

# **SF1636 DATAKATALOG FOR FÆLLESKOMMUNAL REVISIONSLOG**

Version 1.0



Fælleskommunal Infrastruktur  
Datakatalog er senest opdateret: 2026.06.09

## Versionshistorik

Beskrivelsen er versioneret med et versionsnummer bestående af en hovedversion med tilhørende underversion. En underversion er altid bagud kompatibel.

Beskrivelsen kan ændres uden, at det medfører ændring af integrationens versionsnummer, fx ved præciseringer i teksten.

| Integrationsversion | Dato       | Kommentar                                                        |
|---------------------|------------|------------------------------------------------------------------|
| 1.0                 | 2026-06-09 | Første version af datakatalog og standardtekst for revisionslog. |

# Indhold

|                                                              |          |
|--------------------------------------------------------------|----------|
| <b>1. Overordnet beskrivelse.....</b>                        | <b>6</b> |
| 1.1. Design- og arkitekturprincipper .....                   | 6        |
| 1.2. Dannelse og afsendelse af NDJSON-leverancer.....        | 6        |
| 1.3. Filnavne .....                                          | 6        |
| 1.4. Idempotency .....                                       | 7        |
| 1.5. Ansvarsdeling: kontrol, markering og rapportering ..... | 7        |
| <b>2. Beskrivelser af elementerne i revisionsloggen.....</b> | <b>8</b> |
| 2.1. Leverance (første NDJSON-record).....                   | 8        |
| 2.1.1. leverance.recordType .....                            | 8        |
| 2.1.2. leverance.logID .....                                 | 9        |
| 2.1.3. leverance.myndCvr .....                               | 9        |
| 2.1.4. leverance.myndNavn .....                              | 10       |
| 2.1.5. leverance.afsendtSystemID.....                        | 11       |
| 2.1.6. leverance.afsendtSystemNavn .....                     | 11       |
| 2.1.7. leverance.fra .....                                   | 12       |
| 2.1.8. leverance.til .....                                   | 12       |
| 2.1.9. leverance.skemaVer .....                              | 13       |
| 2.1.10. leverance.teknCtx.....                               | 14       |
| 2.1.11. leverance.teknCtx.element .....                      | 14       |
| 2.2. Logregistrering (efterfølgende NDJSON-records) .....    | 16       |
| 2.2.1. logregistrering.recordType .....                      | 16       |
| 2.2.2. logregistrering.ID .....                              | 17       |
| 2.2.3. logregistrering.starttidspunkt.....                   | 17       |
| 2.2.4. logregistrering.sluttidspunkt .....                   | 18       |
| 2.2.5. logregistrering.operation.....                        | 18       |
| 2.2.6. logregistrering.operationTilstand.....                | 19       |
| 2.2.7. logregistrering.initSystemID .....                    | 20       |
| 2.2.8. logregistrering.initSystemNavn .....                  | 20       |
| 2.2.9. logregistrering.initBruger .....                      | 21       |
| 2.2.10. logregistrering.initOrgEnhedsID .....                | 22       |
| 2.2.11. logregistrering.initOrgEnhedsNavn.....               | 22       |
| 2.2.12. logregistrering.initOrgID .....                      | 23       |
| 2.2.13. logregistrering.initOrgNavn .....                    | 24       |
| 2.2.14. logregistrering.execSystemID .....                   | 24       |
| 2.2.15. logregistrering.execSystemNavn .....                 | 25       |
| 2.2.16. logregistrering.srcGdprBehandlKat .....              | 25       |
| 2.2.17. logregistrering.dstGdprBehandlKat .....              | 26       |
| 2.2.18. logregistrering.srcGdprDataKat.....                  | 27       |
| 2.2.19. logregistrering.dstGdprDataKat.....                  | 27       |
| 2.2.20. logregistrering.visteOpl.....                        | 28       |
| 2.2.21. logregistrering.visteOpl.element.....                | 29       |
| 2.2.22. logregistrering.personCpr.....                       | 29       |
| 2.2.23. logregistrering.behandlObj.....                      | 30       |
| 2.2.24. logregistrering.behandlObj.element.....              | 31       |
| 2.2.25. logregistrering.teknCtx.....                         | 32       |
| 2.2.26. logregistrering.teknCtx.element .....                | 33       |

# Læsevejledning

## Formål

Dette dokument er den fælles reference for, hvordan revisionslog udveksles i NDJSON-format mellem afsender og modtager. Dokumentet skal sikre ensartet implementering på tværs af systemer, gøre det muligt for modtager at validere leverancer og dokumentere kompletthed, understøtte revision/audit samt skabe et klart ansvarsskifte mellem afsender og modtager.

## Hvordan dokumentet bruges

For afsender: Brug dokumentet som implementeringsgrundlag for dannelse af NDJSON-filer, udfyldning af elementer samt overholdelse af sekvens- og tidsintervalkrav.

