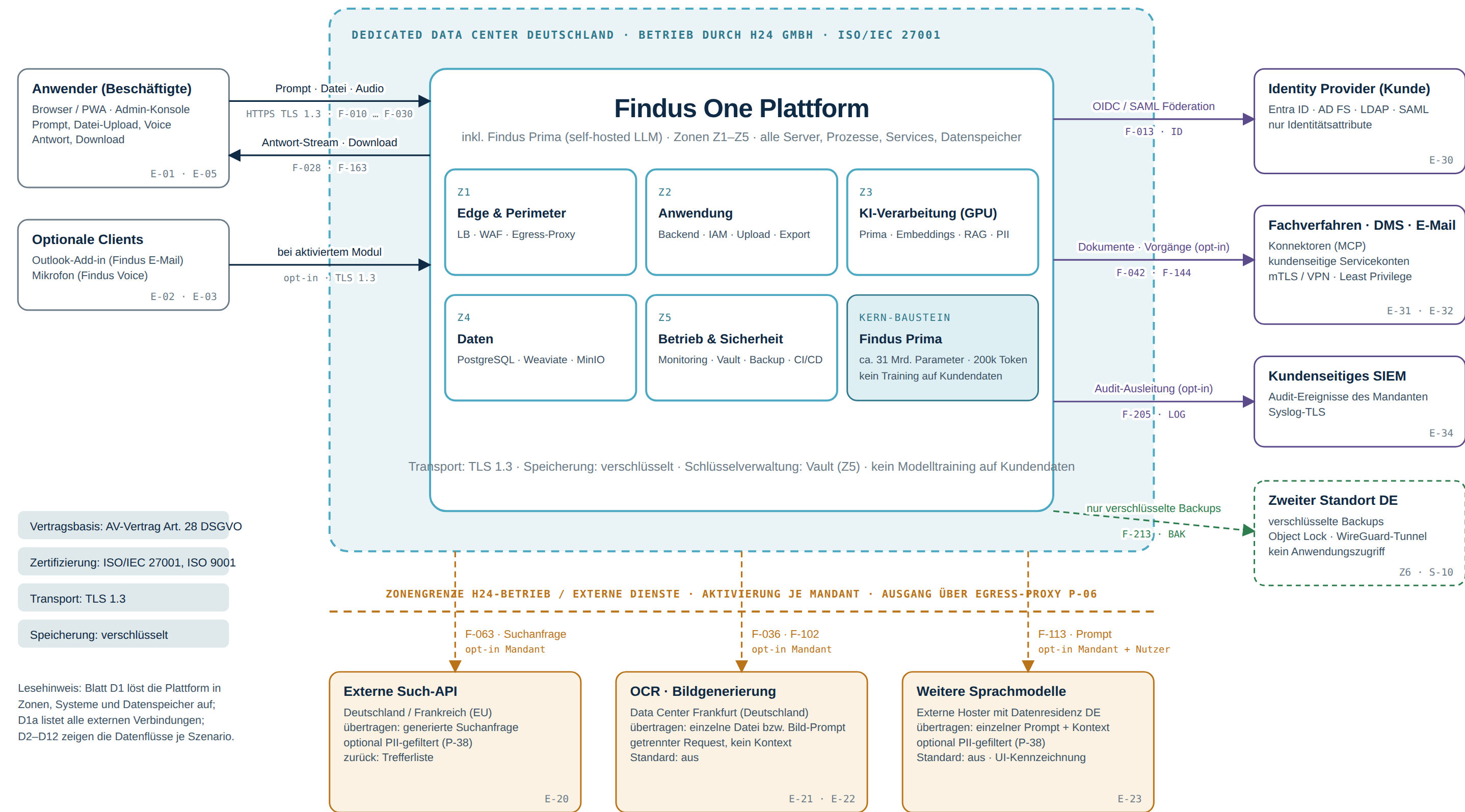
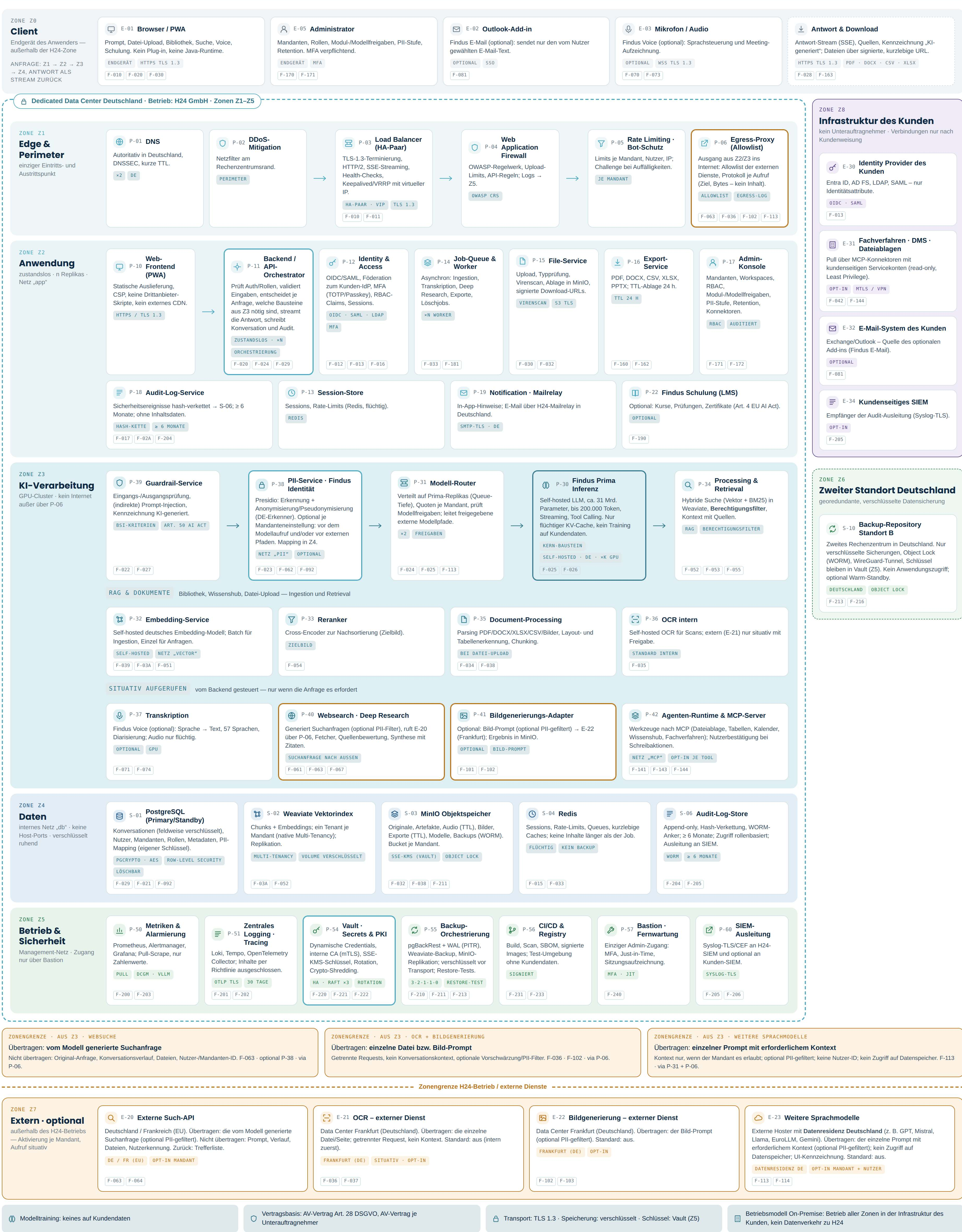






Liste der Verbindungen aus den Zonen Z1–Z5 zu Systemen außerhalb des H24-Betriebs. Jede Zeile entspricht einem Pfeil über eine Vertrauensgrenze auf Blatt D1; die Farbe der linken Kante zeigt die Zielzone.

PFAD	ZIEL	STANDORT	ÜBERGEBENER INHALT	AUSLÖSER	OPT-IN	SCHUTZMECHANISMUS
F-063 · F-065	Externe Such-API / öffentliche Webseiten	Deutschland / Frankreich (EU) · Internet	Generierte Suchanfrage (optional PII-gefiltert); Seitenabruf ohne Nutzerdaten	Findus Suche · Deep Research · Websuche-Tool	Mandant (Standard: an, abschaltbar)	optional PII-Filter · Allowlist · kein Kontext · Egress-Log
F-036	OCR – externer Dienst	Data Center Frankfurt (Deutschland)	Einzelne Datei / Seite	nur bei Scan ohne Textebene + Freigabe	Mandant (Standard: aus)	getrennter Request · Vorschwärzung · kein Kontext
F-102	Bildgenerierung – externer Dienst	Data Center Frankfurt (Deutschland)	Bild-Prompt (optional PII-gefiltert)	nur bei Bild-Anfrage	Mandant (Standard: aus)	optional PII-Filter · kein Kontext
F-113	Weitere Sprachmodelle	Externe Hoster mit Datenresidenz Deutschland	Einzelner Prompt + erforderlicher Kontext (optional PII-gefiltert)	nur bei Wahl eines externen Modells	Mandant + Nutzer (Standard: aus)	optional PII-Filter · UI-Kennzeichnung · Audit je Anfrage
F-013	Identity Provider des Kunden	Kunde	Identitätsattribute (Name, E-Mail, Gruppen)	Login	Kunde (Konfiguration)	OIDC/SAML signiert · TLS 1.3
F-042 · F-144	Kundensysteme (DMS, Fachverfahren)	Kunde	Dokumente / Vorgangsdaten des Kunden	MCP-Konnektor	Kunde (je Konnektor)	mTLS/VPN · Servicekonten · Least Privilege
F-203	E-Mail-Versand (Benachrichtigungen)	H24-Mailrelay Deutschland → Empfänger	Benachrichtigungstexte, keine Inhalte	Ereignis	–	SMTP-TLS · DKIM/SPF
F-205	Kundenseitiges SIEM	Kunde	Audit-Ereignisse des Mandanten	kontinuierlich	Kunde	Syslog-TLS
F-213	Zweiter Standort Deutschland	Deutschland	Verschlüsselte Backups	kontinuierlich / zyklisch	–	WireGuard · Object Lock · Schlüssel nicht am Ziel
Betrieb	Paket-/Image-Quellen (Updates)	Spiegel in Deutschland	keine Kundendaten	Wartung	–	Signaturprüfung · nur aus Management-Netz

EXTERN · OPTIONAL

INFRASTRUKTUR DES KUNDEN

BACKUP-STANDORT DE

BETRIEB

H24-MAILRELAY DE

Jede Nutzung beginnt mit einer authentifizierten Sitzung. Findus One nutzt einen zentralen Identity & Access Service (P-12), der entweder lokale Konten (nur Superuser/Notfall) oder – Regelfall im öffentlichen Bereich – die Föderation mit dem Identity Provider des Kunden (E-30) verwendet. Passwörter werden nie im Klartext übertragen oder gespeichert (Anforderung 3).

ÜBERTRAGUNG AN EXTERNE SYSTEME (Z7)

Keine. Die Föderation zum Kunden-IdP ist eine Verbindung zwischen H24-Zone und Kundenzone; übertragen werden Identitätsattribute.

SPEICHERUNG

Nutzerstammdaten und Rollen in S-01; Session-Referenzen flüchtig in S-04; Audit-Ereignisse in S-06.

