), Identitätsanmaßung oder sonstige Täuschung zu dem Ergebnis kommt, dass der Antragsteller die behauptete Person ist, kann das später

ausgestellte Dokument formal korrekt und technisch echt sein, obwohl seine Grundlage betrügerisch ist.

Die vorgetäuschte Identität ist in diesem Fall gerade deshalb schwer erkennbar, weil sie im Ausstellungsverfahren bereits akzeptiert wurde. Die ICAO weist in diesem Zusammenhang ausdrücklich darauf hin, dass „The processes that authorities follow to establish and verify a person's identity are often laxer than the security of the document" (ICAO, 2018).

> "The processes that authorities follow to establish and verify a person's identity are often laxer than the security of the document."
>
> ICAO

Damit wird deutlich, dass selbst hochsichere Dokumente keine verlässliche Gewähr bieten, wenn der Identitätsprüfungsprozess vor der Ausstellung kompromittiert war. FOGD ist deshalb analytisch nicht als bloßes Dokumentenproblem, sondern als Identitäts- und Ausstellungsproblem zu begreifen. Seine Gefährlichkeit beruht gerade darauf, dass Betrug durch formale Korrektheit verdeckt werden kann. Strategische Diebstähle setzen auf Imitation und Urkundenmanipulation. Zugleich wird die Beteiligung von Insidern einschließlich Fahrern von anerkannten Sicherheitsreports ausdrücklich benannt: „Thieves may recruit [...] truck drivers—to minimize risk during the attack" (TT Club, BSI, 2025).

### 1.2. Mehr Wiederholungstäter

Zahlreiche Fachquellen belegen, dass Eigentumsdelikte in der Logistikbranche zunehmend von Insidern wie Fahrern begangen werden – und dass viele dieser Täter als Wiederholungstäter in Erscheinung treten.

> „Insider theft – often by drivers – is one of the fastest growing threat vectors in Europe."
>
> TAPA

So beschreibt die TAPA in ihrem aktuellen Lagebericht: „Insider theft – often by drivers – is one of the fastest growing threat vectors in Europe" (TAPA, 2023, S. 7). Dabei würden Tätergruppen „gezielt Fahrer in Positionen einschleusen, um später kontrollierten Zugang zu Ware und Prozessen zu erhalten" (TAPA, 2023, S. 8). Diese strukturelle Wiederholungsgefahr wird durch rechtliche und organisatorische Lücken im System ermöglicht. Das Hauptproblem moderner Frachtkriminalität liegt nicht im isolierten Einzeltäter, sondern im wiederholt auftretenden Täter.

Anteil der Wiederholungtäter bei Diebstahl:

**70 %**

EHI

Diebstahl ist generell ein Phänomen, das vor allem durch Mehrfachtäter begründet ist. Nach der EHI bezogenen Auswertung des Handelsverbands Bayern sind „70 Prozent (!) der ertappten Ladendiebe Wiederholungstäter". Zugleich heißt es dort: „Ladendiebstähle nehmen weiter dramatisch zu."

Damit wird deutlich, dass nicht nur die Zahl der Diebstähle steigt, sondern dass diese Zunahme in einem Deliktsfeld erfolgt, in dem die Mehrheit der identifizierten Täter bereits Wiederholungstäter ist (HV Bayern, 2025).

Auch britische Retail Crime Daten bestätigen diesen Zusammenhang zwischen Diebstahlszunahme und Wiederholungstätern. Die Thames Valley Retail Crime Strategy hält fest, Diebstahl sei keineswegs nur ein opportunistisches Einzeldelikt; vielmehr seien „nearly two-thirds of thieves" Wiederholungstäter. Zugleich berichten „65% of retailers", dass die Zahl der Vorfälle mit organisierten kriminellen Gruppen in den letzten zwölf Monaten zugenommen habe (Thames Valley Police, 2024).

Noch deutlicher wird die aktuelle Zunahme bei ASIS International: Für 2024 berichtete „more than half of retailers" eine Zunahme von „repeat offender theft". Diese Quelle belegt nicht nur, dass Wiederholungstäter eine zentrale Tätergruppe sind, sondern ausdrücklich, dass das Problem der Wiederholungstäter selbst zunimmt (Security Management, 2025).

Aktuelle britische Retail Crime Daten zeigen zudem, dass die Zunahme sicherheitsökonomisch besonders relevant ist, weil sich Kriminalität stark auf wenige wiederholt handelnde Täter konzentriert: Die obersten 10 % der Retail Crime Täter waren für 68 % der gesamten erfassten Retail Crime verantwortlich; diese Wiederholungstäter waren außerdem deutlich häufiger gewalttätig oder bewaffnet (Auror, 2026).

Auch der ACS Crime Report 2025 bestätigt den operativen Kern des Problems: „repeat offenders target multiple retail premises stealing goods to order and selling them on." Zugleich wird betont, dass Polizei und Handel Beweise zusammenführen müssen, um solche Wiederholungstäter gezielt zu identifizieren; wo dies gelingt, sinkt das Volumen der Ladendiebstähle (ACS, 2025).

> "crime is highly concentrated among a small group of offenders"
>
> Martinez, Lee, Eck, & O, 2017

Kriminologisch entspricht dies dem bekannten Konzentrationsmuster von Eigentumskriminalität. Eine systematische Übersichtsarbeit hält fest, dass „crime is highly concentrated among a small group of offenders" und dass Prävention gerade diejenigen wenigen Täter adressieren muss, „who are responsible for most of the crime" (Martinez, Lee, Eck, & O, 2017).

Auf europäischer Ebene wird diese wiederholte Täterlogik bei mobilen kriminellen Gruppen sichtbar. Eine Studie des Europäischen Parlaments beschreibt sie als „association of offenders", die „systematically acquire wealth through theft of property or fraud", ein weites Operationsgebiet haben und international aktiv sind. Auch hier liegt der Kern nicht im Einzeldelikt, sondern in der systematisch wiederholten Tatbegehung durch dieselben Täter oder Tätergruppen (European Parliament, 2020).

Farrell und Pease beschreiben denselben Mechanismus mit Blick auf Wiederholungskriminalität: „Most crime is a rehearsal for further crime against the same or similar targets“. Übertragen auf die Logistik bedeutet dies, dass einmal erlangtes Wissen über Routen, Lagerprozesse, Warenwerte, Ansprechpartner, Sicherheitsabläufe und Übergabepunkte später erneut genutzt werden kann (Pease & Farrell, 2017).

> Most crime is a rehearsal for further crime against the same or similar targets.“
>
> Pease & Farrell, 2017

Die relevante Schutzlücke betrifft nicht nur einzelne Dokumente, einzelne Unternehmen oder einzelne Kontrollen, sondern die fehlende Wiedererkennung derselben natürlichen Person. Mehrfachtäter können an unterschiedlichen Stellen der Supply Chain erneut auftreten, etwa als Fahrer, Lagerarbeiter, Disponent, Kontaktperson eines Transportunternehmens, Betreiber eines Fake Carriers oder eingebundene Person bei einem anderen Dienstleister. Einmal erlangtes Insiderwissen bleibt nach einem Rollen oder Unternehmenswechsel verwertbar. Wenn Diebstahlskriminalität steigt, Wiederholungstäter in warenbezogenen Delikten die Mehrheit der identifizierten Täter stellen und zugleich mehr Händler eine Zunahme von „repeat offender theft“ melden, wird die fehlende Wiedererkennung solcher Personen zur zentralen Schutzlücke moderner Frachtkriminalität.

## 1.3. Welche Herausforderungen bestehen bei der Bekämpfung? (Fehlende Transparenz)

### 1.3.1. Mangelnde Transparenz

Für Unternehmen ist es schwierig festzustellen, ob es sich bei einem internen oder externen Mitarbeiter um eine Person handelt, die in kriminelle Machenschaften verwickelt war oder ist. Das Problem liegt in der Datenerfassung. Schwerwiegende Kündigungsgründe sind nicht firmenübergreifend erfassbar, das unangemessene Verhalten ist oft nicht feststellbar und nicht dokumentiert und eine Historie ist beim Arbeitgeberwechsel nicht gegeben.

#### 1.3.1.1. Mangelnde Transparenz in polizeilichen Führungszeugnissen

Die Ursache liegt in den strukturellen Grenzen des Datenschutz- und Strafregisterrechts. Arbeitgeber erhalten keinen vollständigen Einblick in das Bundeszentralregister. Im Regelfall können sie nur ein einfaches Führungszeugnis verlangen, sofern dies für die konkrete Tätigkeit erforderlich und verhältnismäßig ist.

> Umfangreiche Ausnahmen für Eintragungen ins Führungszeugnis:
>
> § 32 Abs. 2 BZRG
>
> Bundesamt für Justiz, 1984

Dieses Führungszeugnis ist kein vollständiger Risikonachweis, sondern ein gesetzlich gefilterter Auszug. § 32 Abs. 2 BZRG nimmt zahlreiche Entscheidungen von der Aufnahme aus, darunter Geldstrafen bis 90 Tagessätze,

Freiheitsstrafen bis drei Monate sowie unter weiteren Voraussetzungen auch Jugendstrafen und Freiheitsstrafen bis zu zwei Jahren (Bundesamt für Justiz, 1984).

Ein leeres Führungszeugnis bedeutet nicht: keine relevanten Vorfälle. Es bedeutet nur: keine nach § 32 BZRG im einfachen Führungszeugnis erscheinenden Einträge.

Für sicherheitskritische Lieferketten ist diese Filterwirkung erheblich. Ein Führungszeugnis ohne Eintrag belegt nicht die Abwesenheit strafrechtlich relevanter Vorfälle. Es zeigt lediglich, dass nach den gesetzlichen Aufnahmegrenzen kein eintragungspflichtiger Sachverhalt ausgewiesen wird. Bei Eigentums- und Vertrauensdelikten entsteht dadurch eine strukturelle Transparenzlücke. Die Relevanz zeigt sich in veröffentlichten Entscheidungen. In einem Fall des LG Gießen war ein Täter an drei Diebstahlskomplexen mit Einbruchsbezug beteiligt; die Sanktion lag dennoch bei 90 Tagessätzen und damit innerhalb der Grenze, bei der eine alleinige Registerstrafe grundsätzlich nicht in das einfache Führungszeugnis aufgenommen wird (LG Gießen, Urteil vom 17.03.2020 - 2 KLs - 401 Js 27674/19). Noch deutlicher ist ein Fall des Bundesverwaltungsgerichts: Ein Täter wurde wegen Diebstahls in 10 Fällen und gemeinschaftlichen Diebstahls in 5 Fällen zu 90 Tagessätzen verurteilt. Eine Serie von 15 Diebstählen kann damit registerrechtlich unterhalb der Sichtbarkeitsschwelle des einfachen Führungszeugnisses bleiben (Urt. v. 24.10.2001, Az.: BVerwG 1 D 47.00).

Eine Verurteilung wegen Diebstahl in 15 Fällen wurde unterhalb der Eintragungsschwelle geahndet.

Bundesverwaltungsgericht

#### 1.3.1.2. Mangelnde Transparenz in Bezug auf Haus- und Hofverbote

Zudem wird in der Praxis bei Vorfällen wie Diebstahl oder systematischer Unterschlagung regelmäßig ein Haus- und Hofverbot ausgesprochen und das Arbeitsverhältnis beendet – allerdings ohne offizielle oder übergreifende Dokumentation. Eine Abfrage beim früheren Arbeitgeber ist nur möglich, wenn der neue Arbeitgeber den tatsächlichen Namen des vorherigen Unternehmens kennt. Fahrer, die diese Information bewusst verschleiern oder falsche Angaben machen (etwa durch Nennung eines Komplizen), können diesen informellen Schutzmechanismus gezielt umgehen. Darüber hinaus besteht die Möglichkeit, dass der frühere Arbeitgeber hierüber keine Auskunft erteilt.

#### 1.3.1.3. Früher praktiziertes Blacklist Sharing ist mittlerweile verboten

Ein pauschales, firmenübergreifendes Blacklist Sharing personenbezogener Negativdaten, wie es früher teils informell oder ohne tragfähige Rechtsgrundlage praktiziert wurde, ist seit Einführung der DSGVO regelmäßig unzulässig. Denn personenbezogene Daten dürfen nur „für festgelegte, eindeutige und legitime Zwecke erhoben“ werden und müssen „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der

Verarbeitung notwendige Maß beschränkt“ sein (Art. 5 Abs. 1 lit. b und c DSGVO, EUR-Lex (Europäische Union, 2016)). Für strafrechtsnahe Negativdaten ist die Schwelle noch höher, weil die Verarbeitung personenbezogener Daten über Straftaten nur „unter behördlicher Aufsicht“ oder auf Grundlage einer ausdrücklichen unions- oder mitgliedstaatlichen Regelung zulässig ist (Art. 10 DSGVO, EUR-Lex (Europäische Union, 2016). Dass schwarze Listen ohne klare Rechtsgrundlage datenschutzrechtlich scheitern, zeigt auch die Aufsichtspraxis: Die niederländische Aufsichtsbehörde stellte bei einer Fraud Blacklist fest, es habe „no statutory basis for processing the personal data on the list“ gegeben (edpb, 2022).

#### 1.3.1.4. Löschung personenbezogener Daten bei Arbeitgeberwechsel

Ein weiteres strukturelles Problem entsteht durch die datenschutzrechtliche Speicherbegrenzung. Arbeitgeber dürfen personenbezogene Daten aus Bewerbungsverfahren, Personalakten, Gesprächsnotizen, Compliance Hinweisen oder internen Ermittlungen nur so lange speichern, wie hierfür ein konkreter rechtlicher Zweck besteht. Nach Ende des Arbeitsverhältnisses entfallen viele ursprüngliche Verarbeitungszwecke; eine weitere Speicherung ist dann nur zulässig, soweit sie etwa zur Erfüllung gesetzlicher Aufbewahrungspflichten, zur Dokumentation arbeitsrechtlich relevanter Vorgänge oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.
In der Praxis führt dies dazu, dass relevante Hinweise auf Vorfälle, Pflichtverletzungen oder interne Ermittlungen nach Ablauf der jeweiligen Zweckbindungs und Aufbewahrungsfristen aus der Personalakte entfernt oder gelöscht werden müssen. Bei einem Arbeitgeberwechsel stehen diese Informationen dem neuen Arbeitgeber regelmäßig nicht zur Verfügung, selbst wenn der Vorfall beim früheren Arbeitgeber intern dokumentiert und verifiziert wurde.

### 1.3.2. Biometrische Verifizierung allein ist nicht ausreichend

Wie in Abschnitt 1.1.3 gezeigt, spielen Identitätsbetrug, Mehrfachidentitäten und FOGD eine zentrale Rolle in modernen Täuschungskonstellationen entlang der Lieferkette. Zugleich wurde in den Abschnitten 1.3.1 und 1.3.3 deutlich, dass fehlende Transparenz und hohe Anforderungen an die datenschutzkonforme Umsetzung die wirksame Bekämpfung solcher Konstellationen zusätzlich erschweren. Vor diesem Hintergrund ist biometrische Verifizierung zwar ein wesentlicher Bestandteil moderner Identitätsprüfung, für sich genommen jedoch nicht ausreichend.

#### 1.3.2.1. Biometrische Verifizierung ist notwendige Grundlage, aber noch keine Lösung des Mehrfachidentitätsproblems

Biometrische Verfahren sind deshalb von besonderer Bedeutung, weil sie nicht nur ein vorgelegtes Dokument, sondern die vorlegende Person selbst verifizieren. Dadurch adressieren sie klassische Täuschungskonstellationen wie den Einsatz gestohlener Dokumente, Impostor Fälle und bestimmte Dokumentenfälschungen deutlich wirksamer als eine reine Sicht oder Dokumentenkontrolle. Biometrische Merkmale wie Gesicht, Iris oder

Fingerabdruck sind individuell, dauerhaft und schwer zu fälschen. Die Identität einer Person lässt sich damit unabhängig von der Dokumentenlage zuordnen. Diese Schutzwirkung wird auch international hervorgehoben. Interpol betont, dass „Criminals and terrorists often make fraudulent use of both fake and genuine identity and travel documents [...]" (Interpol, 2026). Frontex unterstreicht ergänzend: „To combat documents forgery and impostors, the only way is through an integrated approach" (Frontex, 2024).

> Die strukturelle Grenze biometrischer Verifizierung liegt darin, dass sie in der Praxis typischerweise als biometrischer 1:1-Abgleich ausgestaltet ist.
>
> ICAO

Gerade diese Schutzwirkung darf jedoch nicht zu dem Fehlschluss verleiten, biometrische Verifizierung sei allein ausreichend. Sie ist notwendig, löst aber das Problem von Mehrfachidentitäten und FOGD nicht, solange sie auf einen bloßen 1:1-Abgleich beschränkt bleibt.

#### 1.3.2.2. Der biometrische 1:1-Abgleich erfasst keine mehrfach geführten Identitäten

Die strukturelle Grenze biometrischer Verifizierung liegt darin, dass sie in der Praxis typischerweise als biometrischer 1:1-Abgleich ausgestaltet ist. NIST definiert Verifikation ausdrücklich als „one-to-one comparison", während Identifikation als „one-to-many comparison" gegen einen gesamten Datenbestand verstanden wird (Appendix F: Biometrics (NIST, 2002). Ein biometrischer 1:1-Abgleich prüft damit lediglich, ob die aktuell vorliegende Person zu einem einzelnen, bereits ausgewählten Datensatz passt. Nicht geprüft wird hingegen, ob dieselbe natürliche Person bereits unter einer anderen Identität im selben System oder in einem anderen Zusammenhang registriert ist.

Dass biometrische Verifizierung in Identitätsprüfungsprozessen typischerweise genau in dieser Form eingesetzt wird, zeigt auch NIST im Bereich Identity Proofing. Dort wird als biometrische Verifikationsmethode ausdrücklich „Comparing the applicant's facial image to a facial portrait on evidence via an automated comparison" genannt, also der Abgleich des Livebilds mit dem Portrait auf dem vorgelegten Nachweis (NIST SP 800-63-4, Identity Proofing Requirements (NIST, 2026). In den meisten Kontrollumgebungen wird damit nur geprüft, ob eine Person mit dem vorgelegten Datensatz übereinstimmt, nicht jedoch, ob dieselbe Person bereits unter einer anderen Identität im Bestand vorhanden ist.

#### 1.3.2.3. Ohne 1:n-Abgleich bleiben Mehrfachidentitäten strukturell möglich

Genau hierin liegt die zentrale Grenze im vorliegenden Zusammenhang. Identitätsdaten liegen in verschiedenen Organisationen und Plattformen häufig isoliert nebeneinander, ohne dass eine übergreifende Verknüpfung oder ein systematischer Abgleich erfolgt. Interpol beschreibt Identitätsbetrug ausdrücklich als grenzüberschreitendes Phänomen, bei dem Täter unterschiedliche nationale Systeme ausnutzen (Interpol, 2026). Fehlt ein entsprechender Abgleich, können parallele Identitäten in

unterschiedlichen Registern oder Systemen bestehen bleiben.

> Interpol beschreibt Identitätsbetrug ausdrücklich als grenzüberschreitendes Phänomen, bei dem Täter unterschiedliche nationale Systeme ausnutzen.
>
> Interpol, 2026

Für transportbezogene Kriminalität ist dies operativ besonders relevant. In der Logistik werden Fahrer häufig in unterschiedlichen Subunternehmerketten, Auftragnehmerportalen und Flottenmanagementsystemen geführt, die weder technisch interoperabel sind noch ihre Referenzdaten miteinander abgleichen.

Dadurch bleibt es realistisch möglich, dass dieselbe Person in verschiedenen Zusammenhängen unter unterschiedlichen Identitäten erscheint und von den jeweiligen lokalen Prüfprozessen akzeptiert wird. Fälle aus der Praxis zeigen, dass Täter nicht nur Dokumente manipulieren, sondern gezielt Identitäten wechseln oder unterschiedliche Identitätsprofile nutzen, um Entdeckungsrisiken entlang der Lieferkette zu verringern. „Gangs are using impersonation and document forgery to carry out heists“ (Gallagher, 2025).

#### 1.3.2.4. FOGD zeigt besonders deutlich, warum ein 1:1-Abgleich nicht genügt

Besonders deutlich wird die Grenze des 1:1-Abgleichs bei FOGD. Dabei handelt es sich nicht um gefälschte, sondern um echte, amtlich ausgestellte Dokumente, die auf betrügerischer Grundlage erlangt wurden (siehe „Fraudulently obtained genuine documents“ (Interpol, 2026)).

Gerade darin liegt die besondere Schwierigkeit: Das Dokument ist formal echt, enthält echte Sicherheitsmerkmale und kann deshalb reguläre Echtheitsprüfungen bestehen. Auch der biometrische 1:1-Abgleich kann in einer solchen Konstellation technisch korrekt positiv ausfallen, obwohl die zugrunde liegende Identität materiell falsch ist. Die Prüfung bestätigt dann lediglich, dass die vorlegende Person zu genau dem Datensatz passt, den sie gerade verwendet. Sie prüft jedoch nicht, ob dieselbe Person bereits unter einer anderen Identität erfasst wurde.

Diese strukturelle Grenze zeigt sich nicht nur systemübergreifend, sondern auch innerhalb desselben Systems. Wenn dieselbe natürliche Person dort unter mehreren Identitäten erfasst ist, kann der 1:1-Abgleich jede dieser Identitäten für sich genommen formal korrekt bestätigen. Die Prüfung bleibt deshalb auch dann unauffällig, wenn mehrere Identitäten derselben Person nebeneinander bestehen.

Der biometrische 1:1-Abgleich schützt daher nicht zuverlässig vor Mehrfachidentitäten oder FOGD, sofern dieselbe natürliche Person unter mehreren Identitätsprofilen geführt wird.

#### 1.3.2.5. Die Fachliteratur verlangt zur Sicherung der Einzigartigkeit einen Abgleich gegen den Bestand

Dass die entscheidende Grenze im Fehlen eines bestandsbezogenen Abgleichs liegt, verdeutlicht auch die grundlegende Unterscheidung zwischen biometrischer Verifikation und Identifikation. Die Weltbank beschreibt Verifikation als Bestätigung eines biometrischen Anspruchs

durch „a one-to-one (1:1) comparison“, während die Sicherstellung der Einzigartigkeit einer Person einen Abgleich gegen den Bestand erfordert. Internationale Analysen zu digitalen Identitätssystemen betonen insoweit übereinstimmend, dass die Verhinderung von Mehrfachidentitäten belastbare Deduplication Verfahren voraussetzt.

Die Weltbank hebt hervor, dass Identitätssysteme „reliable deduplication mechanisms“ benötigen, um die Einzigartigkeit einer Person sicherzustellen.