For modtager: Brug dokumentet som valideringsgrundlag til at afvise eller markere leverancer med strukturfejl, kodelistebrud, sekvensbrud eller tidsintervalbrud samt til løbende rapportering.

For drift og compliance: Brug dokumentet som fælles kontrakt ved fejlretning, genfremsendelser og dokumentation af revisionsspor.

## Dokumentets opbygning

Afsnit 2.1 beskriver Leverance-recorden, som fungerer som kuvert for NDJSON-filen. Afsnit 2.2 beskriver Logregistrering-records med konkrete loghændelser.

Detaljerede elementdefinitioner, herunder datatype, kardinalitet og eksempler, findes i Excel-datakataloget. JSON-schemaet er den maskinelle baseline for struktur og obligatoriske elementer.

## Sådan læses elementspecifikationerne

Hvert element er beskrevet med formål og semantik, normative krav, afsenderkrav, modtagerkrav og eksempel.

## Normative nøgleord

SKAL angiver et absolut krav.

KAN angiver, at noget er valgfrit eller tilladt.

BØR angiver en stærk anbefaling, som kan fraviges med begrundelse.

MÅ IKKE angiver et forbud.

De normative nøgleord anvendes konsekvent i beskrivelser af elementer, afsenderkrav og modtagerkrav.

Et element er obligatorisk, hvis det fremgår af JSON-schemaets required-liste. Øvrige elementer er valgfrie, medmindre andet eksplicit fremgår.

## NDJSON-rammebetingelser

Filen består af én JSON-record pr. linje. Første linje SKAL være en Leverance-record med recordType = "Leverance". Efterfølgende linjer SKAL være Logregistrering-records med recordType = "Logregistrering".

## Databeskyttelse og sikkerhed

Nogle elementer kan indeholde personhenførbare oplysninger. Ved tvivl bør dataminimering og adgangskontrol prioriteres. teknCtx MÅ IKKE indeholde hemmeligheder som tokens, nøgler eller passwords.

# Begreber

**Afsender:** Det logførende system, der danner og afsender NDJSON-leverancer.

**Modtager:** System eller organisation, der modtager leverancer og foretager validering, kompletthedstjek og rapportering.

**Leverance:** Første record i NDJSON-filen med metadata, logID og dækningsinterval.

**Logregistrering:** Efterfølgende records i NDJSON-filen; hver record repræsenterer en loghændelse.

**NDJSON:** Newline Delimited JSON: ét JSON-objekt pr. linje.

**Sekvensbrud:** Afvigelse i leverance.logID-sekvensen, fx spring, dublet eller uventet rækkefølge.

**Tidsintervalbrud:** Hul eller overlap mellem på hinanden følgende leverancers dækningsinterval for samme afsendende system.

# 1. Overordnet beskrivelse

## 1.1. Design- og arkitekturprincipper

Designet er optimeret til NDJSON, så leverancer kan behandles sekventielt og skalerbart. Der skelnes mellem leveranceniveau og registreringsniveau. Komplethed kontrolleres uafhængigt af hændelsesindhold via logID og dækningsinterval.

Modellen anvender en flad struktur. Elementer, der kan forekomme flere gange, angives som flade arrays af strengværdier. Arrays MÅ IKKE indeholde objekter eller nestede arrays, medmindre dette eksplicit fremgår af JSON-schemaet.

## 1.2. Dannelse og afsendelse af NDJSON-leverancer

Leverancer SKAL afsendes som NDJSON-filer med faste, foruddefinerede intervaller. Intervallet fastlægges i driftsopsætningen eller integrationsaftalen.

Afsender MÅ IKKE afsende enkelttransaktioner som separate leverancer. Logregistreringer SKAL bundtes i leverancer, så hver fil dækker et sammenhængende dækningsinterval.

Filer SKAL være myndighedsopdelte, så én fil/leverance kun vedrører én myndighed.

En NDJSON-fil MÅ IKKE overstige 2 GB målt som rå filstørrelse på disk før eventuel komprimering. Hvis den forventede leverancestørrelse overskrider grænsen, SKAL afsender splitte perioden i flere filer med separate Leverance-records og sammenhængende dækningsintervaller.

Ved split er hver del-fil en selvstændig leverance med egen Leverance-record og eget logID. Del-leverancerne SKAL samlet dække perioden uden huller eller overlap.

## 1.3. Filnavne

Filnavnet skal understøtte:

- entydig identifikation af leverancen ved drift, genfremsendelse og fejlhåndtering
- sortering, fx kronologisk og pr. afsendende system/myndighed, uden at åbne filen
- komplethedskontrol ved at gøre det let at koble filnavn til logID og dækningsinterval
- dataminimering, så filnavnet ikke indeholder personhenførbare oplysninger

Filnavnet er en praktisk konvention. Den normative sandhed ligger i indholdet af Leverance-recorden, men filnavnet bør afspejle centrale metadata for at lette drift og kontrol.