BETEILIGTE KOMPONENTEN

- E-01 Browser / PWA
- P-03 Load Balancer (HA)
- P-10 Web-Frontend (PWA)
- P-11 Backend / API-Orchestrator
- P-12 Identity & Access
- E-30 Identity Provider des Kunden
- S-01 PostgreSQL
- S-04 Redis
- P-18 Audit-Log-Service



S1 · Anmeldung, Single Sign-On und Sitzung — 9 Datenflüsse; Spalten = Zonen, Pfeile = Datenflüsse in Reihenfolge, orange = Übergang zu externen Diensten (opt-in), violett = Kundeninfrastruktur.

Der Kernfluss der Plattform: Ein Prompt wird vom Backend validiert, optional pseudonymisiert, durch Guardrails geprüft, an Findus Prima übergeben und als Stream zurück an den Anwender geliefert. Alle beteiligten Prozesse liegen in Z2 und Z3 im Dedicated Data Center Deutschland.

ÜBERTRAGUNG AN EXTERNE SYSTEME (Z7)

Keine. Findus Prima läuft auf H24-GPUs im Dedicated Data Center Deutschland.

SPEICHERUNG

Konversation in S-01 (löschar); KV-Cache in P-30 nur während der Anfrage im GPU-Speicher; keine Speicherung im Modell.

BETEILIGTE KOMPONENTEN

E-01 Browser / PWA

P-03 Load Balancer (HA)

P-11 Backend / API-Orchestrator

P-39 Guardrail-Service

P-38 PII-Service (Presidio)

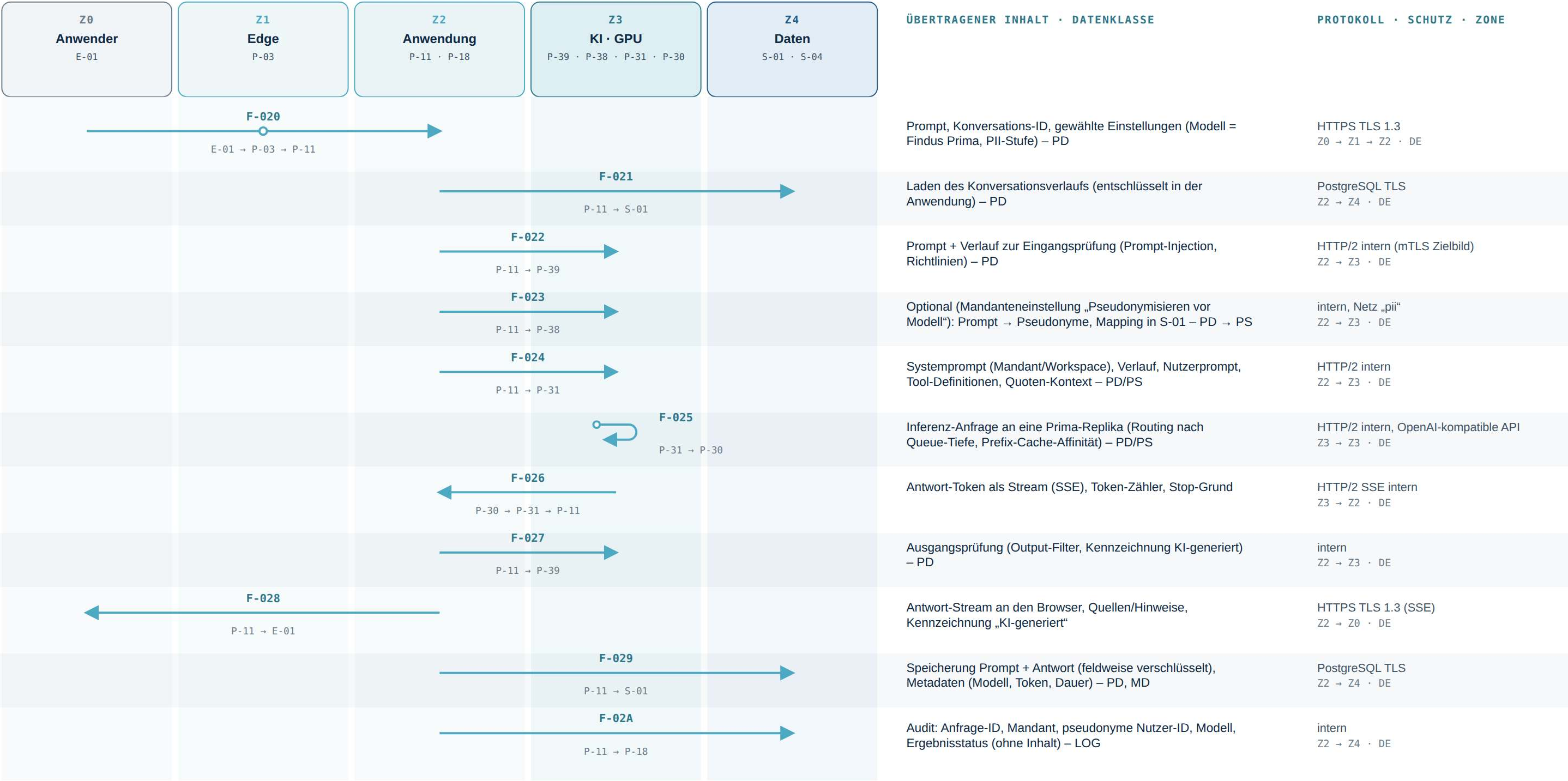
P-31 Modell-Router

P-30 Findus Prima Inferenz

S-01 PostgreSQL

S-04 Redis

P-18 Audit-Log-Service



S2 · Standard-Chat mit Findus Prima (Findus GPT) — 11 Datenflüsse; Spalten = Zonen, Pfeile = Datenflüsse in Reihenfolge, orange = Übergang zu externen Diensten (opt-in), violett = Kundeninfrastruktur.

Beim Upload wird die Datei geprüft, im Objektspeicher abgelegt, durch die Dokumentenverarbeitung in Text und Struktur zerlegt und – je nach Größe – entweder direkt in den Prompt-Kontext (bis 200.000 Token) oder über Embeddings und Retrieval in die Antwort eingebracht. Gescannte Dokumente durchlaufen die OCR; bei aktivierter Mandantenfreigabe kann für komplexe Vorlagen der externe OCR-Dienst im Data Center Frankfurt genutzt werden – dann verlässt genau diese eine Datei die Zone (situativ).

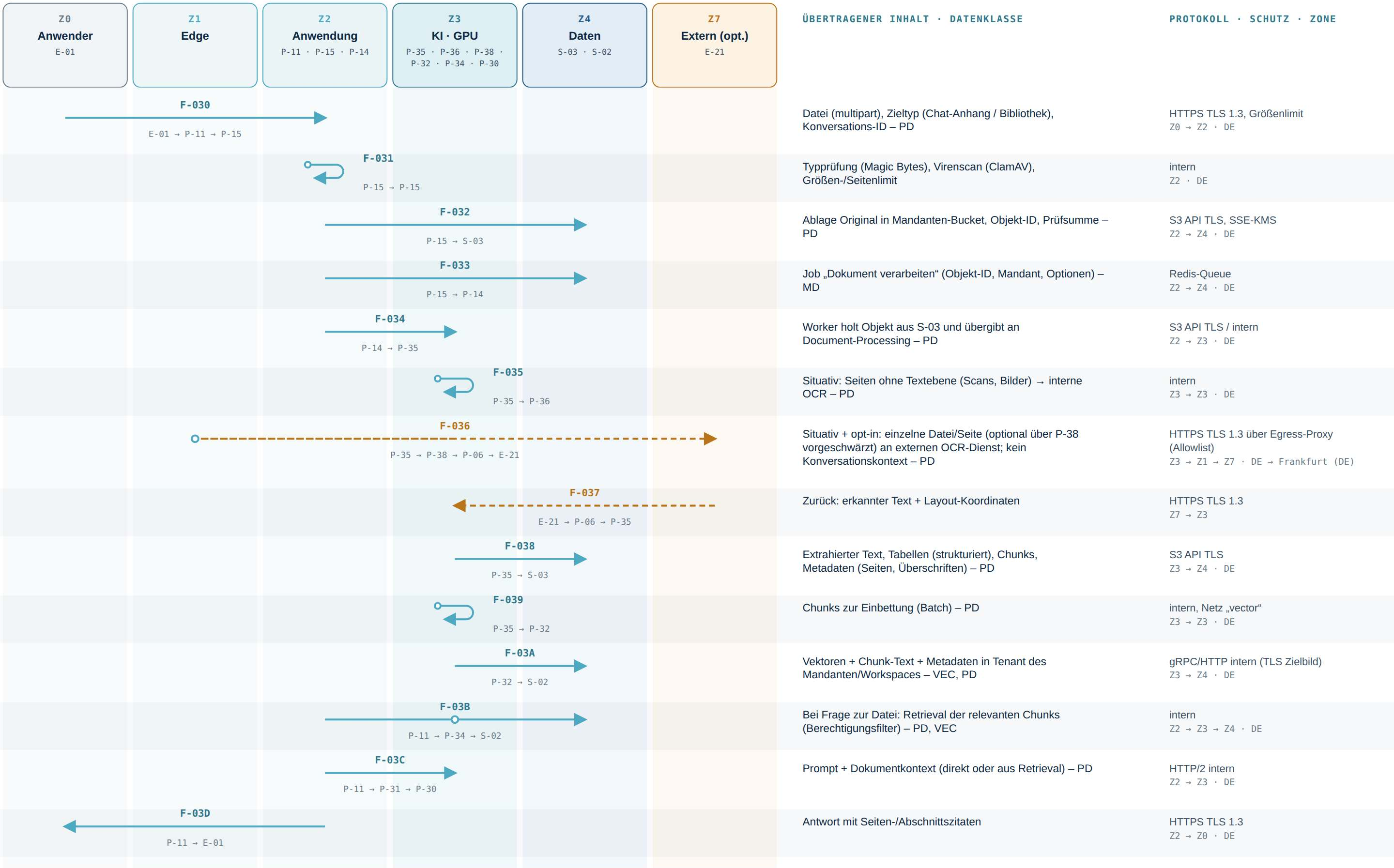
ÜBERTRAGUNG AN EXTERNE SYSTEME (Z7)

Im situativen, mandantenseitig freigegebenen OCR-Pfad (F-036): die einzelne Datei bzw. Seite – ohne Prompt, Verlauf und Nutzerkennung – an den OCR-Dienst im Data Center Frankfurt (Deutschland). Standardpfad: interne OCR ohne externe Übertragung.

SPEICHERUNG

Original in S-03; Artefakte in S-03; Vektoren in S-02; Verweis in S-01. Kaskadierende Löschung bei Löschen der Konversation/Datei.

BETEILIGTE KOMPONENTEN



S3 · Chat mit Datei-Upload (PDF, DOCX, CSV, XLSX, Bilder) und Dokumentenverarbeitung — 14 Datenflüsse; Spalten = Zonen, Pfeile = Datenflüsse in Reihenfolge, orange = Übergang zu externen Diensten (opt-in), violett = Kundeninfrastruktur.

Bibliothek (persönlich/Workspace) und Wissenshub (organisationsweit, Enterprise) verwenden dieselbe Ingestion-Pipeline wie der Datei-Upload, jedoch mit dauerhafter Speicherung, Versionierung, Freigabesteuerung und optionalen Quellenkonnektoren (DMS, SharePoint, Dateiablagen, Websites des Kunden). Für das Diagramm ist wichtig: Alle Quelldaten werden in die Datenzone des Dedicated Data Center Deutschland kopiert und dort indexiert; Konnektoren ziehen Daten (Pull), nie umgekehrt.