World Bank

Die Weltbank hebt hervor, dass Identitätssysteme „reliable deduplication mechanisms“ benötigen, um die Einzigartigkeit einer Person sicherzustellen (ID4D Practitioner’s Guide (The World Bank, 2019). Auf ihrer Fachseite zu biometrischen Daten beschreibt sie Deduplication als den Abgleich eines neu erfassten biometrischen Datensatzes mit allen oder einem relevanten Teil der bereits gespeicherten biometrischen Templates, um Doppelregistrierungen zu erkennen (The World Bank, 2019, S. 122).

#### 1.3.2.6. Erforderlich ist ein kontinuierlicher 1:n-Abgleich

Hinzu kommt, dass Mehrfachidentitäten nicht nur einmalig entstehen, sondern durch spätere Nachregistrierungen, erneute Onboardings und neue Dokumentenvorlagen fortlaufend aufgebaut werden können. Wenn dieselbe Person später unter abweichenden Identitätsangaben erneut erscheint, muss dies anhand gleichbleibender personenbezogener Merkmale erkennbar bleiben. Daraus folgt, dass nicht irgendein einmaliger Abgleich genügt, sondern ein kontinuierlicher 1:n-Abgleich erforderlich ist.

Erforderlich ist ein kontinuierlicher 1:n-Abgleich, um dieselbe natürliche Person auch dann wiedererkennen zu können, wenn sie unter abweichenden Identitätsangaben erneut erscheint.

Die Erforderlichkeit eines solchen fortlaufenden Abgleichs wird zusätzlich durch neuere Täuschungsformen verstärkt. Die zunehmende Nutzung künstlicher Intelligenz zur Generierung biometrisch plausibler Fälschungen, etwa durch Deepfakes, Morphing oder synthetische Identitäten, schafft eine neue Bedrohungsebene. Moderne biometrische Systeme mit Liveness Detection und Anti Spoofing sind daher essenziell, um auch diese Täuschungsversuche zu erkennen. „AI spoofing [...] uses advanced algorithms to create realistic deepfakes in which false biometrics are presented to security systems“ (Biometrics Research Group, 2024).

#### 1.3.2.7. Die praktische Herausforderung liegt in der technisch und rechtlich belastbaren Umsetzung

Gleichzeitig ist ein solcher weitergehender Abgleich technisch und rechtlich anspruchsvoll. NIST beschreibt Identifikation als „the process of matching a biometric record from a single subject probe against an entire database“ (NIST, 2002, Appendix F: Biometrics). Mit wachsender Datenbankgröße steigen die technischen Anforderungen und zugleich die statistischen Fehlerrisiken. Parallel unterliegt die Verarbeitung biometrischer Daten in

Europa einem erhöhten datenschutzrechtlichen Schutzniveau, weil es sich nach Art. 9 DSGVO um besondere Kategorien personenbezogener Daten handelt (2016/679, Art. 9 (Europäische Union, 2016)).

#### 1.3.2.8. Fazit: Erforderlich ist ein kontinuierlicher 1:n-Abgleich

Als Zwischenergebnis ist daher festzuhalten: Biometrische Verifizierung ist notwendig, aber nicht hinreichend. Sie erhöht die Sicherheit gegenüber klassischer Dokumentenprüfung erheblich, verhindert jedoch weder FOGD noch Mehrfachidentitäten zuverlässig, solange sie auf einen bloßen 1:1-Abgleich beschränkt bleibt. Erforderlich ist deshalb ein kontinuierlicher 1:n-Abgleich, um dieselbe natürliche Person auch dann wiedererkennen zu können, wenn sie unter abweichenden Identitätsangaben erneut erscheint.

### 1.3.3. Mangelnde Fähigkeit die benötigte Transparenz datenschutzkonform herzustellen

Die praktische Hürde großer Unternehmen liegt heute oft nicht im fehlenden Sicherheitsinteresse, sondern darin, dass Datenschutztechnologie regelmäßig nicht zu ihrem Kerngeschäft gehört.

**Herausforderung:**

„bridging the gap between the legal framework and the available technological implementation measures“

enisa,2014

Konzerne sind auf Logistik, Produktion, Handel, Mobilität oder Dienstleistungen spezialisiert, nicht darauf, juristisch, organisatorisch und technologisch neue Modelle für den datenschutzkonformen Umgang mit Negativdaten, Verdachtsdaten und unternehmensübergreifenden Warnmechanismen zu entwickeln und operativ belastbar auszurollen. Genau deshalb werden sinnvolle Sicherheitsmechanismen unter DSGVO Bedingungen häufig nicht weiterentwickelt, obwohl ihr Schutzbedarf anerkannt ist. Die EDPB stellt klar, dass Betrugsprävention zwar ein legitimes Interesse sein kann, dies aber „does not mean [...] that it is automatically possible to rely on Article 6(1)(f) GDPR as a legal basis“ und dass dafür strenge „necessity and balancing tests“ zu erfüllen sind. Gleichzeitig verlangt die DSGVO „appropriate technical and organisational measures“ für eine rechtmäßige und sichere Verarbeitung personenbezogener Daten (edpb, 2024).

Das eigentliche Problem ist damit weniger ein Mangel an Problembewusstsein als ein Mangel an spezialisierter Umsetzungsfähigkeit. ENISA beschreibt die zentrale Herausforderung ausdrücklich als „bridging the gap between the legal framework and the available technological implementation measures“ (enisa, 2014).

Wo diese Brücke aus Datenschutzexpertise, Datenarchitektur, Governance und geeigneter Technologie fehlt, werden sicherheitsrelevante Maßnahmen oft nicht innovativ und datenschutzkonform neu aufgesetzt, sondern aus Rechtsunsicherheit, Komplexität und Haftungsrisiko reduziert oder eingestellt. Genau darin liegt das ungenutzte Optimierungspotential vieler Konzerne.

### 1.3.4. Prüfung von Dienstleistern ist nicht ausreichend

Zusätzliche Intransparenz entsteht durch arbeitsteilige Dienstleister und Subunternehmerstrukturen. CISA definiert einen Insider ausdrücklich als „any person who has or had authorized access to or knowledge of an organization's resources" (CISA, 2023). Gleichzeitig beschreibt CISA moderne Liefer- und Dienstleistungsstrukturen als Netzwerk (CISA, 2023). Daraus folgt, dass ein externer Arbeitnehmer bei einem Dienstleister für einen Auftraggeber legitimen Zugang und Insiderwissen aufbauen und dieses für Diebstähle oder deren Begünstigung missbrauchen kann.

Dienstleisterprüfungen validieren Unternehmen, nicht zwingend die tatsächlich eingesetzte oder hinter dem Unternehmen stehende Person.

Wird diese Person später entlassen und wechselt zu einem anderen Dienstleister, der denselben Auftraggeber bedient, kann das bereits erworbene Insiderwissen fortwirken. Genau darin liegt die Grenze rein organisationsbezogener Kontrollen. Unternehmen können zwar Subunternehmer und andere Dienstleister prüfen, aber nicht sicher ausschließen, dass einzelne externe Mitarbeiter ihr Wissen nach einem Anbieterwechsel weiter nutzen. CERT weist darauf hin, dass Insider „authorized access" missbrauchen und zudem wissen, welche Informationen kritisch und schützenswert sind (SEI, 2022). Organisationsprüfungen sind deshalb notwendig, für sich genommen aber nicht hinreichend, wenn personengebundene Risiken über mehrere Dienstleisterstrukturen hinweg fortbestehen.

Auffällige Personen können unter falscher oder wechselnder Identität erneut Zugang zu sicherheitsrelevanten Lieferketten erhalten.

Kriminelle die bereits Insiderwissen aufgebaut haben können über wechselnde Dienstleister/ Subdienstleisterstrukturen erneut Zugang zu denselben Waren, Standorten oder Prozessen erhalten.

## 1.4. Ergebnis: Hauptproblem der unentdeckten Mehrfachtäter verstärkt sich und bleibt ungelöst

Die vorstehenden Ausführungen zeigen, dass sich das Sicherheitsproblem in der Logistik nicht auf einzelne Vorfälle des Frachtdiebstahls oder auf isolierte Täuschungshandlungen reduzieren lässt. Vielmehr verdichten sich die Befunde zu einem strukturellen Gesamtproblem: Personen, die bereits auffällig geworden sind oder unter falscher, wechselnder oder mehrfach genutzter Identität auftreten, können in vielen Fällen erneut Zugang zu sicherheitsrelevanten Lieferkettenpositionen erhalten, ohne zuverlässig erkannt zu werden. Genau hierin liegt das Kernproblem der unentdeckten Mehrfachtäter.

Die Bedrohungslage wird dabei aus mehreren Richtungen gleichzeitig verschärft. Erstens professionalisieren sich

Täterstrukturen erkennbar. Wie die vorstehenden Quellen zeigen, werden Frachtdiebstähle zunehmend strategisch vorbereitet, arbeitsteilig organisiert und unter Nutzung von Insiderwissen, Identitätsbetrug, Identitätswechseln und Imitation umgesetzt. Zweitens stoßen die in der Praxis verbreiteten Prüfmechanismen an strukturelle Grenzen. Weder klassische Dokumentenkontrollen noch isolierte Unternehmensprüfungen noch punktuelle biometrische 1:1 Verifikationen reichen aus, um dieselbe natürliche Person unter abweichenden Identitätsangaben, mit mehrfachen Registrierungen oder unter Nutzung formal echter, aber betrügerisch erlangter Dokumente zuverlässig wiederzuerkennen. Drittens verhindern rechtliche und organisatorische Rahmenbedingungen häufig, dass sicherheitsrelevante Erkenntnisse über Unternehmensgrenzen hinweg in belastbarer und zugleich datenschutzkonformer Weise nutzbar gemacht werden.

Gerade das Zusammenspiel dieser Faktoren führt dazu, dass sich das Problem nicht abschwächt, sondern im Gegenteil verstärkt. Wo Haus und Hofverbote nicht unternehmensübergreifend berücksichtigt werden können, wo frühere Auffälligkeiten beim Wechsel zwischen Arbeitgebern oder Dienstleisterstrukturen faktisch unsichtbar werden, wo Dokumente zwar formal geprüft, Personen aber nicht übergreifend wiedererkannt werden, bleibt für Täter ein realistischer Wiedereinstieg in die Lieferkette möglich. Dies gilt umso mehr, wenn dieselbe Person unter neuer Identität, über einen anderen Dienstleister oder nach einer erneuten Registrierung wieder erscheint. Die Schutzlücke besteht daher nicht nur im erstmaligen Erkennen eines Täuschungsversuchs, sondern vor allem in der fehlenden Fähigkeit, wiederkehrende Risikopersonen über Zeit, Unternehmen und Identitätsvarianten hinweg als dieselbe natürliche Person zu identifizieren.

Hinzu kommt, dass die beschriebenen Defizite nicht nur Sicherheitsrisiken erzeugen, sondern auch operative Fehlanreize begünstigen. Solange Unternehmen auf isolierte Einzelprüfungen beschränkt bleiben, entsteht ein Zustand, in dem erheblicher Prüfaufwand betrieben wird, ohne dass die entscheidende Sicherheitsfrage belastbar beantwortet werden kann: Ist die aktuell vor mir stehende Person tatsächlich unauffällig, oder handelt es sich um dieselbe natürliche Person, die bereits früher unter anderem Namen, mit anderen Dokumenten oder in anderem Unternehmenskontext aufgefallen ist? Genau diese Frage bleibt im Status quo vielfach unbeantwortet.

Als Zwischenergebnis ist daher festzuhalten: Das Hauptproblem moderner Frachtkriminalität liegt nicht allein in der Existenz einzelner Täter, gefälschter Dokumente oder unsicherer Prozesse. Das zentrale Problem liegt vielmehr darin, dass Mehrfachtäter trotz vorangegangener Auffälligkeiten, Identitätswechsel, Unternehmenswechsel oder formaler Neuregistrierung häufig unerkannt bleiben. Solange dieses Problem strukturell ungelöst ist, verstärken sich die bereits beschriebenen Risiken durch Insider, Fake Carrier, Identitätsbetrug und Mehrfachidentitäten fortlaufend. Die bestehenden Kontrollmechanismen reduzieren das Problem daher nicht in

ausreichendem Maße, sondern lassen die maßgebliche Schutzlücke bestehen. Gerade daraus ergibt sich die Notwendigkeit eines Lösungsansatzes, der nicht nur einzelne Dokumente oder einzelne Unternehmen prüft, sondern die Person selbst übergreifend, fortlaufend und belastbar in den Blick nimmt.

## 2. Compliance Efficiency: Logistiker kämpfen mit hohem Aufwand

Die regelmäßige Prüfung von Führerscheinen, Ausweisdokumenten und Aufenthaltstiteln ist in der gewerblichen Logistik nicht nur rechtlich geboten, sondern auch mit erheblichem organisatorischem Aufwand verbunden. Dieser betrifft sowohl das einsetzende Unternehmen als auch die betroffenen Fahrer, insbesondere wenn diese aus Drittstaaten stammen und in Dienstleister- und/oder Subunternehmerstrukturen eingebunden sind.

### 2.1. Pflicht zur regelmäßigen Überprüfung der dienstbezogenen Dokumente

Für Unternehmen mit eigener Fahrerflotte oder regelmäßig eingesetztem Fahrpersonal ergibt sich eine klare arbeits- und haftungsrechtliche Verpflichtung zur systematischen Kontrolle relevanter Personaldokumente.

#### 2.1.1. Pflicht zur Kontrolle der Fahrerlaubnis

Im Folgenden wird auf die Pflicht der Kontrolle der Fahrerlaubnis genauer eingegangen.

##### 2.1.1.1. Pflicht zur Kontrolle der Fahrerlaubnis eigener Mitarbeiter

Arbeitgeber, die ihren Beschäftigten Fahrzeuge überlassen, unterliegen der sog. Halterverantwortung, die sich aus § 21 des Straßenverkehrsgesetzes (StVG) ableitet. Diese Vorschrift stellt es unter Strafe, das Führen eines Kraftfahrzeugs durch eine Person zuzulassen, die keine gültige Fahrerlaubnis besitzt.

Erforderlichkeit der regelmäßigen Kontrolle der Fahrerlaubnis.

Haftungsrisiko & Aufwand

Der Gesetzgeber sieht hierfür eine Freiheitsstrafe von bis zu einem Jahr oder eine Geldstrafe vor (§ 21 Abs. 1 Nr. 2 StVG). Daraus folgt in der Praxis: Selbst wenn der Führerschein zu Beginn des Arbeitsverhältnisses einmalig vorgelegt wurde, reicht dies nicht aus, um dauerhafte Rechtssicherheit zu gewährleisten. Fahrer können ihre Fahrerlaubnis im Verlauf der Beschäftigung verlieren – etwa infolge von Verkehrsverstößen, Fahrverboten, medizinischen Einschränkungen oder strafrechtlichen Maßnahmen.

Der Arbeitgeber muss daher durch ein geeignetes und dokumentiertes Kontrollsystem sicherstellen, dass alle eingesetzten Fahrer auch während ihrer gesamten aktiven Tätigkeit über eine gültige Fahrerlaubnis verfügen. Fachverbände und Kammern empfehlen ausdrücklich regelmäßige Führerscheinkontrollen – typischerweise in Intervallen von drei bis sechs Monaten. Die Handwerkskammer Heilbronn hält fest: „Überlassen

Arbeitgeber ihren Mitarbeitern Fahrzeuge, müssen sie regelmäßig überprüfen, ob die Mitarbeiter über die erforderliche Fahrerlaubnis verfügen“ (Handwerkskammer Heilbronn-Franken, 2021).

Wer Fahrzeuge bereitstellt oder den Einsatz ermöglicht, muss die Fahrerlaubnis prüfen.

2.1.1.2. Pflicht zur Überprüfung der Fahrerlaubnis eingesetzter selbstständiger Fahrer bei Operativer Kontrolle

Bei selbstständigen, dienstleisterbezogenen oder leasinggestützten Fahrermodellen richtet sich die Pflicht zur Fahrerlaubniskontrolle nicht allein nach der Vertragsform, sondern danach, wer das Fahrzeug rechtlich und wirtschaftlich zugeordnet bekommt und dessen Einsatz tatsächlich ermöglicht oder kontrolliert. § 21 StVG erfasst ausdrücklich denjenigen, der „als Halter eines Kraftfahrzeugs anordnet oder zulässt, dass jemand das Fahrzeug führt“ (§ 21 Abs. 1 Nr. 2 StVG).

Nach dem BGH ist Halter, wer das Fahrzeug „für eigene Rechnung in Gebrauch hat“ und die erforderliche „Verfügungsgewalt besitzt“ (BGH, Urteil vom 10.07.2007, VI ZR 199/06 (Bundesgerichtshof, 2007)).

Dies kann auch Unternehmen erfassen: „Halter sind auch Unternehmen, wenn sie Firmenfahrzeuge auf eigene Rechnung in Gebrauch haben“ (BayObLG, Beschluss vom 07.11.2022, 203 StRR 420/22 (Bayerische Staatskanzlei, 2022)). Daraus folgt eine Prüfverantwortung besonders dort, wo ein Unternehmen Fahrzeuge stellt, die Überlassung veranlasst oder den konkreten Einsatz organisatorisch prägt. Vor der Überlassung ist zu prüfen, ob der Fahrer die erforderliche Fahrerlaubnis besitzt; das BayObLG verlangt eine Kontrolle „vor der Fahrzeugüberlassung“ (BayObLG, Beschluss vom 07.11.2022, 203 StRR 420/22 (Bayerische Staatskanzlei, 2022)).

### 2.1.2. Pflicht zur Kontrolle der Arbeitserlaubnis

Im Folgenden wird auf die Pflicht der Kontrolle der Arbeitserlaubnis genauer eingegangen.

2.1.2.1. Pflicht zur kontinuierlichen Kontrolle der Arbeitserlaubnis in Bezug auf eigene Mitarbeiter

Bei eigenen Mitarbeitern besteht die Pflicht zur Kontrolle der Arbeitserlaubnis nicht nur einmalig bei der Einstellung, sondern während der gesamten Dauer der Beschäftigung. Das ergibt sich aus § 4a Abs. 5 AufenthG. Danach muss der Arbeitgeber prüfen, ob die Voraussetzungen für die Beschäftigung vorliegen, und „für die Dauer der Beschäftigung eine Kopie des Aufenthaltstitels, der Arbeitserlaubnis der Bundesagentur für Arbeit oder der Bescheinigung über die Aufenthaltsgestattung oder über die Aussetzung der Abschiebung des Ausländers in elektronischer Form oder in Papierform aufbewahren“ (Bundesamt für Justiz, 2004).

Da diese Unterlagen für die gesamte Beschäftigungsdauer vorzuhalten sind, genügt eine bloße Anfangskontrolle nicht;

vielmehr muss das Unternehmen die fortbestehende Berechtigung laufend im Blick behalten. Kommt der Arbeitgeber dieser Pflicht nicht nach, drohen erhebliche Sanktionen. Die Zollverwaltung formuliert dies ausdrücklich so: „Verstößt ein Arbeitgeber gegen diesen Grundsatz, kann dies eine Geldbuße von bis zu 500.000 € nach sich ziehen (siehe § 404 Abs. 2 Nr. 3 SGB III) (Zoll, 2015).

#### 2.1.2.2. Pflicht zur Prüfung der Arbeitserlaubnis von Mitarbeitern externer Dienstleister/Subunternehmer

Gerade in mehrstufigen Dienstleister-/Subunternehmerstrukturen endet die rechtliche Verantwortung zur Prüfung der Arbeitserlaubnis nicht bereits auf der Ebene des unmittelbaren Angestelltenverhältnisses.

> Wer Leistungen über Dienstleister oder Nachunternehmer erbringen lässt, kann haften, wenn dort Personen ohne erforderliche Arbeitserlaubnis eingesetzt werden.

Vielmehr knüpft das Gesetz ausdrücklich auch an Konstellationen an, in denen ein Unternehmen Leistungen nicht mit eigenem Personal, sondern über beauftragte Unternehmen oder Nachunternehmer erbringen lässt. Für den vorliegenden Zusammenhang ist deshalb § 404 Abs. 1 SGB III von zentraler Bedeutung (§ 404 SGB III). Die Norm lautet:

„Ordnungswidrig handelt, wer als Unternehmerin oder Unternehmer Dienst- oder Werkleistungen in erheblichem Umfang ausführen lässt, indem sie oder er eine andere Unternehmerin oder einen anderen Unternehmer beauftragt, von dem sie oder er weiß oder fahrlässig nicht weiß, dass diese oder dieser zur Erfüllung dieses Auftrags

1. entgegen § 284 Absatz 1 oder § 4a Absatz 5 Satz 1 oder 2 des Aufenthaltsgesetzes eine Ausländerin oder einen Ausländer beschäftigt oder
2. eine Nachunternehmerin oder einen Nachunternehmer einsetzt oder es zulässt, dass eine Nachunternehmerin oder ein Nachunternehmer tätig wird, die oder der entgegen § 284 Absatz 1 oder § 4a Absatz 5 Satz 1 oder 2 des Aufenthaltsgesetzes eine Ausländerin oder einen Ausländer beschäftigt.“

Diese Vorschrift ist für Logistikunternehmen deshalb von besonderer Relevanz, weil sie die Bußgeldverantwortung ausdrücklich auf den Auftraggeber ausdehnt, wenn Leistungen über andere Unternehmen erbracht werden und dabei ausländische Personen ohne die erforderliche aufenthaltsrechtliche Berechtigung eingesetzt werden. Der gesetzliche Fokus liegt damit nicht nur auf dem unmittelbaren Arbeitgeber, sondern auf der gesamten leistungsbezogenen Beauftragungskette. Schon der Wortlaut zeigt, dass nicht nur die direkte Beauftragung eines Unternehmens erfasst wird, sondern auch der Einsatz oder das Tätigwerden von Nachunternehmern.

Besonders bedeutsam ist in diesem Zusammenhang die Formulierung „weiß oder fahrlässig nicht weiß“. Der Auftraggeber kann also nicht nur dann belangt werden, wenn er positive Kenntnis von einem unzulässigen Einsatz hat. Ausreichend kann vielmehr bereits sein, dass er es sorgfaltswidrig unterlässt, die für den Einsatz relevanten

aufenthaltsrechtlichen Voraussetzungen in angemessener Weise zu prüfen oder sich hierzu belastbare Gewissheit zu verschaffen. Der allgemeine gesetzliche Maßstab für Fahrlässigkeit lautet: „Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt“ (§ 276 BGB).