Grundregler:

- Hver fil er en selvstændig leverance.
- Hver fil SKAL have sin egen logID og sin egen Leverance-record med logID i første NDJSON-linje.
- Ved split af en periode i flere filer er hver del-fil fortsat en selvstændig leverance og indgår i sekvenskontrol som en normal leverance.

Navngivning:

```
revisionslog_<myndCvr>_<afsendtSystemID>_<yyyy>_logid-<logID>_part-<n>-of-
<m>.ndjson
```

Hvor:

- <myndCvr> = leverance.myndCvr
- <afsendtSystemID> = leverance.afsendtSystemID, saniteret til filnavnsbrug
- <yyyy> = år udledt af leverance.fra
- <logID> = leverance.logID, unik pr. fil/leverance; zero-padding anbefales
- part-<n>-of-<m> = tæller for den opdelte leverance

Part-segmentet er ikke nødvendigt for entydighed, fordi logID allerede identificerer leverancen. Segmentet er dog nyttigt for mennesker, driftsoverblik og håndtering af opdelte leverancer.

**Eksempel 1:** Leverancen kan rummes i én fil.

```
revisionslog_87654321_HR-PORTAL-01_2026_logid-000200_part-1-of-1.ndjson
```

**Eksempel 2:** Leverancen er opdelt i 3 filer.

```
revisionslog_87654321_HR-PORTAL-01_2026_logid-000043_part-1-of-3.ndjson
```

```
revisionslog_87654321_HR-PORTAL-01_2026_logid-000044_part-2-of-3.ndjson
```

```
revisionslog_87654321_HR-PORTAL-01_2026_logid-000045_part-3-of-3.ndjson
```

## 1.4. Idempotency

Filnavnet udgør modtagers idempotency-nøgle på leveranceniveau. Samme filnavn kan blive leveret flere gange, fx ved at-least-once-levering, og SKAL kunne behandles uden dobbeltindlæsning.

Modtager SKAL behandle identiske filnavne idempotent, så samme fil ikke indlæses flere gange.

Modtager BØR gemme status pr. filnavn, fx modtaget, valideret eller indlæst, og bør ignorere dubletter eller genkøre behandlingen sikkert.

<yyyy> i filnavnet SKAL svare til året udledt af leverance.fra.

Modtager BØR som konsistenscheck verificere, at Leverance-recorden matcher filnavnet, mindst for myndCvr, afsendItSystemID, år og logID.

Opdelte leverancer:

- Hver del-fil er en selvstændig leverance og har derfor eget logID og eget filnavn.
- part-<n>-of-<m> bruges til at gruppere del-filer, men idempotency pr. fil sker via det fulde filnavn.

Logniveau:

- Afsender SKAL holde logregistrering.ID stabil for samme hændelse ved genbehandling eller genfremsendelse.
- Modtager BØR deduplikere loghændelser på logregistrering.ID for at undgå dubletter ved reprocessering.

Genfremsendelse vs. Korrektion:

- Genfremsendelse: samme filnavn, samme logID/part og samme indhold.
- Korrektion: Hvis indholdet ændres, BØR afsender sende en ny fil med nyt logID og nyt filnavn. Afsender KAN angive reference til tidligere logID i leverance.teknCtx, fx "korrektionAfLogID|<tidligere logID

Modtager SKAL kunne behandle gentagne leverancer idempotent. Afsender SKAL holde logregistrering.ID stabil for samme hændelse ved genbehandling eller genfremsendelse.

Modtager BØR deduplikere loghændelser på logregistrering.ID.

## 1.5. Ansvarsdeling: kontrol, markering og rapportering

Afsender har ansvar for korrekt dannelse af leverancer. Modtager har ansvar for at validere format og opdage manglende leverancer eller manglende tidsdækning. Modtager SKAL opdage og rapportere sekvensbrud og tidsintervalbrud.

## 2. Beskrivelser af elementerne i revisionsloggen

Dette afsnit beskriver elementerne i den rækkefølge, de typisk forekommer i en NDJSON-fil.

Dokumentet følger den besluttede baseline for revisionslogmodellen, hvor hver NDJSON-linje enten er en Leverance-record eller en Logregistrering-record. Leverance-recorden indeholder metadata om leverancen, mens Logregistrering-records beskriver de konkrete loghændelser.

Detaljerede elementdefinitioner, herunder datatype, kardinalitet og eksempler, findes i Excel-datakataloget. Dette dokument supplerer med forklarende tekst, semantik samt afsender- og modtagerkrav.

Elementnavne, kardinalitet og obligatoriske elementer skal forstås i overensstemmelse med JSON-schemaet. Et element er obligatorisk, hvis det fremgår af schemaets required-liste.

### 2.1. Leverance (første NDJSON-record)

Afsnittet beskriver Leverance-recorden, som altid er den første linje i en NDJSON-fil. Leverance-recorden indeholder metadata om leverancen og gør det muligt at validere filen, føre komplethedskontrol og håndtere genfremsendelser uden at blande loghændelser sammen.