ÜBERTRAGUNG AN EXTERNE SYSTEME (Z7)

Keine. Konnektoren zu Kundenquellen (E-31) sind Verbindungen in die Kundenzone, kein Drittland, kein Unterauftragnehmer.

SPEICHERUNG

Dauerhaft in S-03 (Original + Artefakte), S-02 (Tenant je Wissensbasis/Mandant), S-01 (Metadaten/ACL).

BETEILIGTE KOMPONENTEN

- E-01 Browser / PWA
- E-05 Administrator
- P-11 Backend / API-Orchestrator
- P-15 File-Service
- P-42 Agenten-Runtime & MCP
- E-31 Fachverfahren / DMS
- P-14 Job-Queue & Worker
- P-35 Document-Processing
- P-36 OCR intern
- P-32 Embedding-Service
- S-02 Weaviate Vektorindex
- S-03 MinIO Objektspeicher
- S-01 PostgreSQL
- P-17 Admin-Konsole



ÜBERTRAGENER INHALT · DATENKLASSE

PROTOKOLL · SCHUTZ · ZONE

Anlegen einer Wissensbasis: Name, Freigaberollen, Quellen, Aktualisierungsintervall – MD	HTTPS TLS 1.3 Z0 → Z2 · DE
Manueller Upload in Bibliothek/Wissensbasis (wie F-030) – PD	HTTPS TLS 1.3 Z0 → Z2 · DE
Opt-in: Abruf von Dokumenten aus Kundenquelle mit kundenseitigem Servicekonto (Least Privilege, read-only) – Authentifizierung	HTTPS/mTLS oder Site-to-Site-VPN Z3 → Z8 · DE → Kunde
Dokumente, Änderungsstände (Delta-Sync), ACL-Informationen (wer darf sehen) – PD, MD	HTTPS/mTLS, S3 TLS Z8 → Z3 → Z4 · DE
Verarbeitung wie S3 (Parsing, OCR, Chunking, Embeddings) – PD → VEC	intern Z2/Z3 → Z4 · DE
Dokument-Metadaten, Version, Quell-ACL → Berechtigungsfilter, Indexstatus – MD	PostgreSQL TLS Z3 → Z4 · DE
Zyklischer Re-Sync (z. B. stündlich/täglich) und Re-Indexierung bei Modellwechsel des Embeddings	intern, geplant Z2 · DE
Audit: Wissensbasis angelegt/geändert, Freigaben, Konnektor aktiviert – LOG	intern Z2 → Z4 · DE

S4 · Findus Bibliothek und Findus Wissenshub – Ingestion (RAG-Indexierung) — 8 Datenflüsse; Spalten = Zonen, Pfeile = Datenflüsse in Reihenfolge, orange = Übergang zu externen Diensten (opt-in), violett = Kundeninfrastruktur.

Fragen an Bibliothek oder Wissenshub werden semantisch (Vektor) und lexikalisch (BM25) gesucht, nach Berechtigung gefiltert, nachsortiert (Reranker) und mit Quellenangaben an Findus Prima übergeben. Der gesamte Pfad bleibt in Z2–Z4.

ÜBERTRAGUNG AN EXTERNE SYSTEME (Z7)
Keine.

SPEICHERUNG
Wie S2; zusätzlich Quellenliste je Antwort in S-01.

BETEILIGTE KOMPONENTEN

E-01 Browser / PWA

P-11 Backend / API-Orchestrator

P-38 PII-Service (Presidio)

P-32 Embedding-Service

P-34 Retrieval-Service

S-02 Weaviate Vektorindex

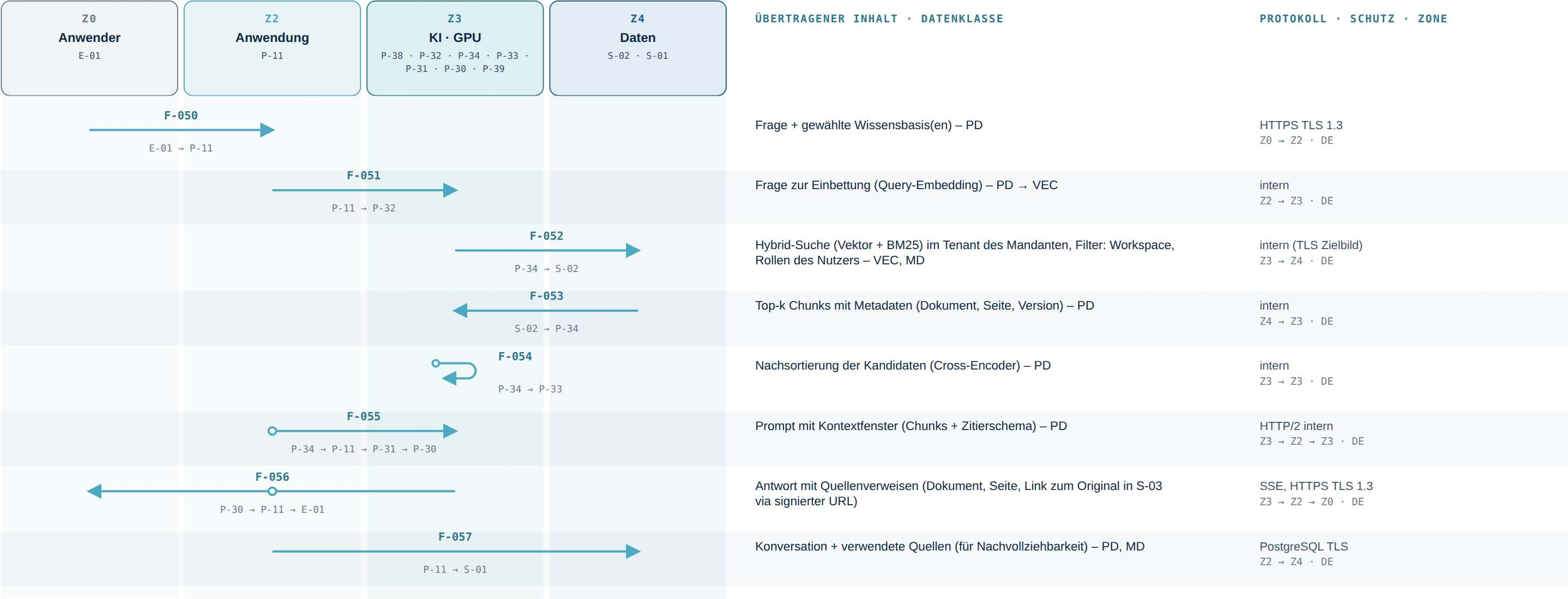
S-01 PostgreSQL

P-33 Reranker

P-31 Modell-Router

P-30 Findus Prima Inferenz

P-39 Guardrail-Service



S5 · RAG-Anfrage (Retrieval-Augmented Generation) — 8 Datenflüsse; Spalten = Zonen, Pfeile = Datenflüsse in Reihenfolge, orange = Übergang zu externen Diensten (opt-in), violett = Kundeninfrastruktur.

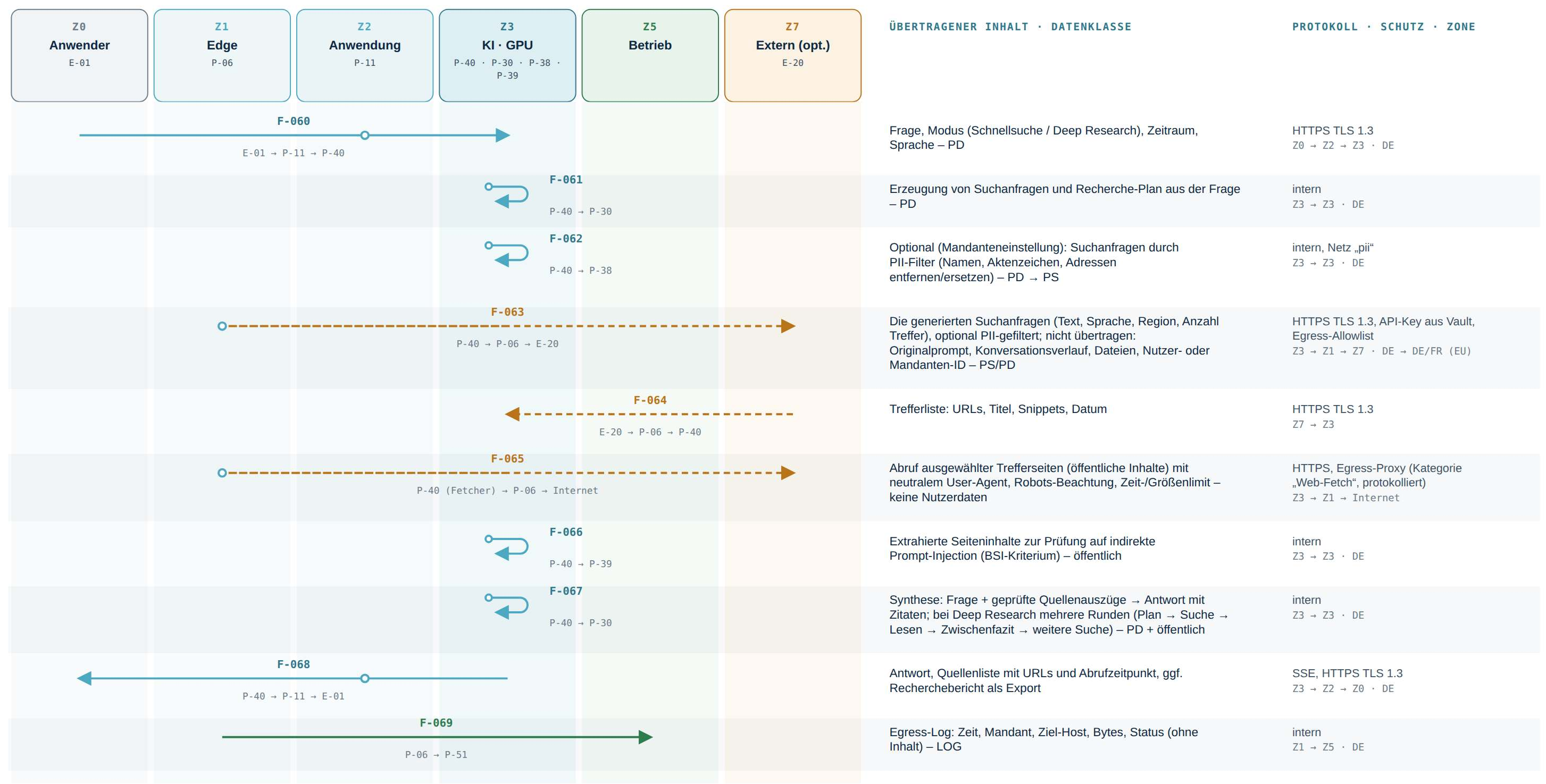
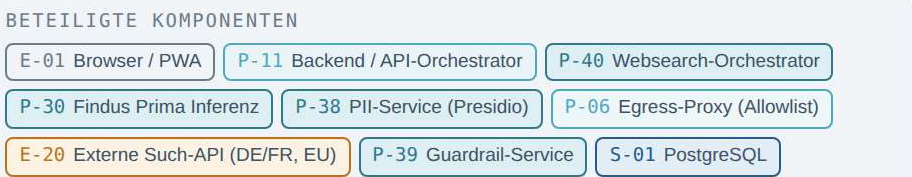
Findus Suche ist der einzige Standardpfad, der Informationen aus dem Internet einbezieht. Die Nutzerfrage selbst verlässt die Zone nicht: Findus Prima formuliert aus der Frage eine oder mehrere Suchanfragen, diese werden durch den PII-Service geprüft und über den Egress-Proxy an die externe Such-API (Deutschland/Frankreich, EU) gesendet. Trefferseiten werden durch einen Fetcher in Z3 geladen, extrahiert, bewertet und von Findus Prima zu einer Antwort mit Zitaten verdichtet. Deep Research wiederholt diesen Zyklus geplant über mehrere Runden.