Daraus folgt für Dienstleister- und Subunternehmerstrukturen, dass aufenthalts- und beschäftigungsrechtliche Nachweise nicht nur im Verhältnis zum eigenen Mitarbeiter rechtlich relevant sind. Sie gewinnen vielmehr auch dort Bedeutung, wo Unternehmen Leistungen arbeitsteilig über Drittunternehmen erbringen lassen und zur Auftragserfüllung konkret eingesetzte Personen nicht aus dem eigenen Personalbestand stammen. In solchen Konstellationen betrifft die Rechtslage gerade nicht nur die abstrakte Zuverlässigkeit des beauftragten Unternehmens, sondern die Frage, ob die tatsächlich eingesetzten ausländischen Personen rechtmäßig beschäftigt werden und ob die hierfür maßgeblichen Nachweise vorhanden und belastbar sind. Dies ergibt sich aus dem Zusammenspiel von § 404 Abs. 1 SGB III und § 4a Abs. 5 AufenthG (§ 404 SGB III; § 4a AufenthG).

Die Zollverwaltung bringt die auftraggeberseitige Verantwortung ausdrücklich auf den Punkt: „Auch ein Auftraggeber kann unter Umständen bußgeldrechtlich belangt werden, wenn ein Nachunternehmer ausländische Arbeitnehmerinnen und Arbeitnehmer unerlaubt einsetzt. Dies ist der Fall, wenn er weiß oder fahrlässig nicht weiß, dass der Nachunternehmer zur Erfüllung des Auftrags unerlaubt Ausländerinnen und Ausländer beschäftigt oder wiederum Nachunternehmen einsetzt oder zulässt, dass Nachunternehmen tätig werden, die unerlaubt Ausländerinnen und Ausländer beschäftigen“ (Zoll, 2015).

Der Bußgeldrahmen für Unternehmen ist erheblich. § 404 Abs. 3 SGB III bestimmt: „Die Ordnungswidrigkeit kann in den Fällen der Absätze 1 und 2 Nummer 3 mit einer Geldbuße bis zu fünfhunderttausend Euro [...] geahndet werden“ (§ 404 SGB III). Damit handelt es sich nicht um eine bloße Nebenpflicht von untergeordneter praktischer Relevanz, sondern um ein rechtlich und wirtschaftlich wesentliches Risiko entlang der gesamten Beauftragungsstruktur.

#### 2.1.2.3. Pflicht zur Kontrollfähigen Vorhaltung der Arbeitserlaubnis bei Zoll und FKS-Prüfungen

Bei Prüfungen durch den Zoll ist für Arbeitgeber insbesondere die aufenthaltsrechtliche Dokumentationspflicht relevant, wenn ausländische Beschäftigte eingesetzt werden.

Aufenthaltstitel und Arbeitserlaubnis müssen bei Zollprüfungen vorliegen. Bußgelder bis zu:

**500.000 €**

Zoll, 2015

Das Aufenthaltsgesetz formuliert dies ausdrücklich. § 4a Abs. 5 AufenthG bestimmt, dass ein: „Arbeitgeber einen Ausländer nur beschäftigen oder mit der Erbringung einer entgeltlichen Dienst- oder Werkleistung beauftragen darf, wenn dieser einen Aufenthaltstitel besitzt. Der Arbeitgeber ist verpflichtet, für

die Dauer der Beschäftigung eine Kopie des Aufenthaltstitels, der Arbeitserlaubnis der Bundesagentur für Arbeit oder der Bescheinigung über die Aufenthaltsgestattung oder über die Aussetzung der Abschiebung in elektronischer Form oder in Papierform aufzubewahren“ (§ 4a AufenthG).

Diese Unterlagen sind im Prüfungsfall vorzulegen. § 4 SchwarzArbG stellt klar, dass das Prüfungsrecht des Zolls nicht an einer bestimmten Form der Unterlagen scheitert. Die Norm lautet: „Das Recht zur Einsichtnahme besteht in Bezug auf die Unterlagen und Daten nach Satz 1 unabhängig von deren Format, Aufbewahrung und Speicherung“ (§ 4 SchwarzArbG).

Für die Sanktion nennt der Zoll auch hier den einschlägigen Bußgeldrahmen: „Verstößt ein Arbeitgeber gegen diesen Grundsatz, kann dies eine Geldbuße von bis zu 500.000 € nach sich ziehen“ (siehe § 404 Abs. 2 Nr. 3 SGB III) (Zoll, 2015).

| RECHTLICH RELEVANTE DOKUMENTEN- UND NACHWEISPFLICHTEN | | | | | |
|---|---|---|---|---|---|
| Sanktionsrahmen und Risikoeinordnung für Logistikunternehmen | | | | | |
| **PFLICHT** | **RECHTSQUELLE** | **INHALT** | **SANKTIONSRAHMEN** | | **BEWERTUNG** |
| BEZEICHNUNG | PARAGRAPHEN | ERKLÄRUNG | UNTERNEHMEN | FAHRER | RISIKO |
| Fortlaufende Prüfung der Fahrerlaubnis | § 21 StVG | Die Fahrerlaubnis ist nicht nur beim Erstkontakt, sondern fortlaufend zu prüfen, wenn sich die Berechtigungslage im Zeitverlauf ändern kann. | Freiheitsstrafe bis 1 Jahr oder Geldstrafe | Freiheitsstrafe bis 1 Jahr oder Geldstrafe | hoch |
| Arbeits und Aufenthalts-berechtigung | § 4a AufenthG<br>§ 404 SGB III<br>§ 95 AufenthG | Beschäftigungsberechtigung ist zu prüfen; einschlägige Dokumente sind während der Beschäftigung aktuell vorzuhalten. | Bußgeld bis 500.000 € | Freiheitsstrafe bis 1 Jahr oder Geldstrafe; zusätzlich bis 5.000 € | sehr hoch |
| Reisepass und Personal-ausweis als Pflicht-dokumente | § 2a SchwarzArbG | Im Speditions-, Transport- und Logistikgewerbe bestehen Mitführungs- und Vorlagepflichten sowie eine Hinweispflicht des Arbeitgebers. | Bußgeld bis 50.000 € | Bußgeld bis 5.000 € | mittel bis hoch |
| Kontrollfähige Vorhaltung bei Zoll und FKS | § 4 SchwarzArbG | Dokumente müssen im Prüfungsfall kurzfristig, geordnet und nachvollziehbar verfügbar sein. | Bußgeld bis 50.000 € je nach Tatbestand | Bußgeld bis 5.000 € je nach Tatbestand | hoch |
| Fahrerqualifizie-rungsnachweise sowie Schulungs- und Zertifikats-nachweise | § 8, § 28 BKrFQG | Qualifikations- und Schulungsnachweise sind fortlaufend prüf und vorlagefähig zu halten. | Bußgeld bis 20.000 € | Bußgeld bis 20.000 € | hoch |
| Dokumenten-pflichten in OSP und Subunterne-hmerstrukturen | § 404 SGB III | Dokumentenbezogene Nachweise sind auch in mehrstufigen OSP und Subunternehmerstrukturen rechtlich relevant. | Bußgeld bis 500.000 € | abhängig von der konkreten Fallkonstellation | sehr hoch |
| Pass und Aufenthalts-dokumente im gewerblichen Güterkraft-verkehr | § 7b, § 19 GüKG | Pass- und Aufenthaltsdokumente sind in einschlägigen Transportkonstellationen einsatzrelevante Pflichtdokumente. | Bußgeld bis 20.000 € | Bußgeld bis 20.000 € | hoch |
| Datenschutz bei Kopie, Scan, Speicherung und Löschung | Art. 5, 17, 25, 32, 83 DSGVO<br>§ 20 PAuswG | Mehrfachkopien und dezentrale Vorhaltung sensibler Dokumente können zu einem unkontrollierten Mehrfachbestand führen. | Bis 20 Mio. € oder 4% des weltweiten Jahresumsatzes | typischerweise keine gleichartige Sanktion als betroffene Person | systemisch sehr hoch |

Tabelle 1: Sanktionsrahmen und Risikobewertung für rechtlich relevante Dokumenten- und Nachweis-pflichten.

### 2.1.3. Mitwirkungspflicht der Fahrer

Auch der Fahrer selbst wird vom Sanktionsrahmen erfasst und ist zur Mitwirkung verpflichtet.

2.1.3.1. In Bezug auf die Arbeitserlaubnis

§ 7b GüKG verlangt unter anderem einen „anerkannten und gültigen Pass, Passersatz oder Ausweisersatz“ sowie den erforderlichen aufenthaltsrechtlichen Nachweis oder eine entsprechende Fahrerbescheinigung. Verstöße gegen das GüKG sind nach § 19 GüKG bußgeldbewehrt; je nach Tatbestand reichen die Bußgeldrahmen bis zu 20.000 €, die der Fahrer zu tragen hat.

Fahrer, die keine deutsche Staatsangehörigkeit besitzen, dürfen nur dann eine Beschäftigung ausüben, wenn sie im Besitz einer gültigen Arbeitserlaubnis oder eines entsprechenden Aufenthaltstitels mit Erwerbserlaubnis sind. Das Aufenthaltsgesetz sieht in § 95 strafrechtliche Folgen vor, wenn sich ein Ausländer ohne den erforderlichen Aufenthaltstitel im Bundesgebiet aufhält oder bestimmte aufenthaltsrechtliche Verstöße begeht. Der Strafrahmen beträgt dabei grundsätzlich Freiheitsstrafe bis zu einem Jahr oder Geldstrafe; in schwereren Fällen, etwa bei Verstößen gegen ein Einreise- oder Aufenthaltsverbot, kann Freiheitsstrafe bis zu drei Jahren oder Geldstrafe drohen (§ 95 AufenthG).

2.1.3.2. In Bezug auf den Führerschein

Fahrer sind zur Mitwirkung an diesen Überprüfungen verpflichtet und setzen sich beim Fahren ohne Führerschein erheblichen, auch rechtlichen Risiken aus. Das Führen eines Kraftfahrzeugs ohne gültige Fahrerlaubnis ist gemäß § 21 des Straßenverkehrsgesetzes (StVG) eine Straftat. Dort heißt es: „Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer ein Kraftfahrzeug führt, obwohl er die dazu erforderliche Fahrerlaubnis nicht hat“ (§ 21 Abs. 1 Nr. 2 StVG).

Fahrer müssen Arbeitserlaubnis und Führerschein gültig nachweisen können. Bei Verstößen drohen Bußgelder, Geldstrafe oder Freiheitsstrafe.

Wie der ADAC erläutert, handelt es sich dabei nicht um eine Ordnungswidrigkeit, sondern: „Wer trotz Fahrverbots oder Entzugs der Fahrerlaubnis Auto fährt, begeht eine Straftat. Im schlimmsten Fall droht eine Haftstrafe“ (ADAC, 2024). Daraus ergibt sich für jeden Fahrer die Pflicht, vor jeder gewerblichen Fahrt sicherzustellen, dass seine Fahrerlaubnis uneingeschränkt gültig ist und den gesetzlichen Anforderungen entspricht.

## 2.2. Aufwand, Grenzen und Risiken bisher üblicher Prüfverfahren

Die vorstehend dargestellten Dokumenten und Nachweispflichten zeigen, dass Unternehmen in der gewerblichen Logistik eine Vielzahl wiederkehrender Prüf- und Dokumentationsprozesse organisieren müssen, um nicht Gefahr zu laufen, die vom Gesetzgeber im jeweils definierten Sanktionsrahmen vorgesehenen Strafen zu tragen.

Dies betrifft nicht nur eigene Fahrer, sondern auch externe Einsatzmodelle, Dienstleister und

Subunternehmerstrukturen, insbesondere bei ausländischem Fahrpersonal mit zusätzlichen aufenthalts- und dokumentationsrechtlichen Anforderungen. In der Praxis werden diese Pflichten jedoch vielfach noch mit manuellen Sicht-, Fristen- und Ablageprozessen erfüllt. Genau hierin liegt ein zentrales Problem: Diese Verfahren sind nicht nur organisatorisch und zeitlich aufwendig, sondern auch inhaltlich nicht dazu geeignet, die in Kapitel 0 beschriebenen modernen Betrugs- und Täuschungskonstellationen zu erkennen, und führen zu Data Spreading, und somit zu erheblichen rechtlichen Haftungsrisiken für die beteiligten Unternehmen.

### 2.2.1. Hoher Aufwand

In der Praxis bedeutet dies, dass Personalverantwortliche in Bezug auf Mitarbeiter:

- Prüfzyklen definieren und überwachen (z. B. alle drei bis sechs Monate),
- Termine mit Fahrern koordinieren,
- Kommunikation in Bezug auf fehlende Dokumente betreiben,
- Gültigkeit und Echtheit visuell oder technisch überprüfen und
- interne Ablagestrukturen auf dem neuesten Stand halten müssen.

Sicht-, Fristen- und Ablageprozesse binden Personal. Bei jedem Fahrer, jedem Nachweis und jeder Wiederholungsprüfung.

Gerade bei Unternehmen mit hoher Fahrerfluktuation, mehreren Standorten oder internationalem Personal kann diese manuelle Prozesskette erhebliche Ressourcen binden. Auch für die betroffenen Fahrer ist der wiederholte Dokumentennachweis mit Herausforderungen verbunden. Sie müssen:

- Terminabsprachen mit dem Unternehmen treffen und diese Termine einhalten,
- etwaige Sprachbarrieren überwinden, um den Zweck der Prüfung zu verstehen, und
- ggf. Formulare unterschreiben oder Erklärungen abgeben.

Hinzu kommen die Prüfungen an Fahreranmeldungen, bei denen oft Ausweise gescannt oder kopiert werden und/oder bei denen sich Fahrer in Listen eintragen, was zeitlichen Aufwand aufseiten der Fahrer und des eingesetzten Personals verursacht, nicht selten zu Warteschlangen vor Fahreranmeldungen führt und Logistische Prozesse verzögert.

Manuelle Prüfungen sind fehleranfällig und erkennen moderne Fälschungen oder Täuschungsfälle oft nicht zuverlässig. Besonders bei FOGD.

### 2.2.2. Mangelnde Wirksamkeit

Trotz dieses Aufwands sind die Prüfungen weder zuverlässig noch sicher. Die Sichtkontrolle oder manuelle Dokumentenprüfung selbst durch geschultes Personal kann die Vielzahl moderner Fälschungstechniken, Morphing oder hochwertig gefälschte Ausweise – in der Regel nicht erkennen.

FOGD kann wie beschrieben nicht einmal durch die besten Dokumentenprüfgeräte

(der Bundesdruckerei) erkannt werden, da der Betrug nicht auf Basis des Dokuments selbst, sondern bereits vorgelagert auf Basis des Breeder Documents erfolgt.

### 2.2.3. Rechtliche Risiken

Die Registrierung von Fahrern an Übergabepunkten, Werkstoren und Sicherheitszonen ist in der Logistik noch immer vielerorts Teil der betrieblichen Praxis. Das zeigt sich etwa in operativen Warehouse Prozessen der Kühlkettenlogistik: Die Global Cold Chain Alliance beschreibt den Wareneingang mit den Worten: „When the delivery vehicle arrives, the driver will present a Bill of Lading (BOL)“ und ergänzt ausdrücklich: „As a precaution against theft, some warehouses ask for and make a copy of the driver’s license“ (GCCA, 2018).

Ergänzend finden sich in europäischen Fahrerforen anekdotische Praxisberichte, wonach bei einzelnen Firmen „auch die Dokumente des Fahrers kopiert werden“ und ausdrücklich „Ausweise (FS, Pass)“ betroffen sein können (Trucker Forum, 2016). Fahrerunterlagen werden an Übergabepunkten nicht immer nur vorgezeigt, sondern fallweise auch kopiert, gescannt, lokal gespeichert oder in Papierform abgelegt. Rechtlich problematisch wird dies dann, wenn aus einer Vielzahl einzelner Erfassungen ein signifikanter Mehrfachbestand sensibler Dokumente entsteht. Diese Verteilung identischer Dokumentenkopien über viele Stellen lässt sich beschreibend als Data Spreading bezeichnen.

Die Zulässigkeit solcher Vorgänge ist rechtlich eng begrenzt. Das Personalausweisportal des Bundes weist ausdrücklich darauf hin: „Ausweiskopien sind mit Ihrem Einverständnis erlaubt.“ Zugleich wird empfohlen, nicht erforderliche Angaben zu schwärzen, was in der Praxis in der Regel an Fahreranmeldungen nicht erfolgt. Auf Ebene der DSGVO gelten darüber hinaus die Grundsätze der Datenminimierung und Speicherbegrenzung. Art. 5 DSGVO verlangt, dass personenbezogene Daten „adequate, relevant and limited to what is necessary“ sein müssen. Art. 17 DSGVO fordert die Löschung „without undue delay“, wenn Daten für den Zweck nicht mehr erforderlich sind. Art. 25 DSGVO verlangt datenschutzfreundliche Voreinstellungen, und Art. 32 DSGVO fordert „appropriate technical and organisational measures“. Je stärker identische Ausweis, Pass, Führerschein oder Aufenthaltsdokumente über verschiedene Standorte, Ordner, Laufwerke und Postfächer verteilt werden, desto schwieriger wird die Einhaltung genau dieser Grundprinzipien (EU-DSGVO).

Verteilte Ausweis- und Fahrerdokumente schaffen DSGVO-Risiken. Bußgelder bis zu:

**20 Mio. €**

EU-DSGVO

Der Sanktionsrahmen ist erheblich. Art. 83 DSGVO sieht für Verstöße gegen zentrale Grundprinzipien und Betroffenenrechte Geldbußen von bis zu 20 Mio. € oder „up to 4 % of the total worldwide annual turnover“ vor. Daraus folgt nicht, dass jede einzelne vergessene Ausweiskopie automatisch zu einer Höchstbuße

führt. Daraus folgt aber sehr wohl, dass Unternehmen, die dokumentenintensive Fahreranmeldungen oder vergleichbare Prozesse selbst betreiben, veranlassen oder dulden und dabei systematisch gegen Datenminimierung, Löschung, Zugriffsbeschränkung oder Sicherheitsanforderungen verstoßen, ein Bußgeldrisiko in genau diesem gesetzlichen Rahmen eröffnen können. Für Unternehmensgruppen kann die maßgebliche Bezugsgröße dabei der weltweite Umsatz der wirtschaftlichen Einheit sein.

## 3. Welche Fähigkeiten bräuchte es, um diese Hauptprobleme zu lösen?

Aus dem zuvor dargestellten Befund ergibt sich, dass die beschriebenen Sicherheits- und Compliance-Risiken mit isolierten Einzelmaßnahmen nicht wirksam adressiert werden können.

Erforderlich ist vielmehr ein Lösungsansatz, der die identifizierten Schwachstellen strukturell aufgreift und sowohl sicherheitsbezogene als auch operative Anforderungen erfüllt. Im Folgenden werden daher die zentralen Fähigkeiten beschrieben, über die eine wirksame Lösung verfügen muss.

Sanktionslisten, Watchlists und Blacklists erkennen Identitätsbetrug strukturell nicht zuverlässig.

### 3.1. Fraud Detection

#### 3.1.1. FOGD-Erkennung gegen Insider, Fake Carrier, Identitätsbetrug und Mehrfachidentitäten

Wie in den Punkten 1.1.1, 1.1.2, 1.1.3, 1.3.2 und 1.4 deutlich wird, nutzen kriminelle Akteure Identitätswechsel, Mehrfachregistrierungen und auch formal echte, aber auf betrügerischer Grundlage erlangte Dokumente, um als Insider in Lieferketten einzudringen oder in Fake-Carrier-Konstellationen tätig zu werden. Deshalb muss eine wirksame Lösung in der Lage sein, nicht nur klassische Dokumentenfälschungen, sondern auch Identitätstäuschung bei formal unauffälligen Unterlagen zu erkennen.

Eine wirksame Lösung muss dieselbe natürliche Person trotz abweichender Dokumente wiedererkennen.

Eine 1:1-Prüfung reicht hier ebenso wenig aus, wie eine Beschränkung auf Sanktionslisten, AML-Screening, PEP-Listen, Watchlists, Blocklisten oder Portrait Blacklists, weil solche Mechanismen im Kern bekannte Namen, bekannte Referenzen oder bekannte Negativmerkmale prüfen, aber nicht verlässlich feststellen, ob dieselbe natürliche Person bereits unter einer anderen Identität im angeschlossenen Netzwerk aufgetreten ist. Die Lösung muss daher insbesondere folgende Fähigkeiten aufweisen:

- Erkennung von Mehrfachidentitäten und Identitätstäuschung auch dann,

wenn vorgelegte Dokumente formal echt erscheinen oder von legitimen Stellen ausgestellt wurden.
- Fähigkeit, dieselbe natürliche Person bei wiederholten Registrierungs- oder Prüfversuchen trotz abweichender Identitätsangaben wiederzuerkennen.
- Unternehmensübergreifende und fortlaufende 1:n Prüfung innerhalb des angeschlossenen Netzwerks, um Wiederauftreten unter geänderter Identität erkennbar zu machen.
- Technische oder prozessuale Verhinderung beziehungsweise Kennzeichnung mehrfacher Anmeldeversuche derselben Person.
- Erkennung und Bewertung von Identitäts- oder Rollenwechseln bei Nutzung unterschiedlicher Unterlagen oder abweichender Registrierungsdaten.
- Ausgestaltung über klassische Listen oder Referenzabgleiche hinaus, da diese FOGD und vergleichbare Täuschungskonstellationen strukturell nicht zuverlässig erfassen.

### 3.1.2. Unternehmensübergreifende Berücksichtigung von Haus- und Hofverboten

Wie in den Abschnitten 1.3.1.2, 1.3.1.3, 1.3.1.4 und 0 beschrieben, werden sicherheitsrelevante Vorfälle in der Praxis häufig durch Haus- und Hofverbote oder interne Ausschlüsse sanktioniert, ohne dass diese Information beim Wechsel zu einem anderen Unternehmen erhalten bleibt. Dadurch können bereits auffällig gewordene Personen erneut Zugang zu Waren, Standorten oder sensiblen Informationen erhalten. Eine wirksame Lösung muss solche Vorfälle deshalb unternehmensübergreifend berücksichtigen können, ohne auf unzulässiges Blacklist Sharing oder die Offenlegung sensibler Detailinformationen angewiesen zu sein. Erforderlich ist ein datenschutzkonformer, datensparsamer und statusbezogener Mechanismus, der bekannte Risikopersonen auch über Unternehmensgrenzen hinweg erkennbar macht.

### 3.1.3. Mehrstufige Verifikation

Wie in den Abschnitten 1.1.3, 1.3.2, 0 und 0 deutlich wird, reichen punktuelle Einzelprüfungen zur wirksamen Abwehr moderner Täuschungs- und Betrugsmuster nicht aus. Gerade bei FOGD, Mehrfachidentitäten, Identitätsmissbrauch und strategisch vorbereitetem Eindringen in Lieferketten entsteht ein wesentliches Risiko daraus, dass einzelne Kontrollsignale für sich genommen unauffällig erscheinen können.

Moderne Identitätstäuschung erfordert mehrstufige Prüfung aus Gerät, Biometrie, Dokumenten und Risikologik.