Leverance-recorden skal ses som en kuvert omkring de efterfølgende Logregistrering-records. Leverancen angiver blandt andet leverancens identifikation, myndighed, afsendende it-system, dækningsinterval og skemaversion.

I JSON-schemaet er Leverance-recorden en flad struktur. Det betyder, at centrale oplysninger angives som topniveau-elementer i Leverance-recorden, fx myndCvr, afsendItSystemID, fra, til og skemaVer.

#### Nøgleprincipper:

- Første record: Leverance SKAL være første NDJSON-record i filen og have recordType = "Leverance".
- Sekvens: logID identificerer leverancen og anvendes til sekvenskontrol for det afsendende it-system.
- Myndighed: myndCvr angiver den myndighed, leverancen vedrører. myndNavn KAN angives som læsevenligt navn.
- Afsendende system: afsendItSystemID angiver det afsendende it-system. afsendItSystemNavn KAN angives som læsevenligt navn.
- Dækningsinterval: fra er inklusiv start, og til er eksklusiv afslutning.
- Skemaversion: skemaVer angiver den version af dataformatet/skemaet, som leverancen følger.
- Teknisk kontekst: teknCtx KAN angives som flad liste af type|værdi-streng og MÅ IKKE indeholde hemmeligheder.

---

#### 2.1.1. leverance.recordType

**Formål:** Markerer at NDJSON-linjen er en Leverance-record og gør det muligt for modtager at skelne Leverance-recorden fra efterfølgende Logregistrering-records.

**Semantik og uddybning:** Elementet fungerer som diskriminator mellem recordtyper. Første linje i en NDJSON-fil SKAL være en Leverance-record med recordType = "Leverance".

#### Normative krav:

- Elementet SKAL angives.
- Elementet SKAL have værdien "Leverance".
- Elementet er obligatorisk i JSON-schemaets required-liste for Leverance.

#### Afsenderkrav:

- Afsender SKAL sætte værdien deterministisk ved serialisering.
- Værdien MÅ IKKE lokaliseres, oversættes eller varieres.

**Modtagerkrav:**

- Modtager SKAL validere, at første NDJSON-record har recordType = "Leverance".
- Modtager SKAL afvise eller markere leverancen som ugyldig, hvis første record mangler recordType eller har en anden værdi.

**Eksempel:** "recordType": "Leverance"

**Typiske faldgruber:**

- Værdien oversættes eller varieres, fx "Delivery", "leverance" eller "LEVERANCE".

---

**2.1.2. leverance.logID**

**Formål:** Entydig identifikation af leverancen med henblik på komplethedskontrol, dubletkontrol, fejlhåndtering og genfremsendelse.

**Semantik og uddybning:** logID identificerer den enkelte Leverance-record. Elementet anvendes sammen med afsendItSystemID og dækningsintervallet fra/til til sekvens- og komplethedskontrol. logID er en leverance-identifikator og MÅ IKKE anvendes som identifikation af en konkret loghændelse.

**Normative krav:**

- Elementet SKAL angives.
- Elementet er obligatorisk i JSON-schemaets required-liste for Leverance.
- Værdien SKAL være entydig inden for den sekvens, som anvendes for det afsendende it-system.
- Værdien MÅ IKKE indeholde personoplysninger eller hemmeligheder.

**Afsenderkrav:**

- Afsender SKAL danne logID på en stabil og konsistent måde.
- Afsender SKAL kunne genfremsende en leverance med samme logID ved genfremsendelse af samme leverance.
- Afsender BØR anvende et format, der understøtter sortering og drift, fx zero-padding.

**Modtagerkrav:**

- Modtager SKAL anvende logID som del af kompletheds- og sekvenskontrol.
- Modtager BØR sammenholde logID med filnavn, afsendItSystemID og dækningsintervallet fra/til.
- Modtager SKAL kunne håndtere genfremsendelse uden dobbeltindlæsning.

**Databeskyttelse og sikkerhed:** logID BØR være en teknisk leveranceidentifikator og MÅ IKKE indeholde personhenførbare oplysninger, CPR-numre, tokens, nøgler eller passwords.

**Eksempel:** "logID": "000043"

**Typiske faldgruber:**

- logID bruges som hændelses-id i stedet for leverance-id.
- logID genbruges til en ændret leverance uden tydelig korrektion.
- logID indeholder forretnings- eller personoplysninger.

---

**2.1.3. leverance.myndCvr**

**Formål:** Angiver CVR-nummeret for den myndighed, som leverancen vedrører.

**Semantik og uddybning:** myndCvr identificerer den myndighed, hvis revisionslogoplysninger leveres. Elementet anvendes til myndighedsopdeling, autorisation, kontrol og drift. Leverancer bør være myndighedsopdelte.