ÜBERTRAGUNG AN EXTERNE SYSTEME (Z7)

Die vom Modell generierten Suchanfragen (F-063, optional PII-gefiltert) an die externe Such-API (Deutschland/Frankreich, EU) sowie Abrufe öffentlicher Webseiten (F-065). Nicht übertragen: Originalprompt, Konversationsverlauf, hochgeladene Dateien, Nutzer- oder Mandantenkennung.

SPEICHERUNG

Konversation inkl. Quellenliste in S-01; Seiteninhalte werden nicht persistiert (nur Zitate in der Antwort).

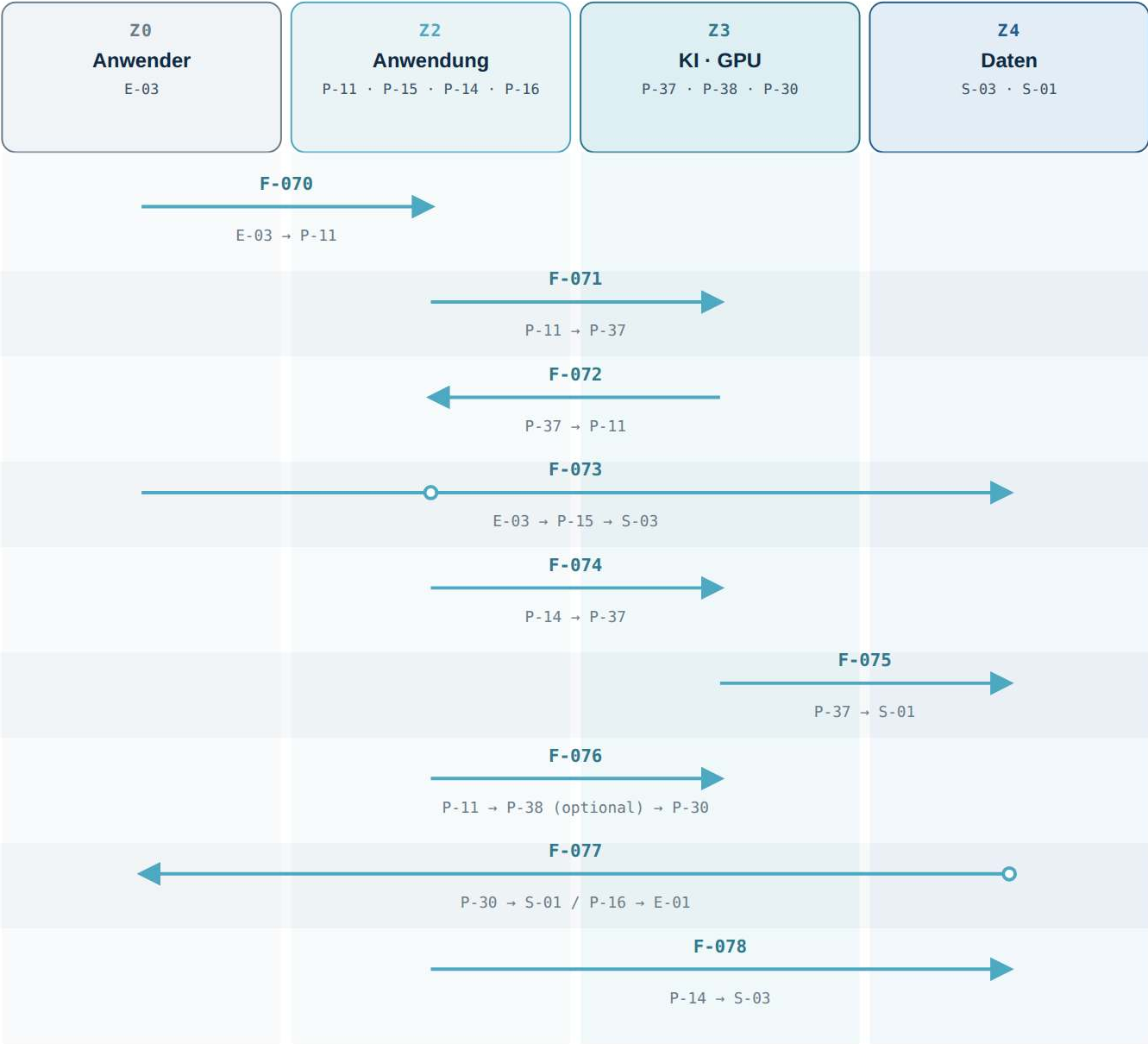


S6 · Findus Suche – Websuche und Deep Research — 10 Datenflüsse; Spalten = Zonen, Pfeile = Datenflüsse in Reihenfolge, orange = Übergang zu externen Diensten (opt-in), violett = Kundeninfrastruktur.

Findus Voice umfasst zwei Nutzungsarten: (a) Sprachsteuerung der KI (kurze Audio-Eingaben, die als Prompt transkribiert werden) und (b) Aufzeichnung von Besprechungen mit anschließender Transkription (bis 57 Sprachen), Sprechertrennung und automatischer Protokollerstellung. Die Transkription läuft im Findus-Prima-Stack auf H24-GPUs; Audiodaten werden nur temporär gespeichert.

ÜBERTRAGUNG AN EXTERNE SYSTEME (Z7)
Keine. Transkription und Protokollerstellung erfolgen vollständig im Dedicated Data Center Deutschland.

SPEICHERUNG
Audio nur temporär (TTL) in S-03 und ausdrücklich nicht in Backups [Zielbild];
Transkript und Protokoll in S-01.



ÜBERTRAGENER INHALT · DATENKLASSE	PROTOKOLL · SCHUTZ · ZONE
Sprachsteuerung: Audio-Chunks (WebRTC/WebSocket) oder Audiodatei – PD	WSS TLS 1.3 Z0 → Z2 · DE
Streaming-Transkription (Sprache → Text, Sprache erkannt) – PD	intern Z2 → Z3 · DE
Transkript-Text → wird als Prompt in S2 weiterverarbeitet	intern Z3 → Z2 · DE
Meeting-Aufzeichnung: Audiodatei (Upload nach Ende oder Chunk-Upload während der Sitzung) – PD	HTTPS TLS 1.3, SSE-KMS, TTL-Bucket Z0 → Z2 → Z4 · DE
Job: Transkription + Diarisierung („Sprecher 1/2/...“, optional Namenszuordnung durch Nutzer) – PD	intern Z2 → Z3 · DE
Transkript mit Zeitmarken und Sprechern – PD	PostgreSQL TLS Z3 → Z4 · DE
Protokollerstellung: Transkript → strukturiertes Protokoll (TOP, Beschlüsse, Aufgaben) mit Findus Prima – PD	intern Z2 → Z3 · DE
Protokoll speichern; Export als DOCX/PDF; Download über signierte URL	PostgreSQL TLS, HTTPS TLS 1.3 Z3 → Z4 / Z2 → Z0 · DE
Löschjob: Audio-Rohdaten nach erfolgreicher Transkription bzw. spätestens nach TTL löschen – BAK-Ausschluss	S3 API Z2 → Z4 · DE

S7 · Findus Voice – Sprachsteuerung und Meeting-Protokolle (optionales Modul) — 9 Datenflüsse; Spalten = Zonen, Pfeile = Datenflüsse in Reihenfolge, orange = Übergang zu externen Diensten (opt-in), violett = Kundeninfrastruktur.

Findus E-Mail ist ein optionales Modul. Das Outlook-Add-in läuft im E-Mail-Client des Kunden (Desktop/Web) und sendet auf Aufforderung des Nutzers den markierten E-Mail-Text bzw. Entwurf an die Findus-API. Die Antwort (Entwurf, Optimierung, Zusammenfassung, Antwortvorschlag) wird im Add-in angezeigt und vom Nutzer übernommen. Findus One greift nicht selbstständig auf das Postfach zu.

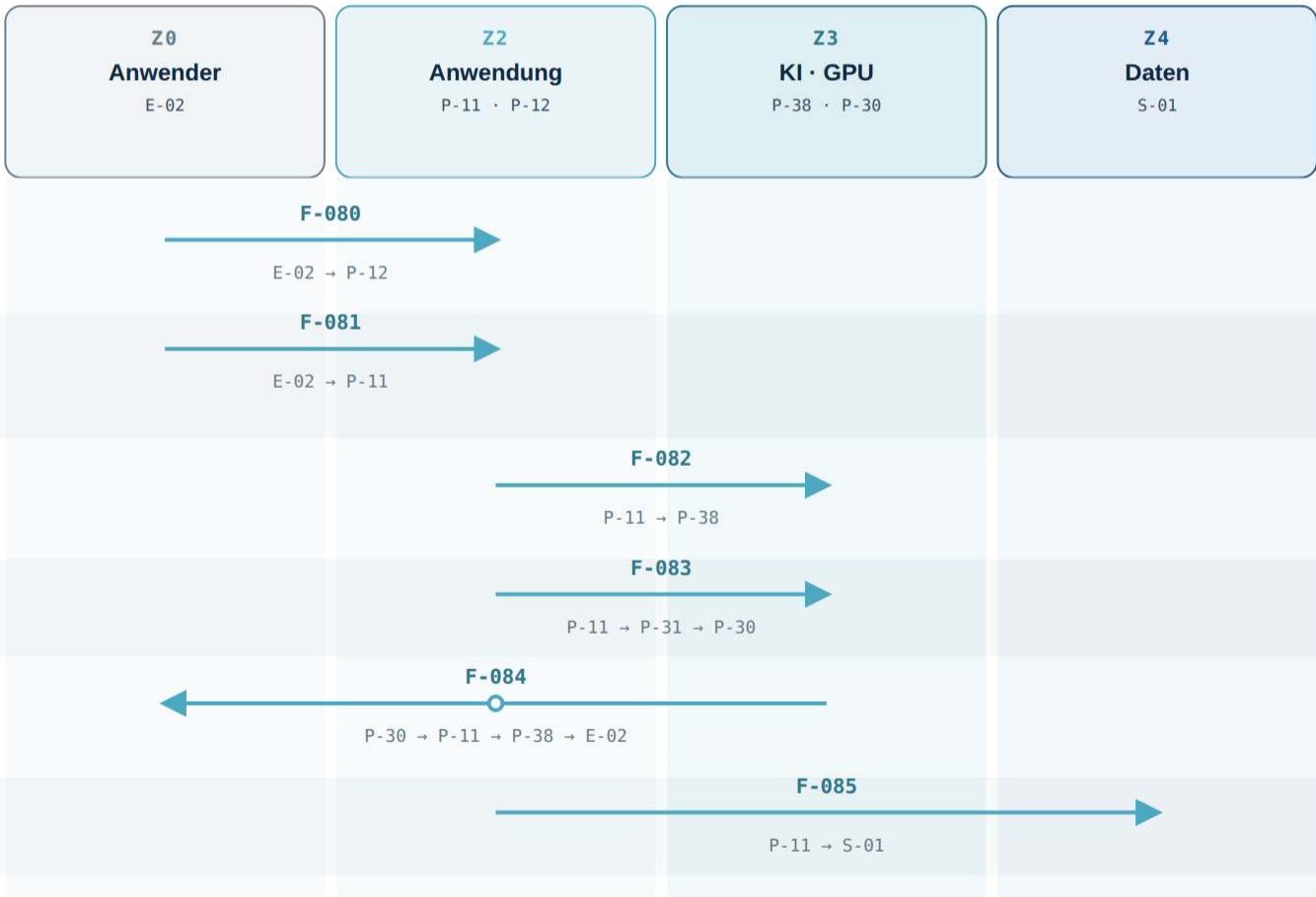
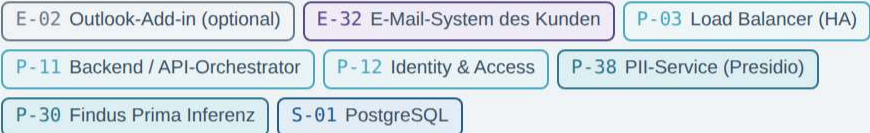
ÜBERTRAGUNG AN EXTERNE SYSTEME (Z7)

Keine. Die E-Mail selbst bleibt im E-Mail-System des Kunden (Z8); an H24 wird nur der vom Nutzer gewählte Text übertragen.