Erforderlich ist deshalb ein mehrschichtiger Prüfansatz, in dem verschiedene Erkenntnisquellen zusammen betrachtet werden und nicht nur ein einzelnes Merkmal über das Ergebnis entscheidet.

Die Lösung muss daher insbesondere folgende Fähigkeiten aufweisen:

- Einbeziehung sicherheitsrelevanter Merkmale des verwendeten mobilen Endgeräts, soweit diese für die Prüfung von Relevanz sind.
- Biometrische Absicherung der Personenfeststellung einschließlich

Nachweis, dass es sich um eine reale und gegenwärtig anwesende Person handelt.
- Prüfung, Auswertung und Plausibilisierung der erforderlichen Nachweise und Unterlagen.
- Technische Zusammenführung der einzelnen Prüfergebnisse in einer einheitlichen Auswertungslogik.
- Unterstützung einer belastbaren Einordnung auch dann, wenn einzelne Signale isoliert betrachtet keine eindeutige Aussage zulassen.

Für Konstellationen mit Auffälligkeiten, Widersprüchen oder fehlender Eindeutigkeit muss die Lösung zudem einen hybriden Prüfansatz unterstützen, bei dem spezialisierte Fraud oder Security Verantwortliche eingebunden werden können. Hierfür sind geeignete Funktionen erforderlich, um vertiefte manuelle Prüfungen auf Basis der bereits vorliegenden Erkenntnisse wirksam zu ermöglichen.

### 3.1.4. Verknüpfte Auswertung sicherheitsrelevanter Erkenntnisse

Wie in den Abschnitten 1.2, 1.3.1, 1.3.2 und 0 deutlich wird, liegt das Problem zum Teil auch darin begründet, dass sicherheitsrelevante Erkenntnisse häufig nebeneinanderstehen, ohne in einen konsistenten Zusammenhang gebracht zu werden. Gerade bei Wiederholungstätern, dokumentierten Auffälligkeiten, Mehrfachidentitäten oder bereits bekannten Ausschlusskonstellationen reicht es nicht aus, einzelne Ergebnisse isoliert zu betrachten. Erforderlich ist deshalb eine Lösung, die vorhandene Erkenntnisse in einer nachvollziehbaren und abgestuften Logik zusammenführt, damit aus mehreren Einzelinformationen eine belastbare sicherheitsbezogene Gesamteinordnung entstehen kann.

Erst die verknüpfte Auswertung von Identität, Dokumenten, Biometrie und Vorfällen zeigt das tatsächliche Sicherheitsbild.

Eine Trust Indikation übersetzt komplexe Prüfungen in ein klares Einsatzsignal. Ohne Detailoffenlegung.

Die Lösung muss daher insbesondere folgende Fähigkeiten aufweisen:

- Zusammenführung relevanter Resultate aus Identitätsprüfung, Dokumentenkontrolle, biometrischer Absicherung und sonstigen sicherheitsrelevanten Prüfschritten in eine einheitliche Bewertungslogik.
- Einbeziehung dokumentierter Täuschungsversuche, sicherheitsrelevanter Vorkommnisse und sonstiger belastbarer Auffälligkeiten, soweit dies datenschutzrechtlich und arbeitsrechtlich tragfähig ausgestaltet ist.
- Berücksichtigung zulässiger sachlicher Zusammenhänge innerhalb rechtlich zulässiger Organisationsstrukturen, ohne unzulässige Offenlegung oder Weitergabe wettbewerblich sensibler Informationen.
- Bildung einer abgestuften sicherheitsbezogenen Einordnung.

### 3.1.5. Trust Indikation

Wie in den Abschnitten 1.3.1, 1.3.2, 1.3.3, 1.3.4, 0 und 2.1 deutlich wird, besteht das Problem nicht nur darin, Auffälligkeiten zu erkennen, sondern auch darin, aus diesen Erkenntnissen eine operativ nutzbare und datenschutzkonforme Aussage für den konkreten Einsatz einer Person in der Supply Chain abzuleiten. Ohne eine solche Einordnung bleibt für Unternehmen häufig unklar, ob die Voraussetzungen für Zugang, Einsatz oder Weiterbeschäftigung im sicherheitsrelevanten Umfeld tatsächlich vorliegen. Zugleich darf eine solche Einordnung nicht in eine allgemeine Leistungs-, Verhaltens oder Persönlichkeitsbewertung übergehen.

Eine wirksame Lösung muss deshalb für jede erfasste Person eine datenschutzkonforme, datensparsame und operativ nutzbare Trust Indikation bereitstellen. Diese muss sich ausschließlich auf die sicherheits- und compliancebezogene Frage beziehen, ob die Voraussetzungen für den Zugang zu schützenswerten Gütern, sensiblen Informationen, kritischen Bereichen oder sicherheitsrelevanten Prozessen erfüllt sind.

Die Bewertung darf sich nur auf Security und Compliance beziehen. Nicht auf Arbeitsleistung oder persönliche Eignung.

Die Lösung muss daher insbesondere folgende Fähigkeiten aufweisen:

- Bereitstellung eines klaren, statusbezogenen Ergebnisses für jede erfasste Person.
- Ausschließliche Ausrichtung auf die sicherheits- und compliancebezogene Einsatzbewertung, nicht auf Arbeitsleistung oder allgemeine persönliche Eignung.
- Berücksichtigung betrugsrelevanter Auffälligkeiten und sonstiger sicherheitsbezogener Hinweise.
- Berücksichtigung der Gültigkeit zentraler einsatzrelevanter Dokumente.
- Berücksichtigung bestehender Haus- und Hofverbote.
- Berücksichtigung der Mitwirkung an erforderlichen Sicherheitsmaßnahmen.
- Abbildung einer abgestuften und eindeutig interpretierbaren Statuslogik.
- Ausgestaltung ohne Offenlegung sensibler Detailinformationen.

Betroffenenrechte müssen gewahrt bleiben, dürfen aber keine Umgehung bestehender Sicherheitsmechanismen ermöglichen.

### 3.1.6. Vermeidung von Umgehungsversuchen

Wie in den Abschnitten 1.1.3, 1.2, 1.3.1.4, 0 und 2.2.3 deutlich wird, besteht ein wesentliches Risiko darin, dass bereits auffällig gewordene Personen unter veränderter Identität oder nach bewusster Spurenbeseitigung erneut in sicherheitsrelevante Strukturen gelangen. Eine wirksame Lösung muss deshalb auch gegen gezielte Umgehungsversuche abgesichert sein, bei denen Betroffenenrechte strategisch genutzt werden, um eine spätere Neuerfassung unter erschwerten Wiedererkennungsbedingungen zu ermöglichen.

Die Lösung muss daher insbesondere folgende Fähigkeiten aufweisen:

- Abbildung eines rechtskonformen Mechanismus, durch den ein Begehren auf Entfernung personenbezogener Angaben nicht automatisch eine sofortige erneute Aufnahme ohne Schutzvorkehrungen ermöglicht.
- Vorsehen einer befristeten Sperrlogik gegen eine erneute Anmeldung nach einem solchen Vorgang, soweit hierfür eine tragfähige rechtliche Grundlage besteht.
- Ausgestaltung der Schutzlogik mit dem Ziel, missbräuchliche Löschanträge zur Verschleierung von Identitäten oder zur Umgehung bereits bestehender Sicherheitsmechanismen zu verhindern.
- Umsetzung im Einklang mit den Vorgaben zu Entfernung, Verarbeitungsbegrenzung, Nachweisführung und sonstigen datenschutzrechtlichen Anforderungen.
- technische und organisatorische Ausgestaltung, die einerseits Betroffenenrechte wahrt und andererseits gezielte Wiederanmeldungen unter Umgehung bestehender Schutzmechanismen erschwert.

## 3.2. Fähigkeitsspektrum Compliance Efficiency durch Automatisierung

Nur wenn ein Unternehmen dies beherrscht, hat das Unternehmen ausreichende Ressourcen, um sich um die Security zu kümmern.

### 3.2.1. Automatisierung regelmäßiger Revalidierung

Eine wirksame Lösung muss eine feste und systemgestützte Revalidierungslogik abbilden. Dies ist notwendig, weil sicherheitsrelevante Risiken nicht nur bei der Erstaufnahme entstehen, sondern sich auch im weiteren Verlauf ergeben können. Die Lösung muss daher insbesondere folgende Fähigkeiten aufweisen:

- Erneute Bestätigung der Identität bei jedem weiteren Prüfprozess.
- Regelmäßige Kontrolle fahrerbezogener Berechtigungen.
- Fristgerechte Überprüfung weiterer einsatzrelevanter Dokumente.
- Erneute Prüfung bei statusrelevanten Änderungen.
- Termingebundene und prozesssichere Abbildung wiederkehrender Kontrollen.
- Eine Ausgestaltung, die den operativen Aufwand gering hält.

### 3.2.2. Reminder und Benachrichtigungen

Eine wirksame Lösung muss fällige Nachprüfungen und Dokumentenkontrollen automatisiert begleiten. Dies ist erforderlich, damit Fristen nicht im manuellen Tagesgeschäft untergehen und nicht konforme Personen nicht unbeabsichtigt in sicherheitsrelevanten Einsätzen verbleiben. Die Lösung muss mindestens folgende Fähigkeiten aufweisen:

- Rechtzeitige automatisierte Benachrichtigungen vor fälligen Nachprüfungen und Dokumentenkontrollen.
- Benachrichtigungen in einer für die jeweilige Person verständlichen oder bevorzugten Sprache.
- Eine abgestufte Eskalationslogik bei nicht fristgerechter Durchführung erforderlicher Prüfungen.
- Die systemseitige Begrenzung oder Sperrung des Einsatzes von Personen mit fehlenden, abgelaufenen oder ungültigen Nachweisen.

- Eine Ausgestaltung, die Compliance-Risiken reduziert und manuelle Prüfprozesse entlastet.

### 3.2.3. Nötige Compliance-Zertifizierungen

Wie in den Punkten 2.2.2, 2.2.3 und 3.1 deutlich wird, setzt eine wirksame Lösung nicht nur eine belastbare Sicherheitslogik voraus, sondern auch den Einsatz von Verifizierungsdiensten, deren Datenschutz und Sicherheitsniveau nachvollziehbar abgesichert ist.

Eine wirksame Lösung muss tausende internationale Dokumenttypen digital prüfen.

Da in diesem Zusammenhang sensible Daten verarbeitet werden, muss die zugrunde liegende Compliance belastbar nachgewiesen sein. Die Lösung muss daher auf Verifizierungsdiensten beruhen, deren Konformität mit den folgenden Datenschutz- und Sicherheitsstandards nachweisbar ist:

- Datenschutz Grundverordnung DSGVO
- ISO IEC 27001
- SOC 2 Type II
- California Consumer Privacy Act CCPA
- California Privacy Rights Act CPRA

Die Einhaltung dieser Anforderungen muss durch geeignete Zertifikate, Prüfberichte oder vergleichbare Nachweise belegt sein, aus denen Geltungsbereich, Aktualität und Aussagekraft klar hervorgehen.

### 3.2.4. Weltweite Anwendbarkeit

Wie in den Punkten 2.2.2, 2.2.3 und 3.1 deutlich wird, beschränken sich Identitäts- und Dokumentenrisiken in der Logistik nicht auf einzelne Staaten oder wenige Standarddokumente. Gerade bei grenzüberschreitenden Lieferketten und beim Einsatz von Fahrern mit unterschiedlichen Herkunfts- und Einsatzbezügen muss eine wirksame Lösung deshalb in der Lage sein, eine umfassende Bandbreite amtlicher Identitätsnachweise zuverlässig zu prüfen.

Automatisierte Revalidierung, Reminder und Sperrlogiken verhindern, dass abgelaufene oder fehlende Nachweise im Tagesgeschäft übersehen werden.

Aus diesem Grund muss eine wirksame Lösung eine international einsetzbare Dokumentenprüfung mit einer Abdeckung von mindestens 12.000 amtlich ausgegebenen Ausweisdokumenttypen bereitstellen. Sie muss in der Lage sein, unterschiedliche Sicherheitsmerkmale, Ausführungen, Serien und länderspezifische Varianten verlässlich zu erkennen und zu validieren. Erforderlich ist hierfür eine fortlaufend gepflegte Referenzgrundlage, die die maßgeblichen Dokumentenspezifika der relevanten Staaten und Behörden abbildet.

### 3.2.5. Digital First Ansatz

Wie in den vorstehenden Anforderungen sowie in den Ausführungen zu operativem Aufwand und Skalierbarkeit deutlich wird, kann eine wirksame Lösung ihren

Nutzen nur entfalten, wenn sie ohne zusätzliche physische Hilfsmittel in bestehende Abläufe eingebunden werden kann. Erforderlich ist deshalb eine vollständig digitale Ausgestaltung, die ohne papiergebundene Nachweise, gesonderte Karten, externe Lesegeräte oder sonstige separate Hardware auskommt. Die Lösung muss auf marktüblichen mobilen Endgeräten sowie auf den in der Logistik gängigen technischen Umgebungen nutzbar sein. Zugleich muss sie sich über etablierte Schnittstellenformate in bestehende Systemlandschaften einfügen lassen, ohne an einen bestimmten Hersteller oder ein einzelnes Plattformökosystem gebunden zu sein.

# 4. Vergleich vorhandener Lösungsansätze auf Basis der geforderten Fähigkeiten

Die derzeit im beschriebenen Zusammenhang eingesetzten Lösungsansätze sind:

1. KYC und Identitätsprüfungsdienste
2. Whitelist- und Fahrerregistersysteme
3. Trusted Carrier und Unternehmensscreening
4. HR, Background Screening und Referenzprüfungen
5. Zugangskontrollen und physische Zutrittssysteme
6. Smart Logistik, Telematik und Asset Tracking
7. Consulting, allgemeine Cyber Security und IT-Services
8. DriverTrust als digitales Fahrer-Identitäts- und Compliance-Management-System.

Vor dem Hintergrund der Bedrohungslage und der aufgezeigten strukturellen Defizite bestehender Kontrollmechanismen ist die Eignung von Lösungsansätzen daran zu messen, in welchem Umfang sie die in Kapitel 3 hergeleiteten Anforderungen tatsächlich erfüllen. Maßgeblich ist dabei, ob ein Ansatz in der Lage und geeignet ist, die identifizierten Sicherheits- und Compliance-Probleme vollständig (und nicht nur einzelne Bestandteile) wirksam zu adressieren. Eine tragfähige Lösung sollte die Anforderungen möglichst vollständig erfüllen, da gerade die identifizierten Lücken zwischen Identitätsprüfung, Betrugserkennung, unternehmensübergreifender Risikoberücksichtigung und operativer Umsetzbarkeit die Hauptursache für stark steigende Schadenszahlen und -volumina sind. Im Folgenden werden daher Lösungsansätze daraufhin untersucht, inwieweit sie die benötigten Fähigkeiten erfüllen.

## 4.1. KYC und Identitätsprüfungsdienste

KYC- und Identitätsprüfungsdienste adressieren einen relevanten Teilbereich des in Kapitel 0 beschriebenen Problemkomplexes. Sie verfügen in der Regel über eine mehrstufige Verifikationsstruktur und bieten oft verknüpfte Prüfmechanismen sowie einen Digital-First-Ansatz. Dies ermöglicht eine strukturierte Identitätsprüfung im Onboarding-Prozess und ist insbesondere für die Erkennung klassischer Dokumentenfälschungen und Impostor-Konstellationen wertvoll.

Das Einsatzprofil von KYC-Diensten ist jedoch konzeptionell auf die einmalige oder fallbezogene Prüfung von Personen im Moment der Registrierung oder Onboarding ausgerichtet. Dies ergibt sich

aus der funktionalen Grundausrichtung dieser Dienste, wie sie u. a. in den gängigen Branchendefinitionen beschrieben wird: KYC steht für die punktuelle Verifizierung einer Person anhand vorgelegter Nachweise, typischerweise als Teil regulatorischer Compliance-Anforderungen im Finanzsektor (FATF, 2020; § 2 GwG).

KYC-Dienste verifizieren den Onboarding-Moment. Nicht den laufenden Einsatz.

Aus dieser konzeptionellen Ausrichtung folgen strukturelle Unterschiede zu den in Kapitel 3 hergeleiteten Anforderungen:

Kontinuierlicher 1:n-Abgleich: KYC-Prozesse sind nach ihrer Grundlogik als 1:1-Verifikation ausgestaltet – d. h. als Abgleich einer Person mit einem ihr zugeordneten Datensatz (NIST, 2026). Die Fähigkeit, dieselbe natürliche Person unter abweichenden Identitätsangaben in einem unternehmensübergreifenden Bestand wiederzuerkennen, ist in der Standardausgestaltung von KYC-Diensten nicht vorgesehen, da sie einen fortlaufenden 1:n-Abgleich voraussetzen würde, der über die regulatorische Funktion solcher Dienste hinausgeht (The World Bank, 2019).

FOGD-Erkennung: Wie in Abschnitt 1.3.2 dargelegt, versagen bei FOGD alle Prüfverfahren, die ausschließlich auf Dokumentenechtheit und 1:1-Abgleich beruhen. Da FOGD formal korrekte, behördlich ausgestellte Dokumente sind, können sie reguläre Echtheitsprüfungen technisch korrekt bestehen (ICAO, 2018; Interpol, 2026). KYC-Dienste, die ihren Prüfprozess auf Dokumentenvalidierung und 1:1-biometrische Verifikation beschränken, adressieren diese Konstellation konzeptionell nicht.

Unternehmensübergreifende Berücksichtigung von Haus- und Hofverboten: Das Wirkprinzip von KYC-Diensten setzt typischerweise am beauftragenden Unternehmen an. Eine unternehmensübergreifende Nutzung sicherheitsrelevanter Statusinformationen – insbesondere in der datenschutzkonformen Form, wie sie in Abschnitt 3.1.2 beschrieben wird – ist nicht Bestandteil des regulatorischen KYC-Rahmens und erfordert eine eigene datenschutzrechtliche Grundlage gemäß Art. 6 und Art. 10 DSGVO (EU-DSGVO).

KYC ersetzt keine fortlaufende Wiedererkennung und keine unternehmensübergreifende Risikologik.

Automatisierte Revalidierung und Reminder-Logik: Die in Abschnitt 3.2.1 und 3.2.2 beschriebene Anforderung an eine fortlaufende automatisierte Prüfung fahrerbezogener Dokumente und Berechtigungen entspricht dem Anwendungsbereich der in Abschnitt 2.1 beschriebenen Compliance-Pflichten (§ 21 StVG, § 4a AufenthG, § 404 SGB III). Diese Anforderung betrifft den laufenden Betrieb im Logistikumfeld und liegt außerhalb des typischen Leistungsumfangs von KYC-Diensten, die primär für regulatorische Onboarding-Anforderungen konzipiert

sind.

Trust Indikation und Compliance-Zertifizierung für den Logistikbereich: KYC-Dienste sind typischerweise auf die Anforderungen des Finanzsektors und regulatorischer Compliance ausgerichtet (GwG, AMLD, FATF). Die in Abschnitt 3.1.5 beschriebene sicherheits- und compliancebezogene Trust Indikation für den Einsatz von Fahrern in der Supply Chain sowie die in Abschnitt 3.2.3 genannten Zertifizierungsanforderungen (ISO/IEC 27001, SOC 2 Type II) sind kein standardisierter Bestandteil des KYC-Leistungsspektrums.

Im Ergebnis lässt sich festhalten: KYC- und Identitätsprüfungsdienste können Identitätsbetrug mit formaler Unkorrektheit (siehe 1.1.3.2) erkennen und somit in der Regel einen im Vergleich zu einfachen Sichtprüfungen durch Angestellte deutlich erhöhten Sicherheitsgrad gewährleisten. Die in Kapitel 3 hergeleiteten Anforderungen an kontinuierliche unternehmensübergreifende Wiedererkennung, FOGD-Erkennung, automatisierte Revalidierung, logistikspezifische Trust Indikation sowie datenschutzkonforme Berücksichtigung von Haus- und Hofverboten sind hingegen konzeptionell nicht Bestandteil des KYC-Leistungsrahmens und werden durch diesen Lösungsansatz daher nicht vollständig adressiert.

### 4.2. Whitelist- und Fahrerregistersysteme

Whitelist- und Fahrerregistersysteme sind Lösungen, die Personen in einem zentralen oder vernetzten Register erfassen und Zugangsentscheidungen an diesen Registrierungsstatus knüpfen. Sie setzen darauf, dass eine Person bereits bekannt, geprüft und freigegeben ist; nicht registrierte Personen werden abgewiesen (NIST, 2002) (siehe hierzu auch Abschnitt 1.3.1)

Die entscheidende Grenze liegt jedoch darin, dass sie eine statusbasierte Abfrage durchführen („Ist diese Identität registriert?“), keinen bestandsweiten 1:n-Abgleich. Wie Abschnitt 1.3.2.2 zeigt, unterscheidet das NIST klar zwischen „one-to-one comparison" (Verifikation) und „one-to-many comparison" (Identifikation); letzteres ist für Mehrfachidentitäten erforderlich (NIST, 2002; The World Bank, 2019).

Besonders bei FOGD (vgl. Abschnitt 1.1.3.3) stößt eine reine Registerprüfung an Grenzen. Interpol definiert FOGD als echte, behördlich ausgestellte Dokumente, die durch Täuschung erlangt wurden. Ein Register erkennt nicht, wenn dieselbe natürliche Person unter anderer Identität bereits registriert ist (Interpol, 2026).

> Whitelist und Fahrerregister beantworten, ob eine Identität registriert ist. Sie erkennen aber nicht zuverlässig, ob dieselbe natürliche Person bereits unter anderer Identität im System vorhanden ist.

Einfache Sperrlogiken verstärken die rechtlichen Risiken in Bezug auf das Anlegen von Listen mit personenbezogenen Daten, wie in 1.3.1.3 gezeigt. Art. 10 DSGVO erlaubt strafrechtsnahe Daten nur unter behördlicher Aufsicht oder gesetzlicher Grundlage. Die niederländische Datenschutzbehörde stellte bei

einer Fraud Blacklist fest: „no statutory basis for processing the personal data on the list“ vorhanden (Autoriteit Persoonsgegevens, 2025; Europäische Union, 2016; edpb, 2022).

Im Ergebnis lässt sich festhalten: Fähigkeiten haben diese Systeme bei Transparenz und Statusverwaltung (vgl. hierzu auch Kapitel 1.3.2.5). Sie ersetzen jedoch keinen 1:n-Abgleich, keine mehrstufige Verifikation und keine datenschutzrechtlich saubere Trust-Logik. Für die beschriebenen Risiken sind sie allein nicht ausreichend (edpb, 2024).