**Normative krav:**

- Elementet SKAL angives.
- Elementet er obligatorisk i JSON-schemaets required-liste for Leverance.
- Værdien SKAL være en string.
- Værdien BØR være et CVR-nummer på 8 cifre.
- Elementet MÅ IKKE indeholde andre identifikatorer end myndighedens CVR-nummer.

**Afsenderkrav:**

- Afsender SKAL angive CVR-nummeret for den myndighed, leverancen vedrører.
- Afsender SKAL sikre, at leverancen ikke blander data for flere myndigheder.
- Afsender BØR validere, at værdien har korrekt CVR-format.

**Modtagerkrav:**

- Modtager SKAL anvende myndCvr til myndighedsopdeling, autorisation og kontrol.
- Modtager BØR validere, at værdien svarer til forventet myndighed.
- Modtager BØR markere eller afvise leverancer, hvor myndCvr ikke svarer til forventet myndighed.

**Databeskyttelse og sikkerhed:** myndCvr er en myndighedsidentifikator og bør ikke indeholde personhenførbare oplysninger.

**Eksempel:** "myndCvr": "87654321"

**Typiske faldgruber:**

- Leverancen indeholder data for flere myndigheder.
- CVR-nummeret angives i et andet format end forventet.
- Myndighedens navn anvendes som teknisk nøgle.

#### 2.1.4. leverance.myndNavn

**Formål:** Angiver et læsevenligt navn for den myndighed, som leverancen vedrører.

**Semantik og uddybning:** myndNavn er et visnings- og driftsvenligt supplement til myndCvr og er ikke den autoritative myndighedsidentifikation.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Leverance.
- Hvis elementet angives, SKAL værdien være en string.

**Afsenderkrav:**

- Afsender KAN angive myndNavn for læsbarhed.
- Afsender BØR anvende en stabil og genkendelig betegnelse.
- Afsender MÅ IKKE anvende myndNavn som erstatning for myndCvr.

**Modtagerkrav:**

- Modtager SKAL kunne modtage leverancer uden myndNavn.
- Modtager MÅ IKKE basere autorisation, myndighedsopdeling eller komplethedskontrol på myndNavn alene.
- Modtager KAN anvende myndNavn til visning, rapportering og manuel fejlsøgning.

**Databeskyttelse og sikkerhed:** myndNavn bør ikke indeholde oplysninger om konkrete personer, sager eller interne forhold.

**Eksempel:** "myndNavn": "Korsbæk Kommune"

**Typiske faldgruber:**

- myndNavn anvendes som teknisk nøgle.
- myndNavn varierer mellem leverancer.
- myndNavn udfyldes med interne eller personhenførbare oplysninger.

---

### 2.1.5. leverance.afsendtSystemID

**Formål:** Angiver ID for det it-system, der har dannet og afsendt leverancen.

**Semantik og uddybning:** afsendtSystemID identificerer det afsendende it-system på leveranceniveau. Sammen med logID og dækningsintervallet fra/til anvendes elementet til sekvens- og dækningskontrol.

**Normative krav:**

- Elementet SKAL angives.
- Elementet er obligatorisk i JSON-schemaets required-liste for Leverance.
- Værdien SKAL være en string.
- Værdien MÅ IKKE indeholde personoplysninger eller hemmeligheder.

**Afsenderkrav:**

- Afsender SKAL angive et stabilt ID for det afsendende it-system.
- Afsender BØR anvende samme afsendtSystemID på tværs af leverancer fra samme system.
- Afsender MÅ IKKE anvende afsendtSystemNavn som erstatning for afsendtSystemID.

**Modtagerkrav:**

- Modtager SKAL anvende afsendtSystemID som del af kontrolgrundlaget.
- Modtager BØR anvende afsendtSystemID sammen med logID og fra/til til sekvens- og dækningskontrol.
- Modtager BØR markere eller undersøge uventede værdier.

**Databeskyttelse og sikkerhed:** afsendtSystemID bør være en teknisk systemnøgle og MÅ IKKE indeholde CPR-numre, bruger-id'er, tokens, nøgler eller passwords.

**Eksempel:** "afsendtSystemID": "HR-PORTAL-01"

**Typiske faldgruber:**

- ID ændres ved almindelige versionsopdateringer.
- Systemnavnet anvendes som teknisk nøgle.
- Værdien indeholder miljø-, bruger- eller personoplysninger.

---

### 2.1.6. leverance.afsendtSystemNavn

**Formål:** Angiver et læsevenligt navn for det it-system, der har dannet og afsendt leverancen.

**Semantik og uddybning:** afsendtSystemNavn er et visnings- og driftsvenligt supplement til afsendtSystemID og er ikke den autoritative systemidentifikation.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Leverance.
- Hvis elementet angives, SKAL værdien være en string.

**Afsenderkrav:**

- Afsender KAN angive afsendtSystemNavn for læsbarhed.
- Afsender BØR anvende et stabilt og genkendeligt systemnavn.

- Afsender MÅ IKKE anvende afsendItSystemNavn som erstatning for afsendItSystemID.