SPEICHERUNG

Standard flüchtig; auf Wunsch in S-01.

BETEILIGTE KOMPONENTEN



ÜBERTRAGENER INHALT · DATENKLASSE

PROTOKOLL · SCHUTZ · ZONE

SSO-Anmeldung des Add-ins (OIDC, Token im Add-in-Kontext) – ID	HTTPS TLS 1.3 Z0 → Z2 · DE
Aktion (Entwurf/Optimieren/Zusammenfassen/Antworten), E-Mail-Text bzw. Thread-Auszug, Betreff, gewünschter Ton; keine Anhänge außer explizit ausgewählt – PD	HTTPS TLS 1.3 Z0 → Z2 · DE
Optional (Mandanteneinstellung): Pseudonymisierung → Namen/Adressen ersetzen – PD → PS	intern Z2 → Z3 · DE
Prompt mit E-Mail-Inhalt → Findus Prima – PD/PS	intern Z2 → Z3 · DE
Ergebnis; bei aktivierter Pseudonymisierung Re-Identifikation vor Rückgabe; Anzeige im Add-in	HTTPS TLS 1.3 Z3 → Z2 → Z0 · DE
Optional (Nutzerentscheidung „im Verlauf speichern“): Konversation; Standard: keine Speicherung, nur Audit-Metadaten – PD/LOG	PostgreSQL TLS Z2 → Z4 · DE

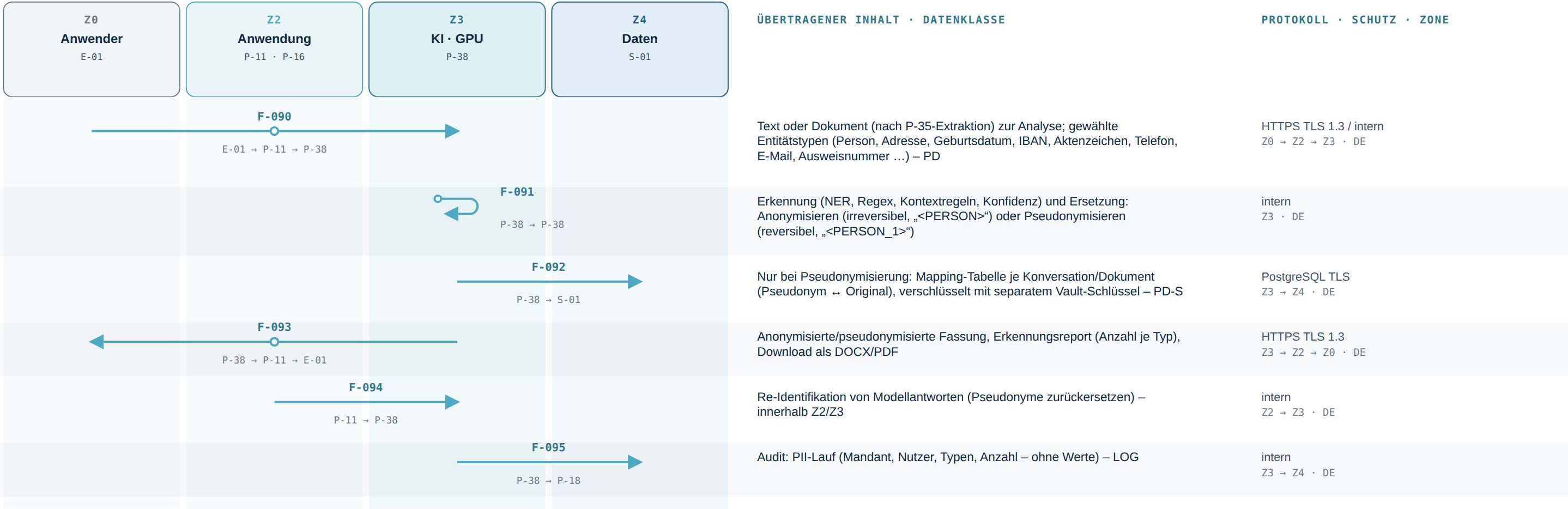
S8 · Findus E-Mail – Outlook-Add-in (optionales Modul) — 6 Datenflüsse; Spalten = Zonen, Pfeile = Datenflüsse in Reihenfolge, orange = Übergang zu externen Diensten (opt-in), violett = Kundeninfrastruktur.

Findus Identität ist sowohl ein eigenständiges Werkzeug (Dokument hochladen → anonymisierte Fassung erhalten) als auch ein optionaler Querschnittsdienst, der je Mandanteneinstellung in anderen Szenarien an definierten Punkten eingreift (vor dem Modellaufruf, vor externen Pfaden). Ohne Aktivierung werden Eingaben unverändert verarbeitet. Die Presidio-basierte Erkennung (NER + Muster für deutsche Identifikatoren) läuft im isolierten Docker-Netz „pii“. Das Mapping zwischen Pseudonym und Original wird getrennt und mit eigenem Schlüssel gespeichert und niemals nach außen gegeben.

ÜBERTRAGUNG AN EXTERNE SYSTEME (Z7)
Keine. P-38 kann je Mandanteneinstellung vor den Pfaden nach Z7 (F-036, F-063, F-102, F-112) aktiviert werden.

SPEICHERUNG
Mapping in S-01 (getrennte Tabelle, eigener Schlüssel); Ergebnisdokument in S-03.

BETEILIGTE KOMPONENTEN
E-01 Browser / PWA P-11 Backend / API-Orchestrator P-38 PII-Service (Presidio)
S-01 PostgreSQL P-54 Vault (Secrets & PKI) P-16 Export-Service



S9 · Findus Identität – Erkennung und Pseudonymisierung personenbezogener Daten — 6 Datenflüsse; Spalten = Zonen, Pfeile = Datenflüsse in Reihenfolge, orange = Übergang zu externen Diensten (opt-in), violett = Kundeninfrastruktur.

Bildgenerierung ist ein optionales, situatives Modul. Der Bild-Prompt wird – bei aktivierter PII-Filterung – pseudonymisiert und über den Egress-Proxy an den externen Bildgenerierungsdienst im Data Center Frankfurt (Deutschland) übergeben. Es wird ausschließlich der Prompt übertragen – kein Konversationskontext, keine Dateien. Das erzeugte Bild wird in MinIO abgelegt.

ÜBERTRAGUNG AN EXTERNE SYSTEME (Z7)

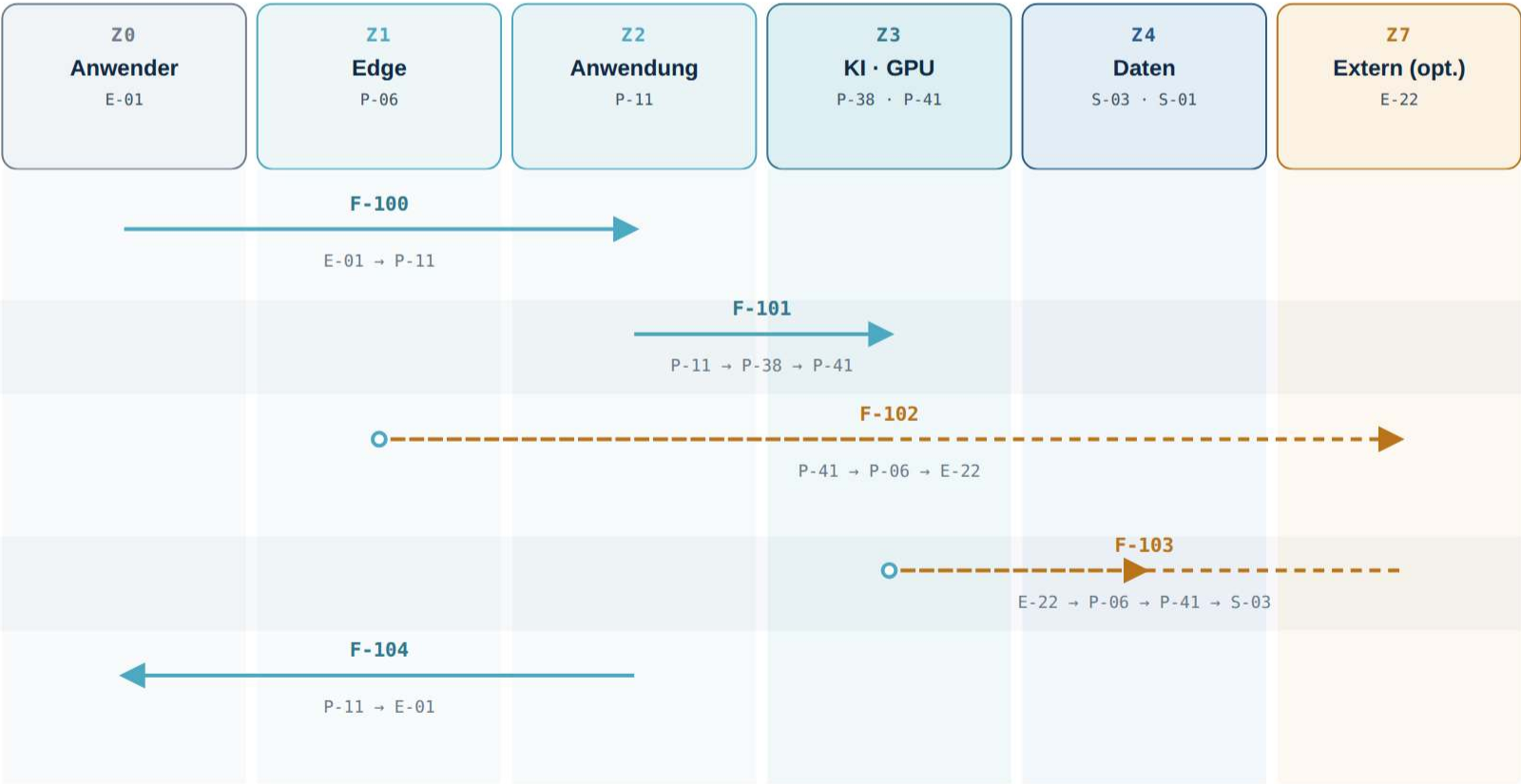
Der Bild-Prompt (F-102, optional PII-gefiltert) an den Bildgenerierungsdienst im Data Center Frankfurt (Deutschland). Zielbild-Option: self-hosted Bildmodell auf H24-GPUs in Z3.