### 4.3. Trusted Carrier und Unternehmensscreening

Trusted Carrier-Systeme und Unternehmensscreenings prüfen Speditionen und Dienstleister auf Stammdaten, Lizenzen, Versicherungen und Registereinträge. Sie adressieren Fake-Carrier-Risiken, indem sie Scheinunternehmen erkennen, die Transportaufträge erschleichen (trans.info, 2021). Aus Kapitel 1.1.2: „Fake Carrier sind Schein-Frachtführer, die sich als seriöse Speditionen ausgeben“ (GDV, 2025a; GDV, 2025b)

Trusted Carrier und Unternehmensscreening prüfen Unternehmen, nicht die handelnde Person. FOGD, Mehrfachidentitäten und Insider-Risiken bleiben bestehen.

Die entscheidende Grenze liegt jedoch darin, dass sie das Unternehmen prüfen, nicht die handelnde Person. TAPA EMEA warnt: „Criminals using digital tools to conceal their true identities, the creation of shell companies and legitimate firms being cloned” (IUMI & TAPA, 2026).

Zudem bleiben FOGD und Identitätsbetrug weiterhin unentdeckt: Solche Systeme erkennen nicht, wenn kriminelle Strukturen echte Dokumente mit gefälschten Identitäten nutzen. Secure Logistics betont: „Ein Handelsregisterauszug oder eine Führerscheinkopie sagen wenig aus, wenn die dahinterstehende Identität nicht überprüft ist“ (vgl. hierzu auch Kapitel 1.1.3.3) (Secure Logistics, 2026).

Datenschutzrechtliche Vorgaben schränken Screening weiter ein: Trusted Carrier und Unternehmensscreenings dürfen personenbezogene Daten nur zweckgebunden und minimal verarbeiten (Art. 5 DSGVO). Strafrechtsnahe Daten sind nur unter behördlicher Aufsicht oder gesetzlicher Grundlage zulässig (Art. 10 DSGVO). Vergleiche auch Kapitel 1.3.1.3: Die Aufsichtspraxis zeigt, dass Schwarze Listen ohne klare Rechtsgrundlage datenschutzrechtlich scheitern (edpb, 2022).

Trusted Carrier und Screenings validieren effektiv Unternehmensdaten (Handelsregister, EU-Transportlizenzen, VIES-USt-Prüfung) und erkennen formale Scheinunternehmen. Sie ersetzen jedoch keinen personenbezogenen 1:n-Abgleich, keine mehrstufige Verifikation und keine Trust-Indikation für Fahrer (TAPA EMEA, 2024a; TAPA EMEA, 2024b).

Im Ergebnis lässt sich festhalten: Trusted Carrier und Screenings sind nützlich gegen Scheinunternehmen, prüfen aber nicht die Person hinter dem Unternehmen. Für FOGD, Mehrfachidentitäten und

Insider-Risiken sind sie allein nicht ausreichend (IUMI & TAPA, 2026; EU-DSGVO).

### 4.4. HR, Background Screening und Referenzprüfungen

HR, Background Screening und Referenzprüfungen prüfen Bewerber auf Vorstrafen, Kreditwürdigkeit, soziale Medien und frühere Arbeitgeber. Sie adressieren die Wiederholungstäter-Risiken aus Kapitel 1.2. Zudem zeigt Kapitel 1.3.1, dass: auch schwerwiegende Kündigungsgründe nicht firmenübergreifend erfassbar sind (§ 32 BZRG).

Datenschutzrechtlich ist die Verarbeitung strafrechtsnaher Daten jedoch eng begrenzt. Art. 10 DSGVO erlaubt sie „nur unter behördlicher Aufsicht“ oder auf gesetzlicher Grundlage, § 26 BDSG nur bei „Erfordernis“ und „Erheblichkeit“ (§ 26 BDSG).

HR, Background Screening und Referenzprüfungen erfassen bekannte Auffälligkeiten nur begrenzt. Sie erkennen keine FOGD, keine Mehrfachidentitäten und keine erneute Registrierung derselben Person unter abweichenden Identitätsangaben.

Diese Verfahren decken zudem keine FOGD oder Mehrfachidentitäten ab. Taylor Wessing betont: „Beim Background-Check dürfen Arbeitgeber nur solche Informationen erheben, für die sie ein berechtigtes Interesse haben.“ Und weiter: „Der Arbeitgeber muss den Bewerber ferner unverzüglich über die durchgeführte Recherche und die Kategorien der verarbeiteten Daten informieren“ (TaylorWessing, 2025). Referenzprüfungen setzen wiederum die Einwilligungen ehemaliger Arbeitgeber voraus (Art. 6 Abs. 1 lit. a DSGVO i.V.m. Art. 7).

Fähigkeiten dieser Lösungsansätze liegen bei Führungszeugnissen und Schufa-Auskunft bei Vertrauenspositionen (§ 32 BZRG). Im Ergebnis lässt sich daher festhalten, dass sie nützlich für bekannte Auffälligkeiten sind, aber nicht die notwendigen Fähigkeiten des 1:n-Abgleichs und mehrstufige Verifikation bieten (vgl. Kapitel 1.3.2) (Haufe, 2024).

### 4.5. Zugangskontrollen und physische Zutrittssysteme

Zugangskontrollen und physische Zutrittssysteme wie Ausweise, Karten, Schranken, Scanner, Drehkreuze oder standortbezogene Zutrittssoftware leisten einen sinnvollen Beitrag zur operativen Absicherung einzelner Standorte. Sie steuern Zugänge, dokumentieren Anwesenheiten und erschweren unberechtigte Zutritte – und adressieren damit Insider-Risiken aus Kapitel 1.1.1 sowie Wiederholungstäter aus Kapitel 1.2.

Zutrittssysteme ohne Fraud Detection und kontinuierlichen biometrischen 1-n Abgleich bieten keinen Schutz vor Kriminellen, die sich als legitime Fahrer ausgeben und gefälschte Dokumente oder FOGD nutzen.

Diese Systeme verhindern unbefugten physischen Zutritt und protokollieren Bewegungen für Nachweisbarkeit (§ 64 Abs. 3 BDSG). Sie sind jedoch auf lokale Zugangskontrolle beschränkt und lösen nicht den personenbezogenen Sicherheits- und Compliance-Problemkomplex. Sie erkennen weder FOGD noch

Mehrfachidentitäten oder Identitätstäuschung, da ihnen ein kontinuierlicher unternehmensübergreifender 1:n-Abgleich fehlt (siehe 1.1.3, 1.3.2). Haus- und Hofverbote bleiben lokal und nicht datenschutzkonform unternehmensübergreifend.

Acre Security bestätigt ihre Kernfähigkeit: Physische Zutrittskontrollsysteme regeln, wer ein Gebäude, einen Raum oder einen sicheren Bereich betreten oder verlassen kann. Im Kern überprüfen sie die Identität und erlauben oder verweigern den Zugriff auf der Grundlage vordefinierter Regeln (acre Security, 2026). Damit bieten sie einen Schutz für Räume und Anlagen.

Blue ID differenziert präzise: „Die Zutrittskontrolle regelt den physischen Zugang zu Räumen und Gebäuden. Die Zugangskontrolle betrifft den Zugang zu IT-Systemen. Die Zugriffskontrolle steuert, welche Daten innerhalb eines Systems abgerufen oder bearbeitet werden dürfen“ (BlueID, 2026). Protokolldaten unterliegen zudem der Speicherbegrenzung nach Art. 5 DSGVO. SimonsVoss formuliert die Anforderung: „Zutrittsprotokolle müssen regelmäßig gelöscht werden, ansonsten könnte die Speicherung gegen das Speicherbegrenzungsprinzip der DSGVO verstoßen“ (SimonsVoss, 2025).

Im Ergebnis lässt sich festhalten: Die Lösungsansätze haben Fähigkeiten bei physischer Absicherung, ersetzen aber keinen personenbezogenen 1:n-Abgleich oder mehrstufige Verifikation wie in Kapitel 1.3.2 gefordert.

## 4.6. Smart Logistik, Telematik und Asset Tracking

Smart Logistik, Telematik und Asset Tracking Lösungen, etwa für Sendungsverfolgung, Fahrzeugortung, Routenmonitoring, Geofencing, Trailer und Sensortracking, verfügen regelmäßig über einen Digital-First-Ansatz und leisten wertvolle Beiträge zur operativen Transparenz, Prozesssteuerung, Diebstahlreaktion und Absicherung logistischer Abläufe. „IoT-basierte Lösungen bieten Logistikunternehmen jederzeit Einblick in den Standort von Fracht und Assets“ über GPS, Sensorik und Multi-Netzwerk-Konnektivität für Echtzeit-Tracking (Giesecke+Devrient, 2021). Telematik kombiniert GPS mit Onboard-Diagnose für Standort und Geschwindigkeit (Impargo, 2023). Dieser Funktionsumfang adressiert jedoch einen anderen Schwerpunkt als den hier untersuchten personenbezogenen Sicherheits- und Compliance-Problemkomplex aus Kapitel 0 und 3.

Weitere strukturelle Grenzen ergeben sich, da diese Lösungsansätze nicht in der Lage sind, FOGD wirksam zu erkennen, weil ihnen personenbezogene Identitätsprüfung, kontinuierlicher unternehmensübergreifender 1:n-Abgleich und belastbare Wiedererkennung derselben natürlichen Person bei abweichenden Identitätsangaben fehlen (vgl. z. B. die Funktionsumfänge bei Modern Drive Technology, 2026).
Sie berücksichtigen keine Haus- und Hofverbote, bieten keine mehrstufige Verifikation der eingesetzten Person, verfügen nicht über verknüpfte Auswertung sicherheitsrelevanter Erkenntnisse

auf Identitäts-, Dokumenten- und Personenebene und stellen keine Trust-Indikation für Sicherheits- und Compliance-Einsatzbewertung bereit.

Am Beispiel GPS zeigt sich: „Sobald GPS-Daten einer konkreten Person zugeordnet werden können (z. B. einem Fahrer), gelten sie als personenbezogene Daten. Damit unterliegen sie der DSGVO“ (Moving Intelligence, 2025).

Telematik und Asset Tracking zeigen, wo sich Ware, Fahrzeuge oder Trailer befinden, beantworten aber nicht, ob die eingesetzte Person sicherheits- und compliancebezogen vertrauenswürdig ist.

Weiterhin bieten sie keinen Mechanismus gegen Umgehungsversuche durch veränderte Identitäten oder erneute Registrierung nach Löschung und typischerweise auch keine automatisierte Revalidierung personenbezogener Berechtigungen sowie keine Reminder zu Compliance-Anforderungen (§ 21 StVG, § 4a AufenthG), keine Verifizierungsdienste mit ISO 27001/SOC 2 und keine Abdeckung der geforderten Gesamtzahl an Ausweisdokumenttypen (vgl. z. B. den Funktionsumfang bei AddSecure, 2025).

Im Ergebnis lässt sich festhalten: Die Lösungsansätze sind sinnvoll in angrenzenden operativen Bereichen (z.B. Geschützte Waren, Effizienzsteigerungen und optimierte Prozesse durch Asset Tracking (A1 Digital, 2023)), können den beschriebenen Problemkomplex aber nicht eigenständig lösen.

### 4.7. Consulting, allgemeine Cyber Security und IT-Services

Consulting, allgemeine Cyber Security sowie IT-Services adressieren IT-Risiken, Prozessoptimierung und Compliance wie ISO 27001 oder DSGVO-Umsetzung. Sie bieten Gap-Analysen, ISMS-Aufbau und Beratung zu Datenschutzvereinbarungen (BWS, 2026; Giel, 2025)

Ihre konzeptionelle Ausrichtung liegt auf systemischer IT-Sicherheit: Die ISO 27001 definiert einen systematischen Ansatz zur Identifizierung, Bewertung und Behandlung von Informationssicherheitsrisiken (BWS, 2026). IT-Compliance umfasst die Einhaltung von Gesetzen, Regeln und Normen im IT-Bereich (Althammer & Kill, 2021). Dies schließt nahtlos an IT-Compliance an, ersetzt jedoch nicht den personenbezogenen Sicherheits- und Compliance-Problemkomplex aus Kapitel 0 und 3.

Consulting, Cyber Security und IT-Services stärken IT Compliance, lösen aber keine personenbezogene Wiedererkennung, FOGD-Erkennung oder logistikspezifische Trust Indikation.

Strukturelle Unterschiede zu den in Kapitel 3 hergeleiteten Anforderungen ergeben sich wie folgt: Consulting-Diensten bieten keinen kontinuierlichen 1:n-Abgleich, da ihr Fokus auf Zugriffsmanagement (IAM) und nicht auf personenbezogener Wiedererkennung bei abweichenden Identitätsangaben liegt. „Identitätssicherheit gehört zur Cybersicherheit und konzentriert sich auf den Schutz digitaler Identitäten und der Systeme, die sie

verwalten“ (IBM, 2024).

Ebenso ermöglichen sie keine FOGD-Erkennung, da sie keine behördlich ausgestellten Dokumente auf Täuschungserlangung prüfen und keine biometrische Dokumentenverifikation bieten (PXL, 2026).

Eine unternehmensübergreifende Berücksichtigung von Haus- und Hofverboten scheitert an Art. 10 DSGVO: Strafdaten dürfen demnach nur unter behördlicher Aufsicht verarbeitet werden. Consulting kann Prozesse DSGVO-konform gestalten, aber keine Blacklists ohne Rechtsgrundlage implementieren. Automatisierte Revalidierung fahrerbezogener Nachweise (§ 21 StVG) oder Reminder-Logik liegt außerhalb ihres typischen Leistungsumfangs, ebenso wie logistikspezifische Trust-Indikationen. Datenschutzrechtlich verstärkt sich dies: Ohne Datenschutzvereinbarung nach Art. 28 DSGVO drohen Verstöße – die Haftung bleibt beim Auftraggeber (Giel, 2025).

Im Ergebnis lässt sich festhalten: Diese Dienste sind wertvoll für IT-Compliance und ISMS-Aufbau, adressieren jedoch keine kontinuierliche unternehmensübergreifende Wiedererkennung, FOGD-Erkennung, automatisierte Revalidierung oder logistikspezifische Trust-Indikationen. Sie ergänzen, lösen den Problemkomplex aber nicht eigenständig.

### 4.8. DriverTrust als digitales Fahrer-Identitäts- und Compliance-Management-System

Der Lösungsansatz von DriverTrust ist auf die Erkennung von FOGD, Identitätstäuschung, Mehrfachidentitäten sowie auf die Abwehr von Insider und Fake-Carrier-Risiken auf Personenebene ausgerichtet. Er verfügt hierfür über einen kontinuierlichen unternehmensübergreifenden 1:n-Abgleich sowie über die Fähigkeit, dieselbe natürliche Person auch bei abweichenden Identitätsangaben wiederzuerkennen.

DriverTrust verbindet Identitätsprüfung, Wiedererkennung, Risikologik und laufende Compliance in einem System.

Zugleich berücksichtigt DriverTrust Haus- und Hofverbote in einer datenschutzkonformen, datensparsamen und statusbezogenen Form, ohne auf problematisches Blacklist Sharing oder die Offenlegung sensibler Detailinformationen angewiesen zu sein.

Darüber hinaus verfügt der Lösungsansatz über eine mehrstufige Verifikation, in der verschiedene sicherheitsrelevante Erkenntnisquellen zusammengeführt und in einer einheitlichen Bewertungslogik ausgewertet werden. Hierdurch wird eine verknüpfte Auswertung sicherheitsrelevanter Erkenntnisse ermöglicht, die auch in komplexen Konstellationen eine belastbare sicherheitsbezogene Einordnung unterstützt.

DriverTrust stellt ferner eine operative Trust Indikation bereit, die sich ausschließlich auf die sicherheits- und compliancebezogene Einsatzbewertung einer Person bezieht und dadurch eine datenschutzkonforme und zugleich praktisch nutzbare Entscheidungsgrundlage schafft. Ebenso umfasst der

Lösungsansatz Mechanismen zur Vermeidung von Umgehungsversuchen, insbesondere für Konstellationen, in denen durch Löschungsbegehren, Wiederanmeldungen oder veränderte Identitätsangaben eine erneute Aufnahme unter erschwerten Wiedererkennungsbedingungen angestrebt wird.

Im Bereich Compliance Efficiency erfüllt DriverTrust zudem die Anforderungen an eine automatisierte regelmäßige Revalidierung, an Reminder- und Benachrichtigungen sowie an einen vollständig digitalen und operativ skalierbaren Einsatz. Soweit Verifizierungsdienste eingebunden werden, beruht der Lösungsansatz auf Verifizierungsdiensten mit nachweisbarer Konformität zu den geforderten Datenschutz- und Sicherheitsstandards. Hinzu kommt die internationale Einsetzbarkeit einschließlich einer Dokumentenprüfung mit der geforderten breiten Abdeckung amtlich ausgegebener Ausweisdokumenttypen.

In der Konsequenz ist DriverTrust als ein Lösungsansatz einzuordnen, der die in identifizierten Anforderungen erfüllt und damit geeignet ist, den beschriebenen Sicherheits- und Compliance-Problemkomplex wirksam zu lösen.

## 4.9. Vergleichstabelle zu Lösungsansätzen

Die nachfolgende Seite enthält eine zusammenfassende Vergleichstabelle, in der die in Kapitel 4 untersuchten Lösungsansätze anhand der geforderten Fähigkeiten gegenübergestellt werden.

| ÜBERSICHT VERFÜGBARER LÖSUNGSANSÄTZE | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | **FÄHIGKEITEN FRAUD DETECTION**<br>1 FOGD Erkennung / 1:n Abgleich<br>2 Haus und Hofverbote unternehmensübergreifend<br>3 Mehrstufige Verifikation<br>4 Verknüpfte Auswertung sicherheitsrelevanter Erkenntnisse<br>5 Trust Indikation<br>6 Vermeidung von Umgehungsversuchen | | | | | | **COMPLIANCE EFFICIENCY / AUTOMATISIERUNG**<br>7 Automatisierte Revalidierung<br>8 Reminder / Benachrichtigungen<br>9 Compliance Zertifizierung d. Verifikationsdienste<br>10 Weltweite Anwendbarkeit / Abdeckung (≥12.000 Dokumenttypen)<br>11 Digital First Ansatz | | | | |
| **LÖSUNGS-ANSATZ** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** |
| 1 KYC und Identitätsprüfungs-dienste | - | - | ✓ | teilw. erfüllt | - | - | - | - | teilw. erfüllt | teilw. erfüllt | ✓ |
| 2 Whitelist- und Fahrerregister-systeme | - | - | - | - | - | - | - | - | - | - | teilw. erfüllt |
| 3 Trusted Carrier und Unternehmens-screening | - | teilw. erfüllt | - | - | - | - | - | - | - | - | teilw. erfüllt |
| 4 HR, Background Screening und Referenzprüfungen | - | - | - | - | - | - | - | - | - | - | teilw. erfüllt |
| 5 Zugangskontrollen und physische Zutrittsysteme | teilw. erfüllt | teilw. erfüllt (nur lokal) | - | - | - | - | - | - | - | - | teilw. erfüllt |
| 6 Smart Logistik, Telematik und Asset Tracking | - | - | - | - | - | - | - | - | - | - | ✓ |
| 7 Consulting, allgemeine Cyber Security und IT-Services | - | - | teilw. erfüllt (Kon-zept) | teilw. erfüllt (Kon-zept) | - | - | - | - | - | - | teilw. erfüllt |
| 8 DriverTrust | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

✓ Erfüllt – Fähigkeit wird vollständig abgedeckt.
teilw. erfüllt – Fähigkeit wird nur eingeschränkt abgedeckt.
- Nicht erfüllt – Fähigkeit wird nicht abgedeckt.

Tabelle 2: Marktübersicht verfügbarer Lösungsansätze für Fraud Detection und Compliance Efficiency / Automatisierung

# 5. Warum DriverTrust diese Anforderungen in der Gesamtschau erfüllt

Die Eignung von DriverTrust zur Bewältigung des beschriebenen Problemkomplexes erklärt sich aus der spezifischen Entstehungs- und Entwicklungslogik des Lösungsansatzes. Ausgangspunkt war die Anforderung, einen bislang nicht hinreichend adressierten Sicherheits- und Compliance-Problemkomplex in der Logistik unter den besonderen Bedingungen datenschutzrechtlicher, arbeitsrechtlicher und operativer Restriktionen lösbar zu machen. Daraus entstand kein isoliert technisches Einzelprodukt, sondern ein anwendungsbezogener Lösungsansatz, der von Beginn an auf die Verbindung mehrerer Anforderungsdimensionen ausgerichtet war.

## 5.1. Entstehung von DriverTrust

Im Folgenden wird auf die Entstehungslogik und Entwicklungslogik von DriverTrust genauer eingegangen.

### 5.1.1. Kollaborativer Ansatz

Die Entstehung von DriverTrust erfolgte als problembezogene Entwicklung aus einem konkret beschriebenen Anwendungsdefizit heraus im Rahmen einer längerfristigen unternehmensübergreifenden Zusammenarbeit unter Einbindung von Versendern, Händlern und Logistikern.

Diese kollaborative Entstehungsstruktur ist für die Leistungsfähigkeit des Systems von wesentlicher Bedeutung, weil der zugrunde liegende Problemkomplex nicht eindimensional technischer Natur ist, sondern zugleich Fragen der verschiedenen kriminellen Modi Operandi, der Identitätsprüfung, der Betrugserkennung, der datenschutzkonformen Informationsverarbeitung, der operativen Einsetzbarkeit und der organisationsübergreifenden Anschlussfähigkeit umfasst. Die Systemarchitektur musste daher von Anfang an auf die gleichzeitige Berücksichtigung unterschiedlicher Anforderungen ausgerichtet werden.

Hierbei wurden von den am Projekt teilnehmenden Parteien Fähigkeiten vorgeschlagen, die anschließend von den anderen teilnehmenden Parteien bewertet wurden. Hieraus ergab sich ein Konsens, der die Auswahl und Reihenfolge der Fähigkeitsentwicklung von DriverTrust kontinuierlich geformt hat und weiter formt, um Relevanz und Praxistauglichkeit sicherzustellen.

> DriverTrust wurde gemeinsam mit Praxisakteuren der Logistik entwickelt und wird fortlaufend an reale Risiken, operative Anforderungen und neue Umgehungsstrategien angepasst.

Diese Kollaboration ist kein abgeschlossener Kreis, sondern erweitert sich kontinuierlich. Für die Leistungsfähigkeit des Lösungsansatzes ist darüber hinaus maßgeblich, dass DriverTrust nicht als statisches System konzipiert wurde. Vielmehr erfolgt die Weiterentwicklung fortlaufend unter Rückkopplung mit den operativen Anforderungen der beteiligten Praxisakteure. Diese Form der bedarfsorientierten Systementwicklung ermöglicht es, neue Umgehungsstrategien, veränderte Risikolagen und zusätzliche

Compliance Anforderungen in die Weiterentwicklung einzubeziehen. Die Leistungsfähigkeit von DriverTrust beruht daher nicht nur auf seinem ursprünglichen Funktionsumfang, sondern auch auf seiner strukturellen Offenheit für adaptive Weiterentwicklung.