**Modtagerkrav:**

- Modtager SKAL kunne modtage leverancer uden afsendItSystemNavn.
- Modtager MÅ IKKE basere kontrol eller autorisation på afsendItSystemNavn alene.
- Modtager KAN anvende navnet til visning, rapportering og manuel fejlsøgning.

**Databeskyttelse og sikkerhed:** afsendItSystemNavn bør ikke indeholde personoplysninger, bruger-id'er, sagsoplysninger eller hemmeligheder.

**Eksempel:** "afsendItSystemNavn": "HR-portal"

**Typiske faldgruber:**

- Navnet anvendes som teknisk nøgle.
- Navnet varierer mellem leverancer.
- Navnet indeholder miljø-, person- eller sagsoplysninger.

---

### 2.1.7. leverance.fra

**Formål:** Angiver starttidspunktet for leverancens dækningsinterval.

**Semantik og uddybning:** fra angiver det tidligste tidspunkt, som leverancen dækker. fra er inklusiv. Værdien SKAL angives som date-time med tidszone.

**Normative krav:**

- Elementet SKAL angives.
- Elementet er obligatorisk i JSON-schemaets required-liste for Leverance.
- Værdien SKAL være en string med formatet date-time.
- Værdien SKAL angives med tidszone, fx offset eller Z.
- fra SKAL være før til.

**Afsenderkrav:**

- Afsender SKAL angive starttidspunktet for dækningsintervallet.
- Afsender SKAL sikre, at fra og til tilsammen afgrænser perioden.
- Afsender BØR sikre sammenhængende leverancer uden huller eller overlap.
- Afsender BØR anvende en konsistent tidszonepraksis.

**Modtagerkrav:**

- Modtager SKAL validere, at fra er til stede og har gyldigt date-time-format.
- Modtager SKAL anvende fra sammen med til til intervalkontrol.
- Modtager BØR markere eller rapportere huller og overlap.

**Eksempel:** "fra": "2026-03-12T00:00:00+01:00"

**Typiske faldgruber:**

- Tidszone udelades.
- fra angives efter eller lig med til.
- fra anvendes som hændelsestidspunkt.

---

### 2.1.8. leverance.til

**Formål:** Angiver sluttidspunktet for leverancens dækningsinterval.

**Semantik og uddybning:** til angiver afslutningen på den periode, som leverancen dækker. til er eksklusiv. Værdien SKAL angives som date-time med tidszone.

**Normative krav:**

- Elementet SKAL angives.

- Elementet er obligatorisk i JSON-schemaets required-liste for Leverance.
- Værdien SKAL være en string med formatet date-time.
- Værdien SKAL angives med tidszone, fx offset eller Z.
- til SKAL være efter fra.

**Afsenderkrav:**

- Afsender SKAL angive sluttidspunktet for dækningsintervallet.
- Afsender SKAL sikre, at til er efter fra.
- Afsender BØR sikre, at næste leverances fra svarer til forrige leverances til.
- Afsender BØR anvende en konsistent tidszonepraksis.

**Modtagerkrav:**

- Modtager SKAL validere, at til er til stede og har gyldigt date-time-format.
- Modtager SKAL validere, at til er efter fra.
- Modtager BØR markere eller rapportere huller og overlap.

**Eksempel:** "til": "2026-03-13T00:00:00+01:00"

**Typiske faldgruber:**

- til behandles som inklusiv.
- Tidszone udelades.
- til angives før eller lig med fra.

### 2.1.9. **leverance.skemaVer**

**Formål:** Angiver hvilken version af dataformatet og JSON-schemaet leverancen følger.

**Semantik og uddybning:** skemaVer gør det muligt for afsender og modtager at anvende samme regler for validering, fortolkning og versionsstyring. Elementet angiver versionen af revisionslogformatet, ikke versionen af det afsendende it-system.

**Normative krav:**

- Elementet SKAL angives.
- Elementet er obligatorisk i JSON-schemaets required-liste for Leverance.
- Værdien SKAL være en string.
- Værdien SKAL angive en version, som modtager kan validere og fortolke.

**Afsenderkrav:**

- Afsender SKAL angive den skemaversion, som leverancen er dannet efter.
- Afsender BØR anvende en stabil versionsstreng, fx major.minor.
- Afsender MÅ IKKE anvende skemaVer til at angive versionen af det afsendende it-system.

**Modtagerkrav:**

- Modtager SKAL anvende skemaVer til at vælge korrekt validerings- og fortolkningsgrundlag.
- Modtager BØR afvise eller tydeligt markere leverancer med ukendt eller ikke-understøttet skemaVer.
- Modtager BØR sikre, at skemaVer stemmer med JSON-schema og datakatalog.

**Eksempel:** "skemaVer": "1.0"

**Typiske faldgruber:**

- skemaVer udelades.
- skemaVer bruges til systemversion.
- Forskellige versioneringsformater anvendes uden dokumentation.