SPEICHERUNG

Bild in S-03, Referenz in S-01.

BETEILIGTE KOMPONENTEN

- E-01 Browser / PWA
- P-11 Backend / API-Orchestrator
- P-38 PII-Service (Presidio)
- P-41 Bildgenerierungs-Adapter
- P-06 Egress-Proxy (Allowlist)
- E-22 Bildgenerierung – Data Center Frankfurt
- S-03 MinIO Objektspeicher
- S-01 PostgreSQL



ÜBERTRAGENER INHALT · DATENKLASSE

PROTOKOLL · SCHUTZ · ZONE

Bildwunsch (Prompt, Format, Stil) – PD	HTTPS TLS 1.3 Z0 → Z2 · DE
Optional: PII-Filter des Prompts (Mandanteneinstellung); Richtlinienprüfung (P-39) – PD/PS	intern Z2 → Z3 · DE
Opt-in Mandant: Bild-Prompt (optional PII-gefiltert) + Parameter; getrennter Request, keine Nutzer-/Mandantenkennung – PD/PS	HTTPS TLS 1.3, API-Key aus Vault, Egress-Allowlist Z3 → Z1 → Z7 · DE → Frankfurt (DE)
Bilddatei → Ablage im Mandanten-Bucket – MD	HTTPS TLS 1.3, S3 TLS Z7 → Z3 → Z4 · DE
Anzeige/Download (signierte URL), Kennzeichnung „KI-generiert“ (Art. 50 EU AI Act) inkl. Metadaten-Markierung [Zielbild: C2PA-Signatur]	HTTPS TLS 1.3 Z2 → Z0 · DE

S10 · Bildgenerierung (optionales Modul) — 5 Datenflüsse; Spalten = Zonen, Pfeile = Datenflüsse in Reihenfolge, orange = Übergang zu externen Diensten (opt-in), violett = Kundeninfrastruktur.

Findus One ist technologieoffen. Neben Findus Prima können Kunden auf ausdrücklichen Wunsch weitere Sprachmodelle (z. B. GPT, Mistral, Llama, EuroLLM, Gemini) freischalten, die bei externen Hostern mit Datenresidenz Deutschland betrieben werden – also in Rechenzentren in Deutschland mit vertraglich zugesicherter Datenverarbeitung ausschließlich in Deutschland. Dieser Pfad ist standardmäßig deaktiviert, wird je Mandant (und optional je Nutzer) freigegeben und im UI gekennzeichnet; die PII-Filterung kann je Mandant vorgeschaltet werden. Externe Modelle haben keinen Zugriff auf Datenspeicher der Plattform; Retrieval, Werkzeuge und Speicherung bleiben in der H24-Zone.

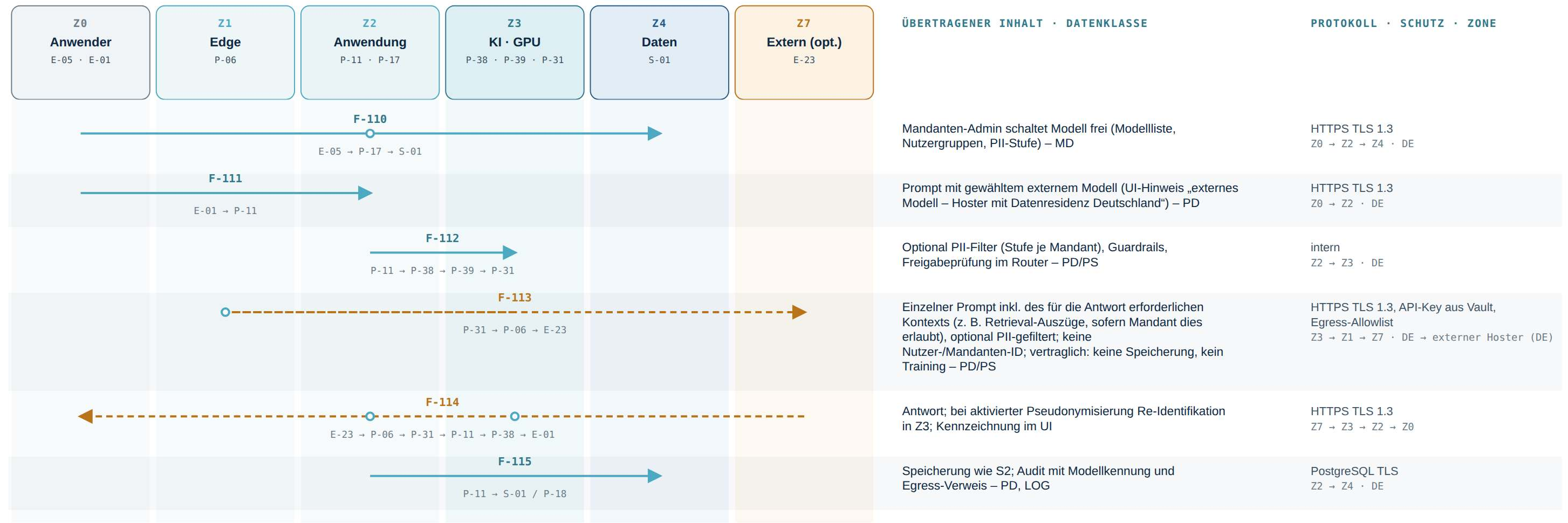
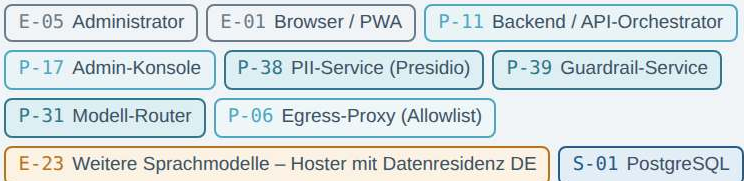
ÜBERTRAGUNG AN EXTERNE SYSTEME (Z7)

Der einzelne Prompt (optional PII-gefiltert) und der dafür erforderliche Kontext (F-113) zu einem externen Hostern mit Datenresidenz Deutschland – ausschließlich bei aktiver Mandantenfreigabe. Je freigegebenem Modell wird der Hostern im Diagramm namentlich mit Rechenzentrumsstandort in Deutschland genannt.

SPEICHERUNG

Wie S2 in S-01; beim externen Anbieter vertraglich keine Speicherung über die Verarbeitung hinaus.

BETEILIGTE KOMPONENTEN



S11 · Optionale Nutzung weiterer Sprachmodelle bei externen Hostern mit Datenresidenz Deutschland — 6 Datenflüsse; Spalten = Zonen, Pfeile = Datenflüsse in Reihenfolge, orange = Übergang zu externen Diensten (opt-in), violett = Kundeninfrastruktur.

Findus One stellt Werkzeuge nach dem Model Context Protocol (MCP) bereit. Findus Prima kann über strukturierte Werkzeugaufrufe (Tool Calling) Aktionen ausführen: Dateien lesen, Tabellen berechnen, in Wissensbasen suchen, Termine vorschlagen, Fachverfahren abfragen. Die Agenten-Runtime plant und führt mehrstufige Aufgaben aus, protokolliert jeden Schritt und fragt bei Schreib- oder Sendeaktionen eine Bestätigung des Nutzers ab.

ÜBERTRAGUNG AN EXTERNE SYSTEME (Z7)
Keine im Standard. Websuche als Werkzeug folgt S6 (nur Suchanfrage).
Fachverfahren liegen in der Kundenzone.

SPEICHERUNG
Ausführungsprotokolle in S-01; Arbeitsdateien in S-03.

BETEILIGTE KOMPONENTEN

E-01 Browser / PWA

P-11 Backend / API-Orchestrator

P-42 Agenten-Runtime & MCP

P-30 Findus Prima Inferenz

P-38 PII-Service (Presidio)

P-39 Guardrail-Service

S-01 PostgreSQL

S-03 MinIO Objektspeicher

E-31 Fachverfahren / DMS



S14 · MCP-Services und Agenten (Werkzeuganbindung) — 8 Datenflüsse; Spalten = Zonen, Pfeile = Datenflüsse in Reihenfolge, orange = Übergang zu externen Diensten (opt-in), violett = Kundeninfrastruktur.

Antworten, Protokolle, Recherchen und anonymisierte Dokumente können als Datei ausgegeben werden. Der Export-Service erzeugt die Datei in Z2, legt sie kurzzeitig im Objektspeicher ab und stellt sie über eine signierte, kurzlebige URL bereit.

ÜBERTRAGUNG AN EXTERNE SYSTEME (Z7)
Keine.

SPEICHERUNG
Exportdatei nur temporär (TTL) in S-03.

BETEILIGTE KOMPONENTEN

E-01 Browser / PWA

P-11 Backend / API-Orchestrator

P-16 Export-Service

S-03 MinIO Objektspeicher

P-03 Load Balancer (HA)



S16 · Datei-Ausgabe und Download (PDF, DOCX, CSV, XLSX, PPTX) — 5 Datenflüsse; Spalten = Zonen, Pfeile = Datenflüsse in Reihenfolge, orange = Übergang zu externen Diensten (opt-in), violett = Kundeninfrastruktur.

Die Admin-Konsole ist der Ort, an dem Kunden die Datenflüsse ihres Mandanten steuern: Welche Module sind aktiv, welche Modelle sind freigegeben, welche PII-Stufe gilt, wie lange werden Konversationen aufbewahrt, welche Konnektoren dürfen genutzt werden. Jede Änderung ist auditiert.

ÜBERTRAGUNG AN EXTERNE SYSTEME (Z7)

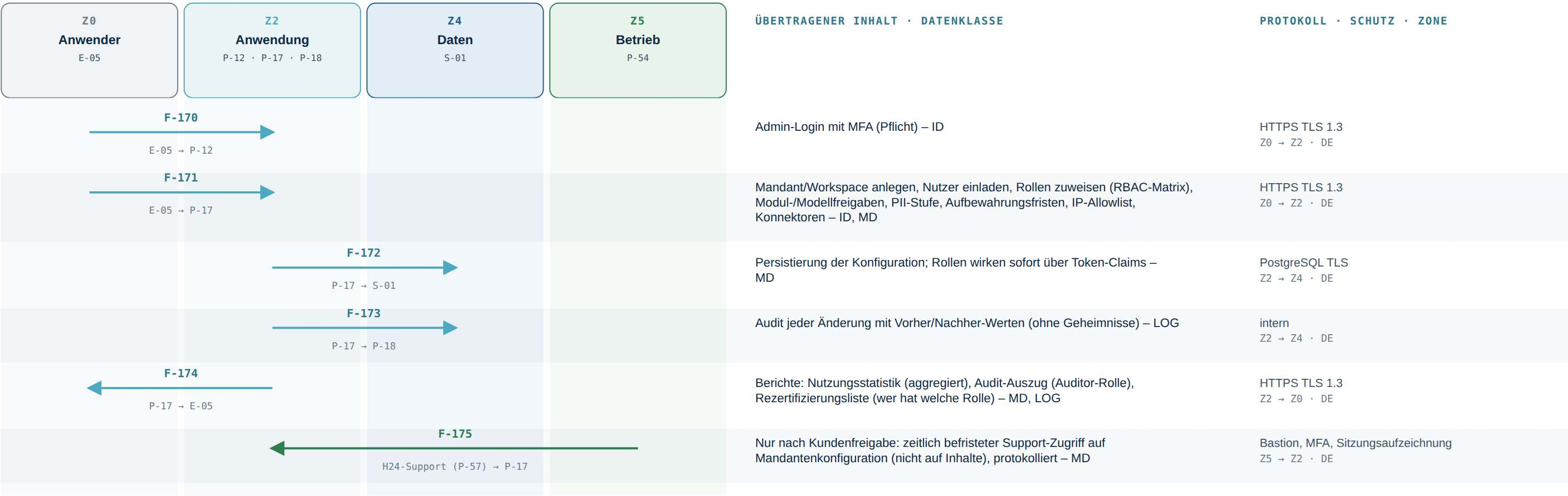
Keine.