### 5.1.2. Privacy by Design

DriverTrust beruht auf einem Privacy by Design orientierten Entwicklungsansatz, bei dem rechtliche und technische Anforderungen nicht nachgelagert aufeinander abgestimmt, sondern bereits auf Ebene der Systemkonzeption gemeinsam berücksichtigt wurden. Hierbei wurden mehrere auf Datenschutz und Arbeitsrecht spezialisierte Kanzleien von Anfang an in das Projekt eingebunden. Sie haben das Projekt bereits konzeptionell mitentwickelt, geformt und geprüft und sind nach wie vor eng mit dem Projekt verbunden, um jeden Entwicklungsschritt zu begleiten. Ein besonderer Fokus lag und liegt auf Datenminimierung, Zweckbindung und Transparenz.

### 5.1.3. Spezialisierung auf Datenschutz

Insbesondere relevant ist der Einsatz spezialisierter Datenschutztechnologie für die Lösbarkeit des beschriebenen Anwendungsfalls. Soweit sicherheitsrelevante Informationen auf Personenebene verarbeitet werden, besteht die zentrale Herausforderung nicht allein in der technischen Erfassung oder Verknüpfung von Daten, sondern in deren datenschutzkonformer, datensparsamer und rechtsstrukturell tragfähiger Ausgestaltung.

DriverTrust wurde von einem auf Datenschutz spezialisierten Entwicklerteam entwickelt. Die DriverTrust betreibende Green Convenience GmbH verfügt über patentrechtlich geschützte Datenschutztechnologie und ist auf die Lösung datenschutzrechtlich anspruchsvoller Anwendungsfälle spezialisiert.

## 5.2. Ein Integrierter Ansatz zum Schließen der Schutzlücke

Das Zusammenwirken aus kollaborativer Entwicklung, Privacy by Design, spezialisierter Datenschutztechnologie und der genutzten Vertragskonstellation erklärt, weshalb DriverTrust die in diesem Whitepaper beschriebenen Anforderungen nicht nur punktuell, sondern in ihrer Gesamtschau adressieren kann.

DriverTrust schließt die Schutzlücke durch die integrierte Verbindung von Wiedererkennung, Fraud Erkennung, rechtskonformer Statuslogik, Trust Indikation und automatisierter Compliance.

Entscheidend ist dabei nicht eine isolierte Einzelmaßnahme, sondern die integrierte Verbindung aus unternehmensübergreifender Wiedererkennung derselben natürlichen Person, Fraud Erkennung, rechtskonformer Berücksichtigung von Haus und Hofverboten, operativ nutzbarer Trust Indikation sowie automatisierten Compliance Prozessen. Erst diese Gesamtschau schließt die beschriebene Schutzlücke wirksam. Die Anwendbarkeit ist nicht auf Fahrer beschränkt, sondern umfasst alle Personen, die unmittelbaren Zugriff auf schützenswerte Güter haben oder einen solchen Zugriff durch

Informationsweitergabe, Zutrittserteilung, Prozessbeteiligung oder organisatorische Mitwirkung ermöglichen können.

### 5.3. Erforderlichkeit von DriverTrust

Ausgangspunkt der datenschutzrechtlichen Bewertung ist der konkret verfolgte Zweck der Verarbeitung. DriverTrust dient nicht einer allgemeinen Überwachung oder Leistungsbewertung von Fahrern, sondern der zweckgebundenen Prüfung, ob eine Person die für sicherheitsrelevante Transporttätigkeiten erforderlichen Voraussetzungen erfüllt und ob Identitätsmissbrauch, Mehrfachidentitäten, FOGD oder ein erneuter Zugang derselben Risikoperson zu schützenswerten Gütern verhindert werden können.

Dieser Zweck ist legitim. Er knüpft an die in den vorstehenden Kapiteln dargestellte Schutzlücke an: Kriminelle Mehrfachtäter nutzen zunehmend Identitätswechsel, Fake Carrier Strukturen und Insiderzugänge über formal echte, aber betrügerisch erlangte Dokumente, um erneut Zugang zu Transportprozessen und schützenswerten Gütern zu erhalten. Die Vermeidung solcher Risiken dient dem Schutz fremden Eigentums, der Verhinderung transportspezifischer Vermögensschäden und der Wahrnehmung bestehender Sorgfaltspflichten innerhalb der Lieferkette.

Die datenschutzrechtliche Detailbewertung dieses Zwecks, der hierfür eingesetzten Verarbeitungsschritte, der Rechtsgrundlagen, der Erforderlichkeit, der Verhältnismäßigkeit sowie der vorgesehenen Abhilfemaßnahmen erfolgt in der Datenschutz Folgenabschätzung zu DriverTrust. Danach besteht der übergeordnete Zweck von DriverTrust insbesondere darin, sicherzustellen, dass eingesetzte Fahrer die für die Transporttätigkeit notwendige Eignung, Zuverlässigkeit und Integrität aufweisen, und dies für die maßgeblichen Akteure nachweisbar zu machen. Im Speziellen zielt DriverTrust darauf ab, Ladungsdiebstahl und vergleichbare Schädigungen für Vermögen und Eigentum der Auftraggeber und Kunden bestmöglich zu unterbinden.

> Erforderlich ist das mildeste Mittel, das notwendig ist, um einen legitimen Zweck wirksam zu erreichen.

Damit ist der Schutz vor FOGD, Identitätsmissbrauch, Mehrfachidentitäten und wiederholt auftretenden Risikopersonen als festgelegter, eindeutiger und legitimer Zweck einzuordnen. Die weitere Prüfung betrifft die Erforderlichkeit und Verhältnismäßigkeit von DriverTrust.

#### 5.3.1. Erforderlichkeit

Im Folgenden wird genauer auf den Themenkomplex Erforderlichkeit und mildestes Mittel eingegangen. Eine tiefergehende Analyse findet sich in der DriverTrust DSFA.

##### 5.3.1.1. Was ist Erforderlichkeit?

Das Prinzip der Erforderlichkeit ist im Datenschutzrecht zweckbezogen zu verstehen. Eine Verarbeitung personenbezogener Daten ist erforderlich, wenn sie zur Erreichung eines festgelegten,

eindeutigen und legitimen Zwecks notwendig ist und dieser Zweck nicht ebenso wirksam durch ein milderes, weniger eingriffsintensives Mittel erreicht werden kann. Dieser Maßstab folgt aus Art. 5 Abs. 1 lit. b und c DSGVO (EU-DSGVO).

#### 5.3.1.2. Das mildeste Mittel zur FOGD-Erkennung

Wie in Kapitel 1.3.2 dargestellt, setzt die zuverlässige Erkennung von FOGD und Mehrfachidentitäten einen kontinuierlichen 1:n-Abgleich voraus. DriverTrust ist darauf ausgelegt, diesen Abgleich zweckgebunden und datensparsam umzusetzen. Grundlage sind ein dokumentiertes Datenschutzkonzept, Privacy by Design, Datenminimierung, Abstraktion biometrischer Merkmale, Zugriffsbeschränkungen sowie ein darauf abgestimmtes vertragliches Setup.

#### 5.3.1.3. Erforderlichkeitsprüfung von DriverTrust

Erforderlichkeit bedeutet, dass der festgelegte Zweck mit einem geeigneten Mittel erreicht werden muss, sofern kein gleich wirksames und zugleich milderes Mittel zur Verfügung steht.

Wie in Kapitel 1 dargestellt, liegt der relevante Zweck in der Vermeidung von Identitätsmissbrauch, FOGD, Mehrfachidentitäten und dem erneuten Zugang bereits auffällig gewordener Risikopersonen zu schützenswerten Gütern. Die in Kapitel 4 untersuchten Einzelmaßnahmen adressieren jeweils nur Teilaspekte dieses Risikos und schaffen insbesondere keine fortlaufende personenbezogene Wiedererkennung derselben natürlichen Person bei abweichenden Identitätsangaben.

Hinzu kommt der haftungsrechtliche Aspekt. Nach § 425 HGB haftet der Frachtführer grundsätzlich für Verlust oder Beschädigung des Gutes zwischen Übernahme und Ablieferung. Eine Entlastung kommt nach § 426 HGB nur in Betracht, soweit der Schaden auch bei größter Sorgfalt nicht vermeidbar war. Die Regelhaftung ist zwar nach § 431 HGB grundsätzlich auf 8,33 Rechnungseinheiten je Kilogramm Rohgewicht begrenzt; diese Begrenzung kann nach § 435 HGB entfallen, wenn der Schaden auf vorsätzliches oder leichtfertiges Verhalten in dem Bewusstsein zurückzuführen ist, dass ein Schaden mit Wahrscheinlichkeit eintreten werde (§ 425 HGB; § 426 HGB; § 431 HGB; § 435 HGB, 1998).

> Zuverlässige FOGD- und Mehrfachidentitätserkennung erfordert einen kontinuierlichen 1:n-Abgleich.

Wie in Kapitel 1.1.3.3 beschrieben, ist es hochwahrscheinlich und weit verbreitet, dass Schäden durch Kriminelle, die FOGD nutzen, dann eintreten, wenn keine FOGD erkennenden Gegenmaßnahmen implementiert sind.

Damit erhält die Erforderlichkeit auch eine wirtschaftliche und haftungsrechtliche Dimension: Wenn Unternehmen erkennbare Risiken für anvertraute Güter kennen und ein geeignetes, zumutbares Schutzmittel verfügbar ist, kann die Nichtnutzung dieses Mittels im Schadensfall haftungsrelevant werden.

DriverTrust ist daher als erforderlich

einzuordnen, soweit auf Grundlage der in Kapitel 4 dargestellten Markt und Alternativprüfung keine weniger eingriffsintensive, datenschutzrechtlich und wettbewerbsrechtlich tragfähige Alternative ersichtlich ist, die den beschriebenen Zweck gleich wirksam erreicht.

## 6. ROI-Berechnung und wirtschaftliche Bewertungslogik

Die wirtschaftliche Bewertung von DriverTrust kann über folgende Berechnungslogik erfolgen:

**Berechnung ROI:**

(Wirtschaftlicher Nutzen pro Jahr

*minus* jährliche Lösungskosten)

*geteilt durch* jährliche Lösungskosten

= ROI

Der ROI von DriverTrust ergibt sich aus dem jährlichen wirtschaftlichen Nutzen abzgl. Lösungskosten. Bewertet werden Schäden, Bearbeitungskosten, Versicherung, Reputation, Neugeschäft, Haftungsrisiken und Compliance Efficiency.

**Berechnung wirtschaftlicher Nutzen:**

Der wirtschaftliche Nutzen pro Jahr setzt sich aus sieben Bestandteilen zusammensetzen, die unternehmensspezifisch erweitert werden können:

Vermiedener direkter Nettoschaden

*plus*

vermiedene interne Bearbeitungskosten

*plus*

Reduzierung der Versicherungskosten

*plus*

reduzierter Reputationsverlust

*plus*

zusätzlicher Deckungsbeitrag durch gewonnene sicherheitskritische Aufträge

*plus*

reduzierte Compliance- und Haftungsrisiken

*plus*

gesteigerte Compliance Efficiency

=

wirtschaftlicher Nutzen pro Jahr

Auf Basis dieser Berechnungslogik können Unternehmen eigene Werte zu Schadenhistorie, Rollenstundensätze, interne Verrechnungssätze, Versicherungsdaten, Kundenrisiken, Vertriebschancen und Prozessaufwände einsetzen und somit ihren spezifischen ROI errechnen.

### 6.1. Vermiedener direkter Nettoschaden

Der direkte Nettoschaden umfasst den beim Unternehmen wirtschaftlich verbleibenden Wert gestohlener, unterschlagener oder nicht mehr verwertbarer Güter. Die EU Road Security Guidance beziffert die Verluste durch Cargo Theft in Europa auf „8.2 EUR billion annually“ (European Commission, 2019).

Zur Plausibilisierung kann dieser Gesamtschaden ins Verhältnis zur Beschäftigtenbasis des europäischen Transport- und Lagersektors gesetzt werden. Eurostat weist für Transportation and Storage „10.4 million persons“ aus (eurostat, 2025).

Der vermiedene direkte Nettoschaden berechnet sich aus dem wirtschaftlich verbleibenden Diebstahlschaden, multipliziert mit der realistisch angesetzten Reduktionsquote durch DriverTrust.

**Berechnung jährlicher Frachtdiebstahlschaden pro Beschäftigtem:**

8,2 Mrd. €

*geteilt durch*

10,4 Mio. Beschäftigte

= 788,46 € Frachtdiebstahlschaden pro Beschäftigtem pro Jahr

Dieser Wert stellt einen rechnerischen Orientierungswert dar. Er kann auf die eigene sicherheitsrelevante Risikopopulation übertragen werden, also auf Fahrer, Lagerarbeiter, Disponenten, Security Mitarbeiter, operative Kontaktpersonen, Subunternehmer und sonstige Personen, die Zugriff auf schützenswerte Güter ermöglichen können. In der Gesamtheit lässt sich so die rechnerische Schadensbasis ermitteln, wofür die folgende Rechnung verwendet werden kann:

**Berechnung Schadensbasis:**

Anzahl sicherheitsrelevanter Personen

*multipliziert mit*

788,46 €

= rechnerische Schadensbasis

Alternativ zur beschriebenen Berechnung der Rechnerischen Schadensbasis aus öffentlichen Durchschnittswerten kann ein Unternehmen auch eine eigene interne, unternehmensspezifische Schadensbasis errechnen. Hierbei ist es notwendig, nicht nur den Schwund als Diebstahl zu bewerten, der direkt einem Diebstahl zugeordnet werden kann, denn spezialisierte Studien gehen davon aus, dass in Europa 65 % des gesamten Schwunds (all losses), einschließlich des Schwunds, der nicht zugeordnet werden kann, durch Diebstahl begründet ist (University of Leicester & ECR Europe, 2004). Demnach kann in der folgenden Berechnung der unternehmensspezifischen Schadensbasis ein sicherheitsrelevanter Anteil ungeklärter Verluste von 65 % begründet angenommen werden.

**Berechnung Schadensbasis (unternehmensspezifisch):**

Bestätigte Diebstahlschäden

*plus*

(sicherheitsrelevanter Anteil ungeklärter Verluste in Prozent

*multipliziert mit*

Gesamtheit ungeklärter Verluste)

= Schadensbasis (unternehmensspez.)

Im nächsten Berechnungsschritt wird berücksichtigt, dass der direkte Schaden nicht immer vollständig beim Unternehmen verbleibt. Transporte sind häufig versichert; außerdem bestehen Haftungsgrenzen. § 431 HGB begrenzt die Entschädigung wegen Verlust oder Beschädigung auf „8,33 Rechnungseinheiten für jedes Kilogramm des Rohgewichts des Gutes“ (§ 431 HGB). In bestimmten Fällen kann auch ein Subunternehmer den Schaden ganz oder teilweise tragen. Im Folgenden werden diese Faktoren herausgerechnet, um den Nettoschaden zu ermitteln:

**Berechnung Nettoschaden:**

Schadensbasis

*minus*

Versicherungsleistung

*minus*

durchsetzbare Kostenübernahme durch Spediteur oder Subunternehmer

= Nettoschaden

In Bezug auf die in der Berechnung angenommene Diebstahlreduktionsquote (Reduktionsquote) ist folgendes zu beachten. Bei voller Abdeckung und mehrjähriger Nutzung kann als Best Case eine Diebstahlreduktion von bis zu 85 % unter den in DriverTrust geführten Personen angenommen werden, was im Folgenden begründet wird. 70 % der Zueignungsdelikte werden durch Wiederholungstäter begangen (HV Bayern, 2025), die in DriverTrust durch Red Status, Identity Continuity und Re-Identification adressiert werden.

Die verbleibenden 30 % der Ersttäter (100 % - 70 % = 30 %) werden durch zusätzliche Risikosignale in DriverTrust adressiert und können zum Teil erkannt werden. DriverTrust geht davon aus, dass von diesen verbleibenden 30 % Ersttätern etwa die Hälfte erkannt werden kann, was somit 15 % entspräche (30 % /2 = 15 %). Diese 15 % (erkannte Ersttäter) addiert mit den bereits genannten 70 % (erkannte Mehrfachtäter) ergibt eine kumulierte maximale Leistungsfähigkeit von 85 % in Bezug auf die Vermeidung von Diebstahl der DriverTrust geführten Personen. Eine Annäherung an diese maximale Diebstahlreduktionsquote von 85 % setzt einen mehrjährigen DriverTrust Einsatz voraus, da das System es unter anderem ermöglicht nach und nach Insider und kriminelle Akteure in der Supply Chain und in Dienstleisterstrukturen zu erkennen und das Unternehmen immer wirksamer zu schützen.

DriverTrust kann interne Bearbeitungskosten reduzieren, weil weniger Schadensfälle weniger Aufwand für Aufklärung, Abstimmung, Regressprüfung, Ersatzbeschaffung, Eskalation und Prozessanpassungen auslösen.

**Berechnung vermiedener direkter Nettoschaden:**

Nettoschaden

*multipliziert mit*

angenommener Reduktionsquote

= vermiedener direkter Nettoschaden

## 6.2. Vermiedene interne Bearbeitungskosten

Ein Schadensfall verursacht Arbeitszeit in mehreren Abteilungen wie Logistik, Security, Legal, Compliance, Finance, Versicherung, Einkauf, Vertrieb, Customer Service und Management. Es kommt auch vor, dass unterschiedliche Rollen mit unterschiedlichen Stundensätzen innerhalb der betroffenen Abteilungen betroffen sind. Deshalb sollte rollenbezogen gerechnet werden, um die Vermiedenen interne Bearbeitungskosten zu ermitteln. Hierfür kann die folgende Rechnung verwendet werden:

**Berechnung vermiedener interner Bearbeitungskosten:**

*Summe bilden*

aus Arbeitszeit aller beteiligten Personen je Rolle

*multipliziert mit*

dem jeweils durchschnittlichen Stundensatz dieser Rolle

= interne Bearbeitungskosten je Diebstahlsfall

*multipliziert mit*

jährlicher Anzahl von Diebstahlsfällen

= interne Gesamt-Bearbeitungskosten

*multipliziert mit*

angenommener Reduktionsquote

= vermiedene interne Bearbeitungskosten

Zu berücksichtigen sind interne Aufklärung, Abstimmung mit Kunde, Versicherung, Polizei, Frachtführer, Spediteur, Subunternehmer, Regressprüfung, Ersatzbeschaffung, Kundeneskalation, Management Reports und Prozessanpassungen.

DriverTrust kann reputationsbezogene Folgeschäden reduzieren, indem kundenkritische Diebstahlereignisse seltener werden und Kundenbeziehungen, Folgeaufträge sowie Vergabechancen besser geschützt werden.

## 6.3. Reduzierte Versicherungskosten

Auch versicherte Schäden bleiben wirtschaftlich relevant. Zu berücksichtigen sind höhere Prämien, schlechtere Versicherungsbedingungen und zusätzliche Sicherheitsauflagen, die auf einen Diebstahlsfall folgen können. Die finanzielle Belastung durch diebstahlsbedingte Versicherungskosten kann wie folgt ermittelt werden:

**Berechnung reduzierter Versicherungskosten:**

Aktuelle diebstahlsbezogene Versicherungskosten

*multipliziert mit*

angenommener Senkungsquote durch DriverTrust

= reduzierte Versicherungskosten

## 6.4. Reduzierter Reputationsverlust

Bei zeitkritischen Lieferketten kann der wirtschaftliche Schaden eines Ladungsdiebstahls deutlich über den unmittelbaren Warenwert hinausgehen. Wird eine Sendung mit produktionskritischen Komponenten, Rohmaterialien oder kundenspezifischen Waren entwendet, können Ersatzbeschaffung, Sondertransporte, Produktionsverzögerungen, Vertragsstrafen, Kundeneskalationen und Reputationsschäden entstehen.

Diese Risikologik wird zu Cargo Theft ausdrücklich beschrieben: „If key components or raw materials are stolen, the manufacturing process can come to a halt“ (Becker Logistics, 2024).

Solche Folgeschäden sind nicht in jedem Fall unmittelbar vom Logistikunternehmen zu tragen. Wirtschaftlich relevant bleiben sie dennoch, weil Diebstahlereignisse Servicebewertungen verschlechtern, bestehende Kundenbeziehungen belasten, Folgeaufträge reduzieren, Ausschlüsse aus Vergaben begünstigen

oder die Akquisition neuer Aufträge erschweren können. Die finanzielle Belastung des Reputationsverlusts aufgrund eines kundenkritischen Diebstahlereignisses kann wie folgt berechnet werden:

**Berechnung Schaden durch Reputationsverlust:**

Anzahl kundenkritischer Diebstahlereignisse pro Jahr

*multipliziert mit*

durchschnittlich erwarteter wirtschaftlicher Folge je kundenkritischem Diebstahlereignis aus Kundenverlust, entgangenem Neugeschäft und schlechteren Vertragsbedingungen

= reputationsbezogene Schadensbasis pro Jahr

reputationsbezogene Schadensbasis pro Jahr

*multipliziert mit*

angenommener Reduktionsquote

= reduzierter Reputationsverlust

DriverTrust kann als Sicherheitsnachweis die Zuschlagschancen bei sicherheitskritischen Transporten erhöhen und zusätzlichen Deckungsbeitrag aus hochwertigen Aufträgen ermöglichen.

## 6.5. Zusätzlicher Deckungsbeitrag durch gewonnene sicherheitskritische Aufträge

DriverTrust stärkt die vertriebliche Position eines Transportunternehmens im Segment sicherheitskritischer Transporte. Auftraggeber hochwertiger, zeitkritischer oder diebstahlgefährdeter Güter berücksichtigen bei der Vergabe zunehmend die Nachweisbarkeit geeigneter Sicherheitsprozesse. Unternehmen, die solche Prozesse strukturiert belegen können, verbessern ihre Chancen in Ausschreibungen, Vergaben und Vertragsverlängerungen.

Darüber hinaus kann DriverTrust als Qualitätsnachweis aktiv im Vertrieb eingesetzt werden, auch wenn Sicherheitsanforderungen nicht ausdrücklich formuliert sind. Das Unternehmen kann damit belegen, dass es die ihm anvertrauten Güter durch einen besonders umfassenden Schutz vor kriminellem Zugriff absichert und zugleich Mechanismen fest verankert hat, die grundlegende Compliance Standards auch in Substrukturen durchsetzen. Dadurch entsteht eine nachvollziehbare Positionierung als zuverlässiger Transportpartner, die die Zuschlagswahrscheinlichkeit bei sicherheitskritischen Transportvolumina erhöhen kann.