---

### 2.1.10. leverance.teknCtx

**Formål:** Angiver supplerende teknisk kontekst på leveranceniveau, fx til drift, korrelation, fejlsøgning, batchidentifikation eller reference ved korrektion.

**Semantik og uddybning:** teknCtx er en flad liste af tekniske kontekstelementer. Hvert element angives som en streng i formatet type|værdi. teknCtx anvendes til tekniske metadata om leverancen og må ikke ændre den forretningsmæssige betydning af leverancen.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Leverance.
- Hvis elementet angives, SKAL værdien være et array.
- Hvert element SKAL følge formatet type|værdi.
- Arrayet MÅ IKKE indeholde objekter eller nestede arrays.
- teknCtx MÅ IKKE indeholde hemmeligheder.

**Afsenderkrav:**

- Afsender KAN angive teknCtx ved behov for teknisk kontekst.
- Afsender SKAL sikre, at hvert element følger formatet type|værdi.
- Afsender BØR anvende stabile og genkendelige typer.
- Afsender MÅ IKKE placere hemmeligheder i teknCtx.
- Afsender BØR undgå personhenførbare oplysninger, medmindre nødvendigt og dokumenteret.

**Modtagerkrav:**

- Modtager SKAL kunne modtage leverancer uden teknCtx.
- Modtager SKAL kunne parse teknCtx som en flad liste af type|værdi-streng.
- Modtager BØR kunne anvende teknCtx til korrelation, drift og fejlsøgning.
- Modtager SKAL kunne håndtere ukendte type-værdier uden at afvise leverancen alene af den grund, hvis formatet er gyldigt.

**Databeskyttelse og sikkerhed:** teknCtx MÅ IKKE indeholde tokens, nøgler, passwords eller andre hemmeligheder.

**Eksempel:** "teknCtx": ["system.miljoe|produktion", "korrelationsId|CORR-20260312-000043"]

**Typiske faldgruber:**

- teknCtx udfyldes som objekter med separate type- og værdi-elementer.
- teknCtx bruges til forretningsdata.
- teknCtx indeholder hemmeligheder.
- Der anvendes meget store arrays.

---

### 2.1.11. leverance.teknCtx.element

**Formål:** Angiver ét teknisk kontekstelement i teknCtx.

**Semantik og uddybning:** Et teknCtx-element er en enkelt string i formatet type|værdi. Hvis type eller værdi indeholder separatoren | eller escape-tegnet \, SKAL tegnene escapes efter den fælles escape-regel for type|værdi-streng.

**Normative krav:**

- Elementet KAN forekomme 0..\* gange i teknCtx.
- Hvis elementet forekommer, SKAL det være en string.
- Elementet SKAL følge formatet type|værdi.
- type-delen SKAL være angivet.
- værdi-delen SKAL være angivet.
- Elementet MÅ IKKE indeholde objekter eller nestede strukturer.

**Afsenderkrav:**

- Afsender SKAL danne hvert teknCtx-element som en type|værdi-streng.
- Afsender BØR anvende stabile type-navne.
- Afsender BØR anvende relevante typer fra datakataloget.
- Afsender MÅ IKKE placere hemmeligheder i værdien.

**Modtagerkrav:**

- Modtager SKAL kunne parse teknCtx-elementer efter type|værdi-formatet.
- Modtager BØR kunne anvende type-delen til indeksering, filtrering og analyse.
- Modtager SKAL kunne håndtere ukendte type-værdier uden at afvise alene af den grund.

**Eksempel:** "system.miljoe|produktion"

**Eksempel:** "korrelationsId|CORR-20260312-000043"

**Typiske faldgruber:**

- Separatoren | udelades.
- Elementet angives som JSON-objekt.
- type-delen ændrer navn uden begrundelse.
- Værdien indeholder hemmeligheder.

## 2.2. Logregistrering (efterfølgende NDJSON-records)

Afsnittet beskriver Logregistrering-records, som udgør alle efterfølgende linjer i NDJSON-filen efter Leverance-recorden. Hver Logregistrering repræsenterer én loghændelse og indeholder de oplysninger, der bruges til audit, sporbarhed, analyse og kontrol.

I JSON-schemaet er Logregistrering-recorden en flad struktur. Centrale oplysninger angives som topniveau-elementer, fx ID, starttidspunkt, operation, operationTilstand, initlSystemID, execltSystemID, visteOpl, personCpr, behandlObj og teknCtx.

Elementer, der kan forekomme flere gange, angives som flade arrays af strengværdier. Det gælder fx visteOpl, behandlObj og teknCtx. Arrays MÅ IKKE indeholde objekter eller nestede arrays, medmindre dette eksplicit fremgår af JSON-schemaet.