SPEICHERUNG

S-01, S-06.

BETEILIGTE KOMPONENTEN

- E-05 Administrator
- P-12 Identity & Access
- P-17 Admin-Konsole
- S-01 PostgreSQL
- P-18 Audit-Log-Service
- P-54 Vault (Secrets & PKI)



S17 · Administration: Mandanten, Rollen, Freigaben, Rezertifizierung — 6 Datenflüsse; Spalten = Zonen, Pfeile = Datenflüsse in Reihenfolge, orange = Übergang zu externen Diensten (opt-in), violett = Kundeninfrastruktur.

Löschflüsse sind im Diagramm genauso wichtig wie Verarbeitungsflüsse: Sie belegen, dass Daten die Plattform tatsächlich wieder verlassen. Löschungen wirken kaskadierend über alle Datenspeicher und – nach Ablauf der Backup-Aufbewahrung – auch in den Sicherungen.

ÜBERTRAGUNG AN EXTERNE SYSTEME (Z7)
Keine.

SPEICHERUNG
Nur Löschnachweise in S-06.

BETEILIGTE KOMPONENTEN

E-01 Browser / PWA

E-05 Administrator

P-11 Backend / API-Orchestrator

P-17 Admin-Konsole

P-14 Job-Queue & Worker

S-01 PostgreSQL

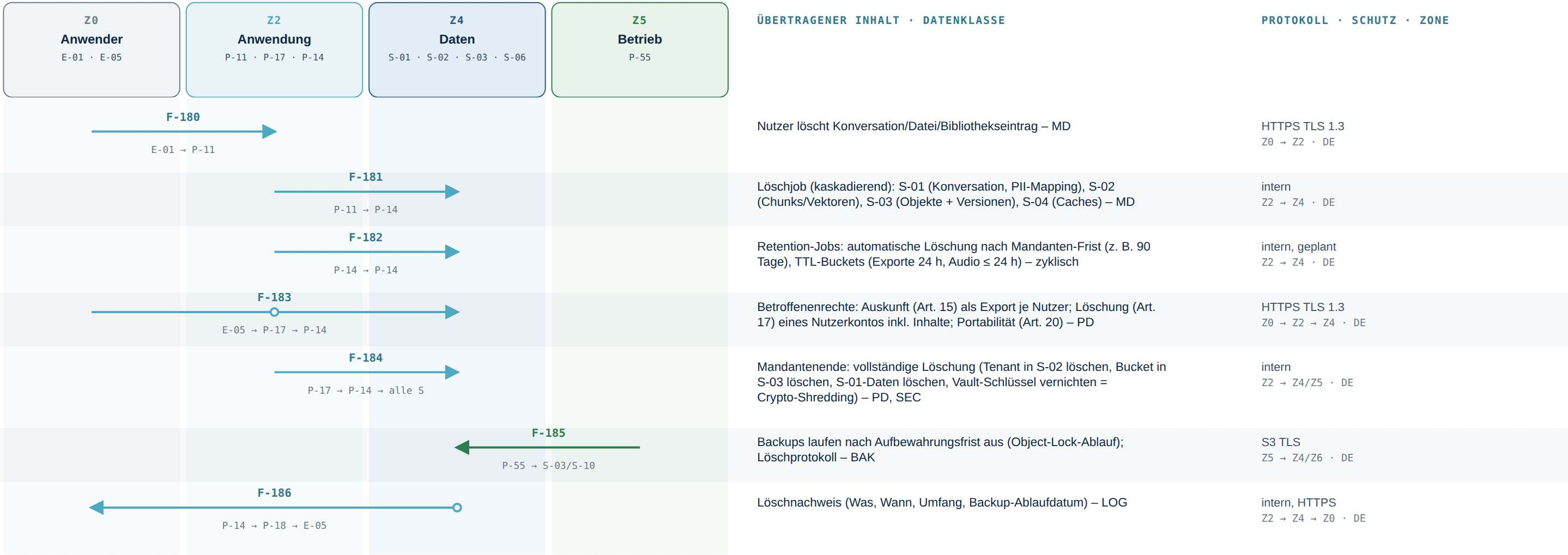
S-02 Weaviate Vektorindex

S-03 MinIO Objektspeicher

S-06 Audit-Log-Store

P-55 Backup-Orchestrierung

S-10 Backup-Repository Standort B



S18 · Löschung, Betroffenenrechte und Mandantenende — 7 Datenflüsse; Spalten = Zonen, Pfeile = Datenflüsse in Reihenfolge, orange = Übergang zu externen Diensten (opt-in), violett = Kundeninfrastruktur.

Das Schulungsmodul stellt Kurse, Wissensprüfungen und Zertifikate bereit. Es verarbeitet keine Inhaltsdaten, nur Identitäts- und Fortschrittsdaten.

ÜBERTRAGUNG AN EXTERNE SYSTEME (Z7)

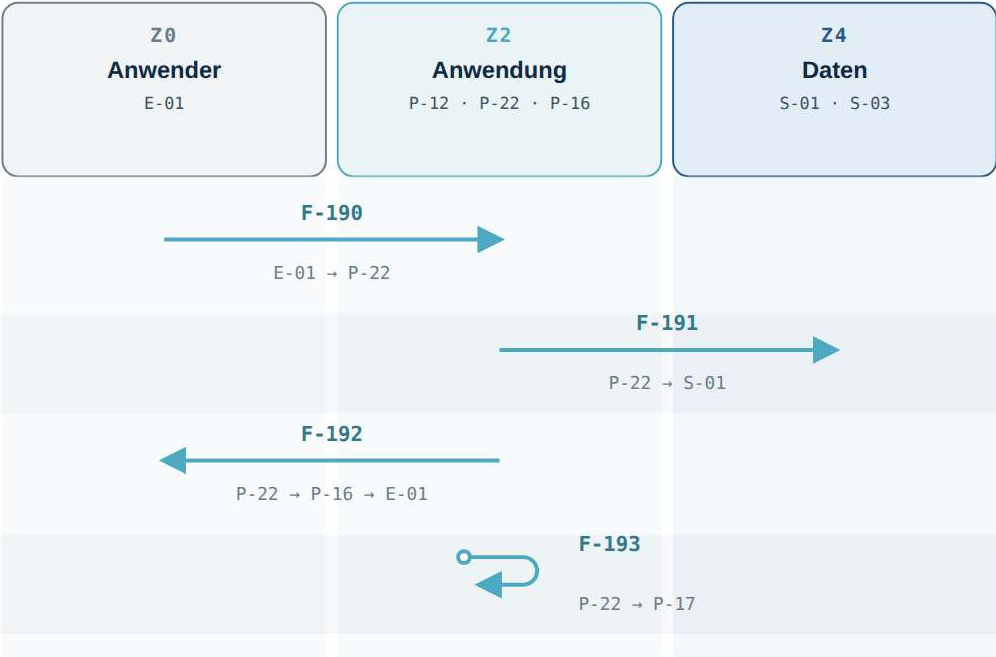
Keine.

SPEICHERUNG

S-01; Kursmedien (Videos) in S-03, ausgeliefert von der H24-Domain in Deutschland (kein externes Video-CDN) [Annahme].

BETEILIGTE KOMPONENTEN

- E-01 Browser / PWA
- P-12 Identity & Access
- P-22 Findus Schulung (LMS)
- S-01 PostgreSQL
- S-03 MinIO Objektspeicher
- P-16 Export-Service



ÜBERTRAGENER INHALT · DATENKLASSE

- Kursaufruf, Lernfortschritt, Prüfungsantworten – ID, MD
- Fortschritt, Ergebnis, Zertifikatsnummer, Datum – ID, MD
- Zertifikat (PDF) als Nachweis für die Dokumentationspflicht – MD
- Mandantenbericht: Schulungsquote (aggregiert), Nachweisliste für Admin – MD

PROTOKOLL · SCHUTZ · ZONE

- HTTPS TLS 1.3
Z0 → Z2 · DE
- PostgreSQL TLS
Z2 → Z4 · DE
- HTTPS TLS 1.3
Z2 → Z0 · DE
- intern
Z2 → Z2 · DE

S19 · Findus Schulung (KI-Kompetenz nach Art. 4 EU AI Act, optionales Modul) — 4 Datenflüsse; Spalten = Zonen, Pfeile = Datenflüsse in Reihenfolge, orange = Übergang zu externen Diensten (opt-in), violett = Kundeninfrastruktur.

Der Monitoring-Stack (Prometheus, Grafana, Loki, Tempo, OpenTelemetry, GPU-Telemetrie) ist self-hosted in Z5; kein SaaS-Monitoring, keine externen Fehlerreporting-Dienste. Logs enthalten keine Prompt-Inhalte, Dateiinhalte oder PII-Mappings – protokolliert werden Ereignis, Zeit, Mandant, pseudonyme Nutzer-ID, Komponente, Ergebnis, Dauer, Token-Zähler, Modell und das Ziel eines Egress-Aufrufs.