Die wirtschaftliche Wirkung ergibt sich aus dem adressierbaren sicherheitskritischen Transportvolumen, dem daraus ableitbaren Deckungsbeitrag sowie der durch DriverTrust beeinflussten Zuschlagswahrscheinlichkeit. Der zu erwartende zusätzliche Deckungsbeitrag durch eine DriverTrust Einführung kann wie folgt berechnet werden:

**Berechnung zusätzlicher Deckungsbeitrag durch DriverTrust:**

Anzahl potenzieller Auftraggeber mit sicherheitskritischen Transporten

*multipliziert mit*

durchschnittlicher Anzahl

Transporteinheiten pro Jahr je Auftraggeber

= sicherheitskritisches Transportvolumen pro Jahr in Transporteinheiten

sicherheitskritisches Transportvolumen pro Jahr in Transporteinheiten

*multipliziert mit*

durchschnittlichem Deckungsbeitrag je Transporteinheit

= adressierbarer jährlicher Deckungsbeitrag

adressierbarer jährlicher Deckungsbeitrag

*multipliziert mit*

durch DriverTrust erhöhte Zuschlagswahrscheinlichkeit

= zusätzlicher jährlicher Deckungsbeitrag durch geschützte Transporte

## 6.6. Compliance und Haftungsrisiken

Wirtschaftliche Risiken entstehen aus Prüf-, Dokumentations- und Nachweispflichten, insbesondere bei Fahrerlaubnis, Aufenthaltstitel, Arbeitserlaubnis und Datenschutz.

Dabei entsteht ein struktureller Zielkonflikt: Unternehmen müssen den rechtmäßigen Einsatz von Personen auch in Subunternehmerstrukturen nachweisen und zugleich personenbezogene Daten auf das notwendige Maß begrenzen.

Ein typisches Beispiel ist die Kontrolle von Aufenthaltstiteln bei Fahrern von Subunternehmern. § 404 SGB III verlangt wirksame Sorgfalt gegen den Einsatz unberechtigter Personen; zugleich kann die standortübergreifende Speicherung von Ausweiskopien zu Data Spreading führen und gegen Datenminimierung sowie Speicherbegrenzung nach Art. 5 DSGVO verstoßen. Beispielhaft können Verstöße Bußgelder von bis zu 500.000 € nach § 404 SGB III sowie bis zu 20 Mio. € oder 4 % des weltweiten Jahresumsatzes nach Art. 83 DSGVO auslösen.

Hinzu kommt das in Kapitel 5.3.1.3 dargestellte Haftungsrisiko, wenn erkannte Gefahren für anvertraute Güter nicht mit geeigneten und zumutbaren Schutzmaßnahmen adressiert werden. DriverTrust ermöglicht es, diesen Zielkonflikt strukturiert, nachweisbar und datensparsam aufzulösen, insbesondere durch statusbasierte Logik und dokumentierte Prozesse.

DriverTrust reduziert Compliance und Haftungsrisiken, indem gesetzliche Prüfpflichten nachweisbar erfüllt, werden bei gleichzeitiger Vermeidung von unnötiger Datenerhebung und dezentraler Ablage.

**Berechnung der Risikowerte für Compliance und Haftung mit und ohne DriverTrust**

*Summe bilden*

relevante Compliance-, Sanktions-, Haftungs- und Regressrisiken aus Kapitel 2 und 5.3.1.3

*multipliziert mit*

Eintrittswahrscheinlichkeit **ohne** DriverTrust

= erwarteter Risikowert **ohne** DriverTrust

*Summe bilden*

relevante Compliance-, Sanktions-, Haftungs- und Regressrisiken aus Kapitel 2 und 5.3.1.3

*multipliziert mit*

Eintrittswahrscheinlichkeit **mit** DriverTrust

= erwarteter Risikowert **mit** DriverTrust

erwarteter Risikowert **ohne** DriverTrust

*minus*

erwarteter Risikowert **mit** DriverTrust

= reduzierte Compliance- und Haftungsrisiken pro Jahr

## 6.7. Compliance Efficiency und Prozessentlastung

Neben Risikoreduktion kann DriverTrust operative Abläufe vereinfachen. Relevant sind insbesondere Frachtübergabe, Anmeldung und Zutritt sowie gesetzliche Prüfpflichten.

In vielen Unternehmen verursachen diese Prozesse Aufwand: Fahrer müssen angemeldet, Zuständigkeiten geklärt, Statusinformationen geprüft, Nachweise kontrolliert, Fristen überwacht und Ergebnisse dokumentiert werden. Wenn Informationen verteilt vorliegen, entstehen zusätzlich Suchaufwand, Rückfragen und Unsicherheiten zum aktuellen Status.
DriverTrust kann diesen Aufwand reduzieren, indem Prüfungen, Reminder und Statusinformationen digital unterstützt werden. Fahrer können erforderliche Schritte über die App in ihrer Sprache erledigen. Der grüne DriverTrust Status mit zugehöriger DriverTrust ID (Kennung im System) stellt ein kontinuierliches digitales Zertifikat dar, mit dem sich Mitarbeiter schneller, sicherer und datenschutzfreundlicher als bisher gegenüber Personen oder Systemen authentifizieren können, zum Beispiel an Fahreranmeldungen oder Zutrittskontrollen die mit dem Schutz schützenswerter Güter zusammenhängen.

DriverTrust ersetzt manuelle Registrierung durch eine digitale Freigabe über Status und DriverTrust ID. Dadurch sinken Prüfaufwand, Wartezeiten, Sprachbarrieren und unnötige Datenerhebung bei Anmeldung, Zutritt, Frachtübergabe und gesetzlichen Prüfpflichten.

DriverTrust beschleunigt operative Prüf- und Freigabeprozesse, weil vor Ort keine klassische Registrierung mehr erforderlich ist. Die zu überprüfende Person muss sich weder in Listen eintragen noch Namen, Geburtsdaten, Ausweise oder sonstige Dokumente vorlegen. Für die Freigabe genügt die Anzeige der DriverTrust ID und des grünen Status in der App. Dadurch entfallen manuelle Erfassungsschritte, Wartezeiten und fehleranfällige Papierprozesse. Sprachkenntnisse der zu überprüfenden Person sind hierfür nicht erforderlich, da die Prüfung digital, standardisiert und barrierearm über die App erfolgt. Hierdurch können Schlangen und Verzögerungen bei Fahreranmeldungen, Zutrittskontrollen, Frachtübergaben oder vergleichbaren Prüfprozessen vermieden oder deutlich reduziert werden. Zugleich ist der Prozess sicherer und datenschutzkonformer als der heutige Status quo, weil er dem Grundsatz der Datenminimierung folgt:

Vor Ort werden nur die für die jeweilige Freigabe erforderlichen Informationen sichtbar gemacht, während unnötige Erhebungen von Namen, Geburtsdaten, Ausweisdaten oder sonstigen Dokumenten entfallen. Dadurch werden operative Abläufe bei Anmeldung, Zutritt und gesetzlichen Prüfpflichten vereinfacht und zugleich Datenschutz- sowie Haftungsrisiken reduziert. Auf Wunsch kann DriverTrust zusätzlich mit digitalen Pförtnersystemen kombiniert werden. Die Steigerung der Compliance Efficiency kann hierbei wie folgt berechnet werden:

**Berechnung der Steigerung von Compliance Efficiency:**

*Summe bilden*

der Prüfungen, Anmeldungen, Zutritte, Frachtübergaben und Zollkontrollen pro Jahr

*multipliziert mit*

eingesparter Zeit je Vorgang

*multipliziert mit*

durchschnittlichem Stundensatz der beteiligten Rollen

= gesteigerte Compliance Efficiency

Bei der Berechnung ist es wichtig für gesetzliche Prüfpflichten (siehe Kapitel 2), die bisher möglicherweise nicht ausreichend durchgeführt wurden einen Aufwand anzusetzen, den die einsetzende Firma gehabt hätte, wenn sie sich an die entsprechende Pflicht vollumfänglich gehalten hätte.

### 6.8. Ergebnis

Die wirtschaftliche Wirkung von DriverTrust ergibt sich aus der Gesamtschau.

DriverTrust kann schrittweise in bestehende Logistikprozesse eingeführt werden, um Frachtsicherheit und Compliance Efficiency zu steigern.

Relevant sind vermiedene Warenverluste, eingesparte interne Bearbeitungskosten, gesparte Versicherungskosten, zusätzliche Auftragschancen, Absenkung von Compliance und Haftungsrisiken sowie die laufende Entlastung durch automatisierte Compliance-Prozesse, die einen erheblichen wirtschaftlichen Nutzen begründen.

## 7. Schlussfolgerung und Möglichkeiten zur Einführung von DriverTrust

Die vorstehenden Ausführungen zeigen, dass sich die Bedrohungslage im Bereich der Frachtkriminalität in den vergangenen Jahren nicht nur verschärft, sondern auch strukturell verändert hat. Neben klassischen Diebstahlsformen treten zunehmend strategisch vorbereitete und arbeitsteilig organisierte Täuschungskonstellationen in den Vordergrund, insbesondere unter Einbeziehung von Insidern, Fake-Carrier-Strukturen, Identitätsbetrug und Mehrfachidentitäten.

Zugleich wird deutlich, dass die in der Praxis bislang eingesetzten Kontroll- und Prüfmechanismen diesen Problemkomplex nur teilweise adressieren und die maßgeblichen Schutzlücken fortbestehen. Aus der Analyse ergibt sich, dass eine wirksame Lösung nicht auf einzelne Prüfbausteine beschränkt sein darf. Erforderlich ist vielmehr ein

Lösungsansatz, der Identitätsprüfung, unternehmensübergreifende Wiedererkennung, datenschutzkonforme Berücksichtigung sicherheitsrelevanter Statusinformationen, mehrstufige Verifikation, verknüpfte Auswertung sicherheitsrelevanter Erkenntnisse sowie automatisierte Revalidierungs- und Benachrichtigungsprozesse in einer operativ nutzbaren Struktur zusammenführt.

Die Gegenüberstellung der verfügbaren Lösungsansätze zeigt, dass die untersuchten Alternativen jeweils nur Teilaspekte des beschriebenen Anforderungsprofils abdecken. DriverTrust ist demgegenüber als derjenige Lösungsansatz einzuordnen, der die in Kapitel 3 abgeleiteten Anforderungen in ihrer Gesamtschau adressiert und damit geeignet ist, den beschriebenen Sicherheits- und Compliance-Problemkomplex wirksam zu lösen.

DriverTrust ist auf den Einsatz in bestehenden Logistik- und Lieferkettenstrukturen ausgelegt. Die Einführung kann schrittweise erfolgen und sowohl eigene Fahrer als auch externe Dienstleister und Subunternehmerstrukturen einbeziehen, ohne dass bestehende Prozesse von Beginn an vollständig ersetzt werden müssen. Die Lösung ist für mobile, mehrsprachige und arbeitsteilige Einsatzumgebungen konzipiert. Wiederkehrende Prüfungen, Revalidierungen und dokumentenbezogene Erinnerungsprozesse lassen sich systemseitig abbilden, wodurch administrativer Aufwand reduziert und die praktische Umsetzbarkeit im Tagesgeschäft erleichtert wird. Damit verbindet DriverTrust sicherheitsbezogene Wirksamkeit mit operativer Anschlussfähigkeit und niedriger Einführungshürde.

Dieser Mehrwert greift auch in Sicherheitsumgebungen mit besonders hohen regulatorischen Anforderungen, etwa im luftfrachtbezogenen Umfeld und bei High Value Cargo. Luftsicherheitsrechtliche Anforderungen sichern vor allem Zugang, Prozesskonformität und die Integrität der sicheren Luftfrachtkette ab.

Das LBA stellt klar, dass auch Personen mit ‚lediglich' unbegleitetem Zugang zu sicherer Luftfracht eine Überprüfung nach § 7 Luftsicherheitsgesetz benötigen (§ 7 LuftSiG). DriverTrust ersetzt diese regulatorischen Anforderungen nicht, sondern ergänzt sie um einen zusätzlichen Schutzgegenstand auf Personenebene: die fortlaufende Wiedererkennung derselben natürlichen Person über Zeit, Dokumente, Unternehmen und Registrierungsanlässe hinweg.

Gerade für High Value Cargo ist dies relevant, weil dadurch nicht nur formale Zugangsberechtigungen, sondern auch Mehrfachidentitäten, Wiederauftreten unter abweichenden Angaben, unternehmensübergreifende Haus- und Hofverbote, wiederkehrende Revalidierung und eine operative Trust Indikation adressiert werden.

DriverTrust erweitert damit hochregulierte Sicherheitsumgebungen nicht um mehr Bürokratie, sondern um genau jene identitäts- und risikobezogene Sicherheitsschicht, die bei modernen Täterstrukturen zusätzlich erforderlich ist. Für Unternehmen, die von den dargestellten Risiken betroffen sind oder in sicherheitsrelevanten Logistik- und

Lieferkettenumgebungen tätig sind, spricht daher vieles dafür, einen Lösungsansatz einzusetzen, der die identifizierten Anforderungen strukturell und lückenlos erfüllt.

## 8. Kollaboration und Autoren

Dieses Whitepaper wurde auf Grundlage einer unternehmensübergreifenden fachlichen Kollaboration entwickelt. Die Version 1.0 dient als Grundlage für die weitere Kommentierung, Ergänzung und Schärfung durch Unternehmen und Fachakteure aus Logistik, Sicherheit, Compliance und angrenzenden Bereichen. Rückmeldungen, Ergänzungen und fachliche Hinweise sind ausdrücklich willkommen und können in die Weiterentwicklung künftiger Versionen einfließen.

Unternehmen, die die beschriebenen Risiken, Anforderungen oder mögliche Umsetzungswege vertiefen möchten, können über den nachfolgenden Kontakt in den fachlichen Austausch treten.

In Zusammenarbeit mit namhaften Forschungsinstitutionen wie der TU Darmstadt, Branchenverbänden und Kanzleien wie Osborne Clarke, Schönberger Dielmann und LPA Law Tax versteht sich die Green Convenience GmbH als innovatives Team, das essenzielle Probleme in der Lieferkette löst.

**Kontakt**

Für fachlichen Austausch, Pilotierung und Einführung von DriverTrust:

Benjamin Dauth
General Manager DriverTrust

E-Mail: b.dauth@driver-trust.de

Rana Kiyan
Senior Sales Manager

E-Mail: r.kiyan@driver-trust.de

Zentraler Unternehmenskontakt

Tel.: +49 69 380 2980 64

E-Mail: team@driver-trust.de

www.driver-trust.de

LinkedIn

Fachartikel im Handelsblatt

DriverTrust ist ein Produkt der Green Convenience GmbH

Green Convenience GmbH
HRB97824
c/o TechQuartier, Platz der Einheit 2
60327 Frankfurt am Main
Deutschland

Version 1.0

Mai 2026

## 9. Literaturverzeichnis

A1 Digital. (18. August 2023). *Asset Tracking mit IoT: Die Zukunft der Logistik*. (A1 Digital International GmbH & Co KG, Herausgeber) Abgerufen am 05. Mai 2026 von https://www.a1.digital/de/news/digitales-asset-tracking-logistik-sicherheit-effizienz-und-zukunftstrends

acre Security. (25. April 2026). *Die 7 Arten der physischen Zugangskontrolle, die Sie kennen müssen*. Abgerufen am 05. Mai 2026 von https://www.acresecurity.com/de/blog/physical-access-control

ACS. (2025). *The Crime Report 2025*. ( Association of Convenience Stores, Herausgeber) Abgerufen am 22. April 2026 von https://cdn.acs.org.uk/public/ACS%20Crime%20Report%202025.pdf

ADAC. (09. Dezember 2024). *Fahren ohne Führerschein: Strafe und Konsequenzen*. (Allgemeiner Deutscher Automobil-Club e.V., Herausgeber) Abgerufen am 22. April 2026 von https://www.adac.de/verkehr/recht/bussgeld-punkte/fahren-ohne-fuehrerschein/

AddSecure. (08. August 2025). *Telematik einfach erklärt für Transport und Logistik*. Abgerufen am 05. Mai 2026 von https://www.addsecure.de/blog/telematik-einfach-erklaert-fuer-transport-und-logistik/

AG Geldern. (15. Mai 2023). *Amtsgericht Geldern, Urteil vom 15.05.2023, Az. 5 Ds 597/22*. Abgerufen am 05. Mai 2026 von https://nrwe.justiz.nrw.de/lgs/kleve/ag_geldern/j2023/5_Ds_597_22_Urteil_20230515.html

Althammer & Kill. (28. April 2021). *Datenschutz durch IT-Compliance*. (Althammer & Kill GmbH & Co. KG, Herausgeber) Abgerufen am 05. Mai 2026 von https://www.althammer-kill.de/aktuelles/news/detail/datenschutz-durch-it-compliance

Auror. (07. April 2026). *Rise in violent retail crime in UK linked to repeat offenders, new data shows*. (Auror Limited, Herausgeber) Abgerufen am 22. April 2026 von https://www.auror.co/media-center/rise-in-violent-retail-crime-in-uk-linked-to-repeat-offenders-new-data-shows

Autoriteit Persoonsgegevens. (09. April 2025). *Police and judicial authorities - Black list*. Abgerufen am 22. April 2026 von https://www.autoriteitpersoonsgegevens.nl/en/themes/police-and-judicial-authorities/black-list

Bayerische Staatskanzlei. (07. November 2022). *Unternehmensinterne Delegation der Halteraufgaben; Überlassung eines Kraftfahrzeugs an einen Nichtberechtigten: Prüfungspflichten des Kraftfahrzeughalters*. Abgerufen am 22. April 2026 von https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2022-N-46007

Becker Logistics. (Oktober 2024). *The Rise of Cargo Theft | Causes & Solutions*. Abgerufen am 05. Mai 2026 von https://beckerlogistics.com/wp-content/uploads/2024/10/White-Paper-PDF.pdf

Biometrics Research Group. (25. Oktober 2024). *AI Poses Threat to Biometric Authentication, New Report Warns – But How Soon?* (Biometrics Research Group,

Inc., Herausgeber) Abgerufen am 22. April 2026 von https://www.biometricupdate.com/202410/ai-poses-threat-to-biometric-authentication-new-report-warns-but-how-soon

BlueID. (März 2026). *Zutrittskontrolle im Datenschutz*. Abgerufen am 05. Mai 2026 von https://www.blue-id.com/de/blog/zutrittskontrolle-im-datenschutz

Börse Global. (19. April 2026). *Phantom Carrier: Logistik-Branche im Visier organisierter Betrüger*. (AD HOC NEWS Portal Aktiengesellschaft, Herausgeber) Abgerufen am 22. April 2026 von https://www.ad-hoc-news.de/boerse/news/ueberblick/phantom-carrier-logistik-branche-im-visier-organisierter-betrueger/69209111

Bundesamt für Justiz. (23. Januar 1953). *§ 21 Abs. 1 Nr. 2 StVG*. Abgerufen am 22. April 2026 von Straßenverkehrsgesetz (StVG) - § 21 Fahren ohne Fahrerlaubnis: https://www.gesetze-im-internet.de/stvg/__21.html

Bundesamt für Justiz. (21. September 1984). *§ 32 BZRG*. Abgerufen am 22. April 2026 von Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz - BZRG) § 32 Inhalt des Führungszeugnisses: https://www.gesetze-im-internet.de/bzrg/__32.html

Bundesamt für Justiz. (01. Januar 1998). *§ 404 SGB III*. Abgerufen am 22. April 2026 von Sozialgesetzbuch (SGB) Drittes Buch (III) - Arbeitsförderung - (Artikel 1 des Gesetzes vom 24. März 1997, BGBl. I S. 594) § 404 Bußgeldvorschriften: https://www.gesetze-im-internet.de/sgb_3/__404.html

Bundesamt für Justiz. (01. Juli 1998). *§ 425 HGB*. Abgerufen am 05. Mai 2026 von Handelsgesetzbuch § 425 Haftung für Güter- und Verspätungsschäden. Schadensteilung: https://www.gesetze-im-internet.de/hgb/__425.html

Bundesamt für Justiz. (28. Juni 1998). *§ 426 HGB*. Abgerufen am 05. Mai 2026 von Handelsgesetzbuch § 426 Haftungsausschluß: https://www.gesetze-im-internet.de/hgb/__426.html

Bundesamt für Justiz. (28. Juni 1998). *§ 431 HGB*. Abgerufen am 05. Mai 2026 von Handelsgesetzbuch § 431 Haftungshöchstbetrag: https://www.gesetze-im-internet.de/hgb/__431.html

Bundesamt für Justiz. (28. Juni 1998). *§ 435 HGB*. Abgerufen am 05. Mai 2026 von Handelsgesetzbuch § 435 Wegfall der Haftungsbefreiungen und -begrenzungen: https://www.gesetze-im-internet.de/hgb/__435.html

Bundesamt für Justiz. (01. August 2004). *§ 4 SchwarzArbG*. Abgerufen am 22. April 2026 von Gesetz zur Bekämpfung der Schwarzarbeit und illegalen Beschäftigung (Schwarzarbeitsbekämpfungsgesetz - SchwarzArbG) § 4 Befugnisse bei der Prüfung von Unterlagen und Daten: https://www.gesetze-im-internet.de/schwarzarbg_2004/__4.html

Bundesamt für Justiz. (2004). *§ 4a AufenthG*. Abgerufen am 22. April 2026 von Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet 1) (Aufenthaltsgesetz - AufenthG) § 4a Zugang zur Erwerbstätigkeit: https://www.gesetze-im-internet.de/aufenthg_2004/__4a.html

Bundesamt für Justiz. (30. Juli 2004). *§ 95 AufenthG*. Abgerufen am 22. April 2026 von Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet 1) (Aufenthaltsgesetz - AufenthG) § 95 Strafvorschriften: https://www.gesetze-im-internet.de/aufenthg_2004/__95.html

Bundesamt für Justiz. (November 2005). *§ 276 BGB*. Abgerufen am 22. April 2026 von Bürgerliches Gesetzbuch (BGB) § 276 Verantwortlichkeit des Schuldners: https://www.gesetze-im-internet.de/bgb/__276.html

Bundesamt für Justiz. (15. Januar 2005). *§ 7 LuftSiG*. Abgerufen am 05. Mai 2026 von Luftsicherheitsgesetz (LuftSiG) § 7 Zuverlässigkeitsüberprüfungen: https://www.gesetze-im-internet.de/luftsig/__7.html

Bundesamt für Justiz. (26. Juni 2017). *§ 2 GwG*. Von Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz - GwG) § 2 Verpflichtete, Verordnungsermächtigung: https://www.gesetze-im-internet.de/gwg_2017/__2.html abgerufen

Bundesamt für Justiz. (25. Mai 2018). *§ 26 BDSG*. Abgerufen am 22. April 2026 von Bundesdatenschutzgesetz (BDSG) § 26 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses: https://www.gesetze-im-internet.de/bdsg_2018/__26.html