ÜBERTRAGUNG AN EXTERNE SYSTEME

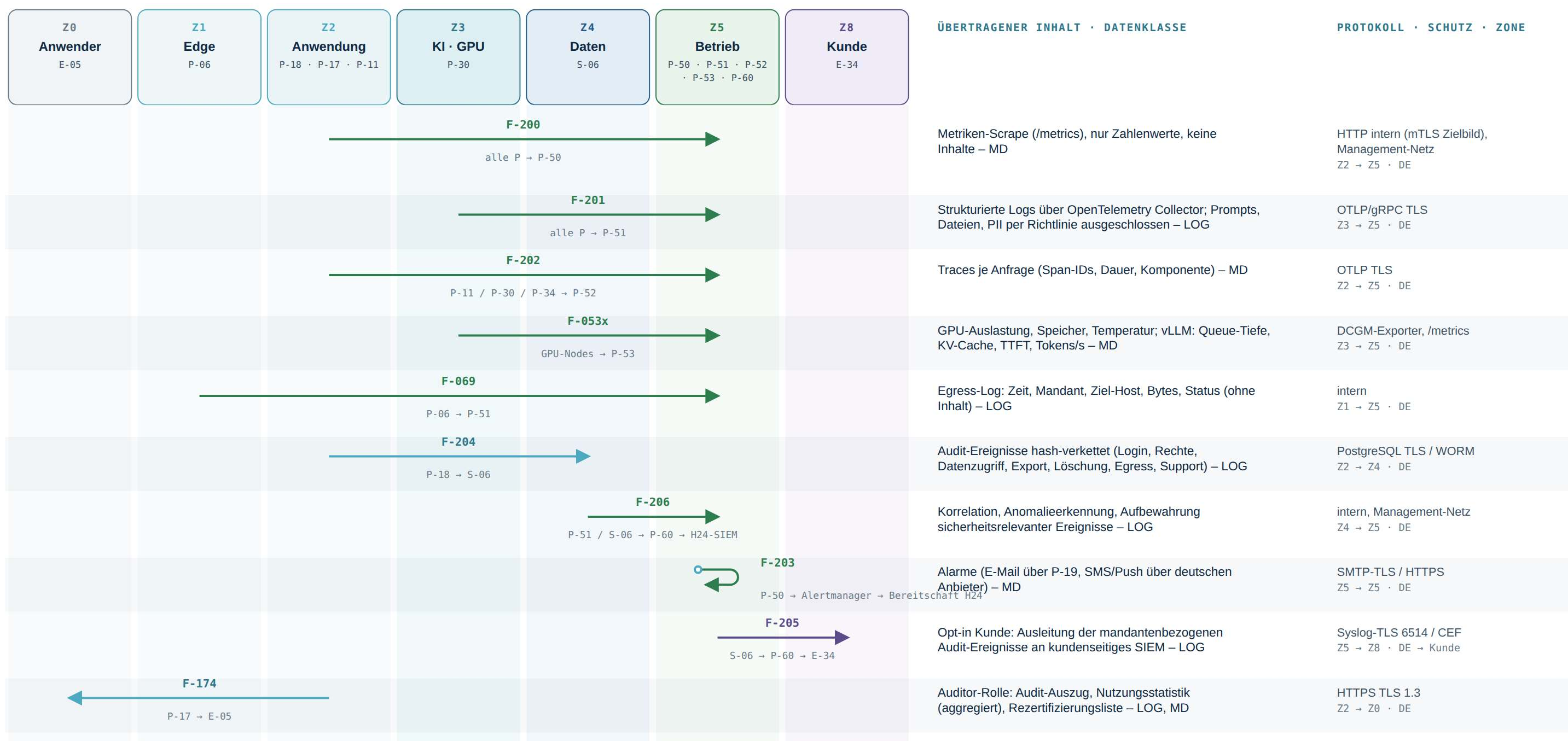
Keine. Optional: Ausleitung der mandantenbezogenen Audit-Ereignisse an das SIEM des Kunden (F-205, Syslog-TLS, opt-in).

AUFBEWAHRUNG

Audit ≥ 6 Monate (konfigurierbar ≤ 12), Betriebslogs 30 Tage, Metriken 13 Monate aggregiert; Hash-Verkettung je Mandant, täglicher Anker-Hash im WORM-Bucket.

BEISPIEL-ALARME

KV-Cache > 95 % für 2 min · TTFT p95 > 3 s · 5xx-Rate > 1 % · Egress zu nicht gelistetem Host · Replikationsverzug > 60 s · Backup älter als 8 h · Restore-Test fehlgeschlagen



D11 · Monitoring, Logging, Audit und SIEM — Betriebsflüsse: Ziele im Dedicated Data Center Deutschland bzw. am zweiten deutschen Standort; Ausleitung an ein Kunden-SIEM opt-in.

Schlüssel liegen in Vault (Z5) im Dedicated Data Center Deutschland, nicht am Backup-Standort. Backups: PostgreSQL mit pgBackRest und WAL-Archivierung (PITR, RPO ≤ 15 min), Weaviate-Backup je Tenant, MinIO Site Replication zum Standort B, Object Lock (WORM), 30 Tage + 12 Monatssicherungen, monatliche Restore-Tests. Deployment: nur signierte Images aus der H24-Registry, Test-Umgebung ohne Kundendaten. Fernwartung: ausschließlich über Bastion mit MFA, Just-in-Time-Zugriff und Sitzungsaufzeichnung.

ÜBERTRAGUNG AN EXTERNE SYSTEME

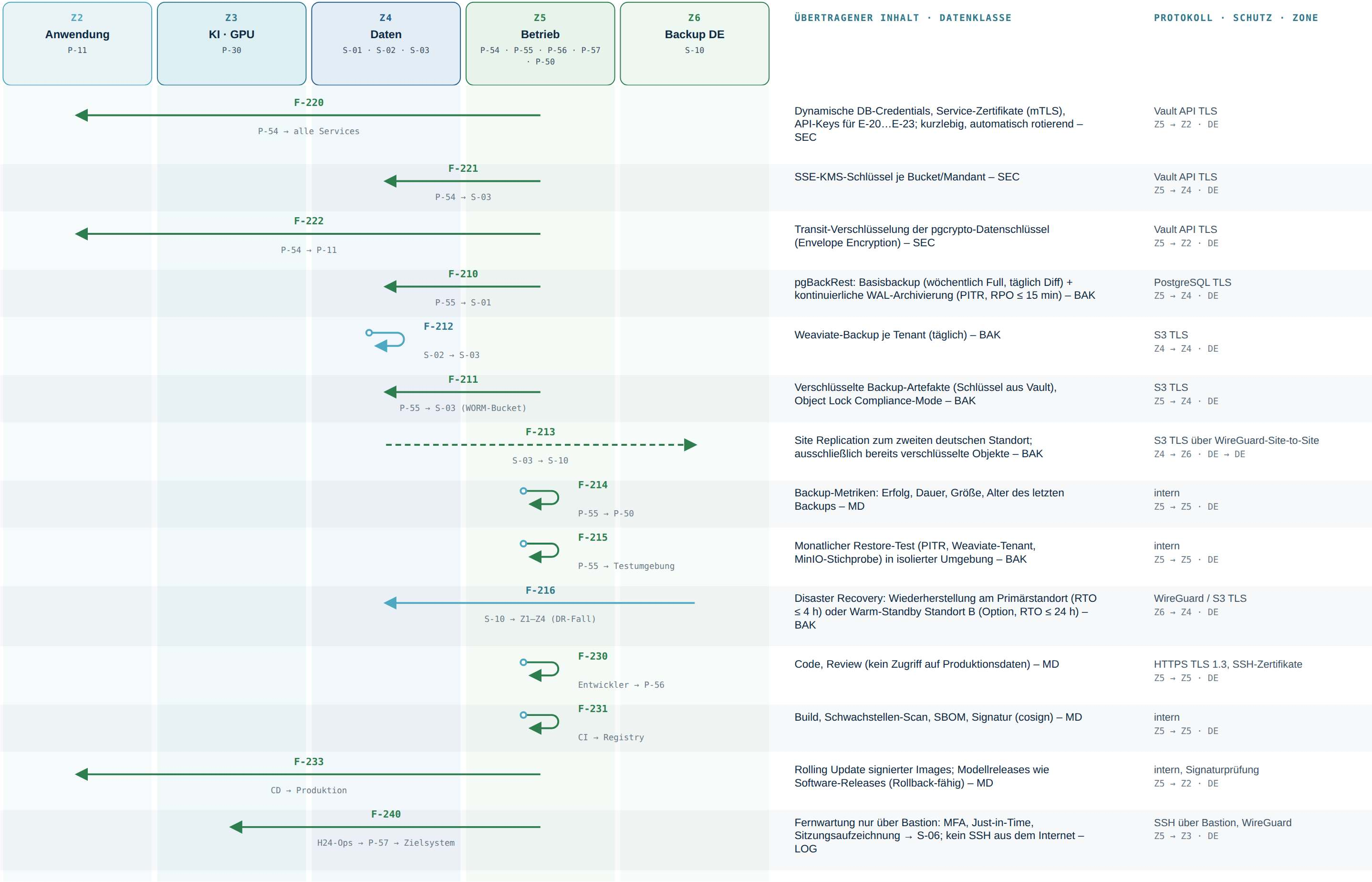
Keine. Backups gehen verschlüsselt zum zweiten Standort in Deutschland (F-213); Schlüssel bleiben in Vault.

RPO / RTO (ZIEL)

PostgreSQL RPO ≤ 15 min, RTO ≤ 4 h · Weaviate täglich, RTO ≤ 8 h · MinIO kontinuierlich, RTO ≤ 4 h · Vault täglich, RTO ≤ 2 h · Standortverlust: Warm-Standby Standort B, RTO ≤ 24 h (Option)

KEIN BACKUP (BEWUSST)

Audio-Rohdaten (TTL ≤ 24 h), Exportdateien (TTL 24 h), Redis (flüchtig) – damit Löschzusagen einhaltbar bleiben. Mandantenende: Crypto-Shredding der Vault-Schlüssel macht auch Backup-Kopien unlesbar.



D12 · Backup, Disaster Recovery, Schlüsselverwaltung, Deployment und Fernwartung — Betriebsflüsse; Ziele im Dedicated Data Center Deutschland bzw. am zweiten deutschen Standort; Ausleitung an ein Kunden-SIEM opt-in.

ZONEN

- Z0

Anwender-Endgerät
beim Kunden · außerhalb der H24-Zone
- Z1

Edge & Perimeter
Dedicated Data Center Deutschland
- Z2

Anwendung
Dedicated Data Center Deutschland
- Z3

KI-Verarbeitung · GPU
Dedicated Data Center Deutschland
- Z4

Daten
Dedicated Data Center Deutschland · internes Netz
- Z5

Betrieb & Sicherheit
Dedicated Data Center Deutschland
- Z6

Backup-Standort
Zweiter Standort Deutschland
- Z7

Externe Dienste (optional)
außerhalb des H24-Betriebs
- Z8

Infrastruktur des Kunden
beim Kunden

DATENKLASSEN

- PD

Personenbezogene Daten (Inhalt)
- PD-S

Besondere Kategorien (Art. 9 DSGVO) möglich
- PS

Pseudonymisierte Inhalte (bei aktivierter PII-Filterung)
- ID

Identitäts- und Zugangsdaten
- MD

Metadaten / Konfiguration
- VEC

Embeddings / Vektoren
- LOG

Audit- und Betriebsprotokolle
- SEC

Geheimnisse (nur Vault/PKI)
- BAK

Backups (verschlüsselt)

NOMENKLATUR

- P-nn

Prozess / Service (Container)
- S-nn

Datenspeicher
- E-nn

Externe Entität (Anwender, Kunde, Unterauftragnehmer)
- F-nnn

Datenfluss – eindeutige ID, identisch mit Konzept Kap. 9/10 und Flow-Register
- Z-n

Zone mit Vertrauensgrenze

PFEILE

- Kernfluss innerhalb der H24-Zone (TLS 1.3 / mTLS-Zielbild)
- Optionaler Fluss zu externen Diensten (Z7) – opt-in, über Egress-Proxy, optional
- Fluss in die Infrastruktur des Kunden (Z8) – nach Kundenweisung
- Backup zum zweiten deutschen Standort (Z6) – nur verschlüsselt
- Betriebsfluss (Monitoring, Logging, Secrets, Deployment)

KENNZEICHNUNGEN

- OPTIONAL

Modul wird je Mandant aktiviert; ohne Aktivierung existiert der Fluss nicht.
- SITUATIV

Nur wenn die konkrete Anfrage es erfordert (Backend entscheidet).
- ZIELBILD

Geplante Härtung gegenüber dem Ist-Stand (z. B. mTLS intern, AES-256).
- F-024

Flow-Chips an Karten: wichtigste ein-/ausgehende Datenflüsse der Komponente.