Bundesdruckerei. (27. Februar 2019). *Dokumentenprüfgeräte für die Ausweisprüfung*. (Bundesdruckerei Gruppe GmbH, Herausgeber) Abgerufen am 22. April 2026 von https://www.bundesdruckerei.de/de/innovation-hub/meldestellen-mit-it-gegen-falsche-identitaeten

Bundesgerichtshof. (10. Juli 2007). *BGB §§ 254 Ea, 823 Ac; StVG §§ 9, 17*. Abgerufen am 22. April 2026 von https://www.bundesgerichtshof.de/SharedDocs/Entscheidungen/DE/Zivilsenate/VI_ZS/2006/VI_ZR_199-06.pdf?__blob=publicationFile&v=1

Bundesverwaltungsgericht. (24. Oktober 2001). *Urt. v. 24.10.2001, Az.: BVerwG 1 D 47.00*. Abgerufen am 05. Mai 2026 von https://www.anwalt24.de/urteile/bverwg/2001-10-24/bverwg-1-d-4700

BWS. (2026). *ISO 27001 Beratung für Unternehmen – praxisnah & zertifizierungsbereit*. (BWS Consulting Group GmbH, Herausgeber) Abgerufen am 05. Mai 2026 von https://bws-group.de/unsere-leistungen/informationssicherheit/iso-27001-beratung/

CISA. (März 2023). *Information and Communications Technology Supply Chain Security*. (Cybersecurity & Infrastructure Security Agency, Herausgeber) Abgerufen am 22. April 2026 von https://www.cisa.gov/topics/information-communications-technology-supply-chain-security

CISA. (März 2023). *Insider Threat Mitigation*. (Cybersecurity & Infrastructure Security Agency, Herausgeber) Abgerufen am 22. April 2026 von https://www.cisa.gov/topics/physical-security/insider-threat-mitigation

Debus, J. (08. September 2024). *Scheinspeditionen klauen Ladungen – Wie Phantom-Frachtführer vorgehen*. (TruckHero, Herausgeber) Abgerufen am 22. April 2026 von https://blog.truckhero.de/scheinspeditionen-klauen-ladungen/

Dekeyser, F. (08. Juni 2022). *Fake Carrier Fraus in Europe | TAPA EMEA Conference Presentation – Supply Chain Security*. Abgerufen am 22. April 2026 von https://tapaemea.org/wp-content/uploads/2022/07/Day-2-Session-2-Frederick-Dekeyser.pdf

DVZ. (21. Oktober 2021). *Fake-Carrier-Prävention: TAPA gründet Arbeitsgruppe*. (DVZ Deutsche Verkehrs-Zeitung, Herausgeber) Abgerufen am 22. April 2026 von https://www.dvz.de/unternehmen/logistik/detail/news/fake-carrier-praevention-tapa-

gruendet-arbeitsgruppe.html
edpb. (7. April 2022). *Tax Administration fined for fraud 'black list'*. (European Data Protection Board, Herausgeber) Abgerufen am 22. April 2026 von https://www.edpb.europa.eu/news/national-news/2022/tax-administration-fined-fraud-black-list_en
edpb. (08. Oktober 2024). *Guidelines 01/2024 on Processing of Personal Data Based on Legitimate Interest | Article 6(1)(f) GDPR*. (European Data Protection Board, Herausgeber) Abgerufen am 22. April 2026 von https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf
enisa. (Dezember 2014). *Privacy and Data Protection by Design – From Policy to Engineering*. (EU Agency for Network and Information Security, Herausgeber) Abgerufen am 22. April 2026 von https://www.enisa.europa.eu/sites/default/files/publications/Privacy%20and%20Data%20Protection%20by%20Design.pdf
Euractiv, AFP. (30. Oktober 2018). *Thousands obtained EU citizenship for €5000 in Bulgarian scam*. (Euractiv Media BV, Herausgeber) Abgerufen am 22. April 2026 von https://www.euractiv.com/news/thousands-obtained-eu-citizenship-for-e5000-in-bulgarian-scam
Europäische Union. (27. April 2016). *EU-DSGVO*. Abgerufen am 22. April 2026 von Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679
European Commission. (08. Dezember 2016). *COM(2016) 790 final*. Abgerufen am 05. Mai 2026 von COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN | Action plan to strengthen the European response to travel document fraud: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52016DC0790
European Commission. (16. Oktober 2018). *COM(2018) 696 final*. Abgerufen am 05. Mai 2026 von REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of the Action Plan to strengthen the EU response to travel document fraud: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52018DC0696
European Commission. (2019). *EC Security Guidance for the European Commercial Road Freight Transport Sector*. Abgerufen am 05. Mai 2026 von https://transport.ec.europa.eu/document/download/4dcd1d96-d190-42d9-948a-bb1fe34c2554_en?filename=roadsec-abridged-version_en.pdf
European Parliament. (2020). *Organised Property Crime in the EU.* Abgerufen am 22. April 2026 von https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656042/IPOL_STU%282020%29656042_EN.pdf
Europol. (12. April 2011). *Bavarian State Criminal Police share new tool for identifying fake ID documents*. Abgerufen am 22. April 2026 von https://www.europol.europa.eu/media-press/newsroom/news/bavarian-state-criminal-police-share-new-tool-for-identifying-fake-id-documents
Europol. (28. Juli 2025). *Eight Arrested in Takedown of Fake Document Distribution Hub Disguised as Greek Travel Agency*. Abgerufen am 22. April 2026 von

https://www.europol.europa.eu/media-press/newsroom/news/eight-arrested-in-takedown-of-fake-document-distribution-hub-disguised-greek-travel-agency

Europol. (2026). *Forgery and Trafficking of Administrative Documents*. Abgerufen am 22. April 2026 von https://www.europol.europa.eu/crime-areas/forgery-and-trafficking-of-administrative-documents

eurostat. (01. September 2025). *Businesses in the transportation and storage sector*. Abgerufen am 05. Mai 2026 von https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/10091.pdf

FATF. (März 2020). *Guidance on Digital Identity*. (Financial Action Task Force, Herausgeber) Abgerufen am 22. April 2026 von https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf

FreightWaves. (16. Juli 2025). *Insider threat cargo theft cases rose in Q2*. (FreightWaves, Herausgeber) Abgerufen am 22. April 2026 von https://www.freightwaves.com/news/insider-threat-cargo-theft-cases-rose-in-q2-expert-says

Frontex. (05. März 2024). *An Integrated Approach to Combat Document and Identity Fraud*. (European Border and Coast Guard Agency, Herausgeber) Abgerufen am 22. April 2026 von https://www.frontex.europa.eu/media-centre/news/news-release/an-integrated-approach-to-combat-document-and-identity-fraud-29m6RJ

Gallagher. (September 2025). *The Changing Nature of Cargo Theft*. (Arthur J. Gallagher & Co., Herausgeber) Abgerufen am 22. April 2026 von https://www.ajg.com/be/news-and-insights/features/changing-nature-of-cargo-theft/

GCCA. (2018). *Guide to Effective Warehouse Operations*. (Global Cold Chain Alliance, & International Association of Refrigerated Warehous, Herausgeber) Abgerufen am 22. April 2026 von https://www.gcca.org/legacy-system/FinalWarehouseOpsManual2018.pdf

GDV. (14. Oktober 2025a). *Verschwundene Lkw-Ladungen: Versicherer warnen vor hohen Schäden durch Phantomfrachtführer*. (Gesamtverband d. Deutschen Versicherungswirtschaft, Herausgeber) Abgerufen am 22. April 2026 von https://www.gdv.de/gdv/medien/medieninformationen/verschwundene-lkw-ladungen-versicherer-warnen-vor-hohen-schaeden-durch-phantomfrachtfuehrer-193494

GDV. (15. Oktober 2025b). *Die Zahl betrügerischer Frachtaufträge steigt deutlich: In den ersten sieben Monaten des Jahres 2025 wurden bereits 88 Fälle sogenannter Phantomfrachtführer registriert.* (GDV Gesamtverband der Deutschen Versicherung e.V., Herausgeber) Abgerufen am 22. April 2026 von https://www.linkedin.com/posts/gdv-verband_die-zahl-betr%C3%BCgerischer-frachtauftr%C3%A4ge-steigt-activity-7384154331555745792-_okP/

Giel, M. O. (07. Juli 2025). *Externe IT-Betreuung und Datenschutz – Ein unterschätztes Risiko*. Abgerufen am 05. Mai 2026 von https://giel-rechtsanwalt.de/allgemein/datenschutzvereinbarung-it-dienstleister/

Giesecke+Devrient. (23. Oktober 2021). *Vorteile der IoT-Lösungen von G+D für Logistik- und Transportdienstleister*. Abgerufen am 05. Mai 2026 von https://www.gi-de.com/de/branchen/transport-logistik/transport-logistikdienstleistungen

Handelsblatt. (18. Dezember 2025). *Wie Banden mithilfe von KI Lkw-Ladungen kapern*.

(Handelsblatt GmbH, Herausgeber) Abgerufen am 22. April 2026 von https://www.handelsblatt.com/unternehmen/dienstleister/logistik-wie-banden-mithilfe-von-ki-lkw-ladungen-kapern/100178873.html

Handwerkskammer Heilbronn-Franken. (2021). *Pflicht zur Führerscheinkontrolle*. Abgerufen am 22. April 2026 von https://www.hwk-heilbronn.de/artikel/pflicht-zur-fuehrerscheinkontrolle-62,0,5913.html

Haufe. (02. Dezember 2024). *Datenschutzrechtliche Zulässigkeit von Background-Checks (BB 2024, Heft 49, S. 2868)*. Abgerufen am 22. April 2026 von Anmerkung zu LAG Düsseldorf, 10.4.2024 – 12 Sa 1007/23: https://www.haufe.de/id/beitrag/datenschutzrechtliche-zulaessigkeit-von-background-checks-bb-2024-heft-49-s-2868-HI16685864.html

HV Bayern. (27. Juni 2025). *Ladendiebstahl: Immer mehr Banden unterwegs*. (Handelsverband Bayern e.V., Herausgeber) Abgerufen am 22. April 2026 von https://www.hv-bayern.de/aktuelles/meldungen/2025-06-27-Ladendiebstahl-Immer-mehr-Banden-unterwegs.php

IBM. (2024). *Was ist Identitätssicherheit?* (IBM Deutschland GmbH, Herausgeber) Abgerufen am 05. Mai 2026 von https://www.ibm.com/de-de/think/topics/identity-security

ICAO. (Februar 2016). *Guide for Assessing Security of Handling and Issuance of Travel Documents*. (International Civil Aviation Organization, Herausgeber) Abgerufen am 22. April 2026 von Part 1- Best Practices on Secure Issuance of Travel Documents: https://www.icao.int/sites/default/files/TRIP/Publications/Guide-PART-1-Format-Revised-27March.SM.pdf

ICAO. (Mai 2018). *ICAO Trip Guide on Evidence of Identity*. (International Civil Aviation Organization, Herausgeber) Abgerufen am 22. April 2026 von https://www.icao.int/sites/default/files/TRIP/Publications/ICAO-Guide-on-Evidence-of-Identity.pdf

Impargo. (20. Januar 2023). *Telematik in der Transportlogistik - Definition und Nutzen*. Abgerufen am 05. Mai 2026 von https://impargo.de/blog/telematik-in-der-transportlogistik

Interpol. (2026). *Identity and Travel Document Fraud*. Abgerufen am 22. April 2026 von https://www.interpol.int/en/Crimes/Counterfeit-currency-and-security-documents/Identity-and-travel-document-fraud

ITW Security Division. (Februar 2017). *Fraudulently Obtained Genuine (FOG) Documents - An ITW Security Division White Paper*. Abgerufen am 22. April 2026 von https://www.itwsf.com/Portals/0/Documents/White-Papers/Fraudulently%20Obtain%20Genuine%20FOG%20Documents.pdf

IUMI & TAPA. (Februar 2026). *IUMI and TAPA EMEA issue joint warning on fake carrier fraud and cargo crime risks*. (International Union of Marine Insurance, & Transported Asset Protection Association, Herausgeber) Abgerufen am 22. April 2026 von https://iumi.com/wp-content/uploads/2026/02/IUMI-and-TAPA-EMEA-joint-warning-on-fake-carrier-fraud-and-cargo-crime-risks.pdf

Le Parisien. (19. Dezember 2011). *Plus de 10 % des passeports biométriques seraient des faux*. Abgerufen am 22. April 2026 von https://www.leparisien.fr/faits-divers/plus-de-10-des-passeports-biometriques-seraient-des-faux-19-12-2011-1775325.php

LG Gießen. (17. März 2020). *LG Gießen, Urteil vom 17.03.2020 - 2 KLs - 401 Js 27674/19*.

Abgerufen am 05. Mai 2026 von https://openjur.de/u/2322350.html

Logistik Heute. (25. April 2025). *Ladungsdiebstahl: „Strategischer" Diebstahl war 2024 herausragender Wachstumstrend*. (HUSS-VERLAG GmbH, Herausgeber) Von logistik-heute.de: https://logistik-heute.de/news/ladungsdiebstahl-strategischer-diebstahl-war-2024-herausragender-wachstumstrend-210099.html abgerufen

Martinez, N. N., Lee, Y., Eck, J. E., & O, S. (01. August 2017). *Ravenous wolves revisited: a systematic review of offending concentration*. (Springer Nature, Herausgeber) Abgerufen am 22. April 2026 von https://link.springer.com/article/10.1186/s40163-017-0072-2

Modern Drive Technology. (2026). *Asset Tracking System für Lieferketten und Logistikprozesse*. Abgerufen am 05. Mai 2026 von https://www.moderndrive.de/asset-tracking-system/

Moving Intelligence. (25. Juli 2025). *DSGVO, BDSG und Mitbestimmungspflichten*. Abgerufen am 05. Mai 2026 von https://movingintelligence.de/blog/gps-tracking-dsgvo-firmenfahrzeuge

Munich Re. (26. März 2025). *Cargo Theft Tactics and Trends Report 2025*. (Munich Re Specialty Insurance (UK) Limited, Herausgeber) Abgerufen am 22. April 2026 von https://www.munichre.com/specialty/global-markets-uk/en/insights/cargo-and-freight/cargo-theft-tactics-and-trends-report-2025.html

NIST. (13. November 2002). *Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability*. (National Institute of Standards and Technology, Herausgeber) Abgerufen am 22. April 2026 von https://www.nist.gov/system/files/documents/2021/10/25/nist_appendix_pact_nov02.pdf

NIST. (2026). *Identity Assurance Level Requirements*. (National Institute of Standards and Technology, Herausgeber) Abgerufen am 22. April 2026 von https://pages.nist.gov/800-63-4/sp800-63a/ial/

NL Times. (29. November 2023). *€1.7 million worth of iPhones stolen from company at Schiphol*. Abgerufen am 22. April 2026 von https://nltimes.nl/2023/11/29/eu17-million-worth-iphones-stolen-company-schiphol

OCCRP. (02. November 2018). *Bulgarian Officials Charged in Passport Scam*. (Organized Crime and Corruption Reporting Project, Herausgeber) Abgerufen am 22. April 2026 von https://www.occrp.org/en/news/bulgarian-officials-charged-in-passport-scam

OLG Hamm. (07. Januar 2020). *Oberlandesgericht Hamm, Beschluss vom 07.01.2020, Az. 1 RVs 79/19*. Abgerufen am 05. Mai 2026 von https://nrwe.justiz.nrw.de/olgs/hamm/j2020/1_RVs_79_19_Beschluss_20200107.html

Pease, K., & Farrell, G. (27. März 2017). Preventing repeat and near repeat crime concentrations. In N. Tilley, & A. Sidebottom, *The Handbook of Crime Prevention and Community Safety* (Bd. 2). Routledge. Abgerufen am 22. April 2026 von https://eprints.whiterose.ac.uk/id/eprint/111258/

Politico. (28. Januar 2016). *EU's passport fraud 'epidemic'*. Abgerufen am 05. Mai 2026 von https://www.politico.eu/article/europes-fake-forged-stolen-passport-epidemic-visa-free-travel-rights/

PXL. (2026). *Automatisierte Identitätsverifikation*. (PXL Vision AG, Herausgeber) Abgerufen am 05. Mai 2026 von https://www.pxl-vision.com/de/loesung/automatisierte-

identitaetsverifikation
Roanoke Insurance Group Inc. (März 2025). *Cargo Theft Report 2025*. Abgerufen am 22. April 2026 von https://www.roanokegroup.com/static/73c489ff6fee4a12740dc05f14737119/2025-Cargo-Theft-Report_0425.pdf
Robertson, D. J., Watson, D. G., Mungall, A., Wade, K. A., Nightingale, S. J., & Butler, S. (27. Juni 2018). Detecting morphed passport photos: a training and individual differences approach. Von https://link.springer.com/article/10.1186/s41235-018-0113-8 abgerufen
Schunk Group. (11. Juni 2025). *Frachtdiebstahl – Wenn der Frachtführer ein 'Fake' ist*. (SCHUNCK GROUP GmbH, Herausgeber) Abgerufen am 22. April 2026 von https://schunck-group.de/aktuelles/frachtdiebstahl-wenn-der-frachtfuehrer-ein-fake-ist/
Secure Logistics. (2026). *Fake Carriers: ein neues Kapitel im Ladungsdiebstahl*. Abgerufen am 22. April 2026 von https://secure-logistics.nl/de/nachricht/fake-carriers-een-nieuw-hoofdstuk-in-ladingfraude/
Security Management. (03. November 2025). *External Theft Incidents Increased 19 Percent in 2024, Retail Report Finds*. (ASIS International, Herausgeber) Abgerufen am 22. April 2026 von https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2025/november/external-retail-theft/
SEI. (07. September 2022). *Common Sense Guide to Mitigating Insider Threats, Seventh Edition*. (Software Engineering Institute, Herausgeber) Abgerufen am 22. April 2026 von https://www.sei.cmu.edu/library/common-sense-guide-to-mitigating-insider-threats-seventh-edition
SimonsVoss. (31. März 2025). *Datenschutz & Zutrittskontrolle: DSGVO-konforme elektronische Schließanlagen in Unternehmen*. ( SimonsVoss Technologies GmbH, Herausgeber) Abgerufen am 05. Mai 2026 von https://blog.simons-voss.com/technologie/datenschutz-zutrittskontrolle-dsgvo-konforme-elektronische-schliessanlagen-in-unternehmen/
SVG. (09. März 2026). *Save the Date: Phantomfrachtführer – Online-Expertenforum 20. April 2026*. (SVG Bundes-Zentralgenossenschaft Straßenverkehr eG, Herausgeber) Abgerufen am 22. April 2026 von https://www.svg.de/meldungen/detailansicht/save-the-date-phantomfrachtfuehrer-online-expertenforum-20-april-2026
TAPA. (2023). *Recorded Cargo Crime & Supply Chain Security Risks*. (Transported Asset Protection Association, Herausgeber) Abgerufen am 22. April 2026 von https:/tapaemea.org/wp-content/uploads/2023/11/TAPA-EMEA-9-months-of-recorded-cargo-crime.pdf
TAPA EMEA. (2024a). *Driver Security Guide.* Transported Asset Protection Association.
TAPA EMEA. (2024b). *TAPA EMEA intelligence service*. (Transported Asset Protection Association, Herausgeber) Abgerufen am 22. April 2026 von https://tapaemea.org/incident-service/
TaylorWessing. (2025. Dezember 2025). *Schadensersatz nach Background-Check - Die Bedeutung der Information im Bewerbungsverfahren*. Abgerufen am 22. April 2026 von https://www.taylorwessing.com/de/insights-and-events/insights/2025/12/schadensersatz-nach-background-check
Thames Valley Police. (Januar 2024). *Retail Crime Strategy*. Abgerufen am 22. April 2026

von https://www.thamesvalley-pcc.gov.uk/wp-content/uploads/2024/01/Retail-Crime-Strategy-PUBLICATION-VERSION-FINAL.pdf

The World Bank. (01. Juni 2019). *Practitioner's Guide – Identification for Development (ID4D)*. (World Bank Group, Herausgeber) Abgerufen am 22. April 2026 von https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

trans.info. (15. Oktober 2021). *TAPA gründet eine Organisation im Kampf gegen Phantom-Frachtführer*. (European Road Transport Institute Foundation, Herausgeber) Abgerufen am 22. April 2026 von https://trans.info/de/tapa-gruendet-eine-organisation-im-kampf-gegen-phantom-frachtfuehrer-258518

trans.info. (08. September 2025). *Cargo theft surges 438 per cent across Europe. Criminals adopt sophisticated tactics*. (European Road Transport Institute Foundation, Herausgeber) Abgerufen am 22. April 2026 von https://trans.info/en/cargo-theft-surges-419606

Transportversicherungsmakler. (03. Dezember 2025). *Fake Carrier / Phantom-Frachtführer – Erkennung und Prävention*. (Schirmer Assekuranz Makler GmbH, Herausgeber) Abgerufen am 22. April 2026 von https://www.transport-makler.de/Fake-Carrier--Phantom-Frachtfuehrer_3258.aspx

Trucker Forum. (05. Januar 2016). *Datenschutz und Ausweispflicht*. Abgerufen am 22. April 2026 von https://trucker-forum.at/index.php?thread/6000-datenschutz-und-ausweispflicht/

TrustRiskControl. (2024). *Phantom-Frachtführer: Risiko erkennen, Prävention umsetzen, Schäden begrenzen*. (TRUST RISK CONTROL Int. Insurance Development GmbH, Herausgeber) Abgerufen am 22. April 2026 von https://trustrc.com/phantom-frachtfuehrer-risiko-erkennen-praevention-umsetzen-schaeden-begrenzen/

TT Club, BSI. (April 2025). *Cargo Theft Report 2024 – Supply Chain Security*. Abgerufen am 22. April 2026 von https://www.ttclub.com/fileadmin/uploads/tt-club/Documents/TT_and_BSI_annual_theft_report/TT_Club_Report_-_Supply_Chain_Report_April_2025.pdf

University of Leicester & ECR Europe. (Juli 2004). *SHRINKAGE IN EUROPE 2004: A SURVEY OF STOCK LOSS IN THE FAST MOVING CONSUMER GOODS SECTOR*. Abgerufen am 05. Mai 2026 von http://www.cgccrime.org.za/archive/Shrinkage%20Conference/Speakers%20Presentations/ECR%20Europe%20Shrinkage%20Report%202004.pdf

Zoll. (2015). *Folgen für Unternehmen bei Nichtbeachtung im Zusammenhang mit Aufenthaltstitel*. (Generalzolldirektion, Herausgeber) Abgerufen am 22. April 2026 von Unternehmen | Fachthemen | Arbeit | Aufenthaltstitel | Folgen bei Nichtbeachtung: https://www.zoll.de/DE/Fachthemen/Arbeit/Aufenthaltstitel/Folgen-bei-Nichtbeachtung/folgen-bei-nichtbeachtung_node.html