### Nøgleprincipper:

- Hver Logregistrering SKAL have recordType = "Logregistrering".
- ID identificerer den enkelte loghændelse og anvendes til audit, deduplikering og korrelation.
- starttidspunkt SKAL angives; sluttidspunkt KAN angives, når afslutningstidspunktet er observerbart.
- operation SKAL angives; operationTilstand SKAL angives som overordnet udfald.
- initlSystemID og execltSystemID SKAL angives.
- visteOpl beskriver oplysningstyper, ikke konkrete oplysningsværdier.
- personCpr KAN anvendes ved én entydigt identificeret fysisk person; ved flere personer anvendes behandlObj.
- teknCtx KAN anvendes til teknisk korrelation, fejlsøgning, statuskoder og driftsoplysninger og MÅ IKKE indeholde hemmeligheder.

---

### 2.2.1. logregistrering.recordType

**Formål:** Markerer at NDJSON-linjen er en Logregistrering-record.

**Semantik og uddybning:** Elementet fungerer som diskriminator mellem recordtyper. Alle NDJSON-linjer efter Leverance-recorden SKAL være Logregistrering-records med recordType = "Logregistrering".

#### Normative krav:

- Elementet SKAL angives.
- Elementet SKAL have værdien "Logregistrering".
- Elementet er obligatorisk i JSON-schemaets required-liste for Logregistrering.

#### Afsenderkrav:

- Afsender SKAL sætte værdien deterministisk.
- Værdien MÅ IKKE lokaliseres, oversættes eller varieres.

#### Modtagerkrav:

- Modtager SKAL validere recordType.
- Modtager SKAL afvise eller markere recorden som ugyldig, hvis recordType mangler eller er forkert.

**Eksempel:** "recordType": "Logregistrering"

#### Typiske faldgruber:

- Værdien oversættes eller varieres.

---

### 2.2.2. logregistrering.ID

**Formål:** Entydig identifikation af den enkelte loghændelse.

**Semantik og uddybning:** ID identificerer én Logregistrering-record og anvendes til audit, deduplikering, genfremsendelse, fejlhåndtering og korrelation. ID MÅ IKKE forveksles med leverance.logID.

**Normative krav:**

- Elementet SKAL angives.
- Elementet er obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Værdien SKAL være en string.
- Værdien BØR være entydig inden for afsenders relevante logdomæne.
- Værdien MÅ IKKE indeholde CPR-numre, tokens, nøgler, passwords eller andre hemmeligheder.

**Afsenderkrav:**

- Afsender SKAL angive ID for hver Logregistrering-record.
- Afsender BØR danne ID stabilt og konsistent.
- Afsender BØR genanvende samme ID ved genfremsendelse af samme hændelse.
- Afsender MÅ IKKE anvende leverance.logID som erstatning for logregistrering.ID.

**Modtagerkrav:**

- Modtager SKAL validere, at ID er til stede og er en string.
- Modtager BØR anvende ID til deduplikering, audit, fejlhåndtering og korrelation.
- Modtager BØR kunne håndtere, at samme ID modtages igen ved genfremsendelse.

**Databeskyttelse og sikkerhed:** ID bør være en teknisk hændelsesidentifikator og bør ikke indeholde personhenførbare oplysninger.

**Eksempel:** "ID": "LOG-0001"

**Typiske faldgruber:**

- ID udelades.
- ID ændres ved genfremsendelse.
- leverance.logID bruges som hændelses-id.
- ID indeholder personhenførbare værdier.

---

### 2.2.3. logregistrering.starttidspunkt

**Formål:** Angiver hvornår den loggede hændelse eller systemaktivitet startede.

**Semantik og uddybning:** starttidspunkt angiver starttidspunktet for den konkrete Logregistrering-record og anvendes til audit, sortering, søgning, korrelation og tidsmæssig afgrænsning. Det må ikke forveksles med leverance.fra.

**Normative krav:**

- Elementet SKAL angives.
- Elementet er obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Værdien SKAL være en string med formatet date-time.
- Værdien SKAL angives med tidszone, fx offset eller Z.

**Afsenderkrav:**

- Afsender SKAL angive starttidspunkt.
- Afsender SKAL angive værdien i gyldigt date-time-format med tidszone.
- Afsender BØR anvende en konsistent tidszonepraksis.
- Afsender BØR sikre, at starttidspunkt ligger inden for Leverance-recordens dækningsinterval fra/til.

**Modtagerkrav:**

- Modtager SKAL validere, at starttidspunkt er til stede og har gyldigt date-time-format.
- Modtager BØR anvende starttidspunkt til audit, sortering, søgning og korrelation.
- Modtager BØR markere eller rapportere logregistreringer uden for dækningsintervallet.

**Eksempel:** "starttidspunkt": "2026-03-12T11:18:05+01:00"

**Eksempel:** "starttidspunkt": "2026-03-12T10:18:05Z"

**Typiske faldgruber:**

- Tidszone udelades.
- starttidspunkt forveksles med leverance.fra.
- Lokaltid angives uden offset eller Z.

**2.2.4. logregistrering.sluttidspunkt**

**Formål:** Angiver hvornår den loggede hændelse eller systemaktivitet sluttede, hvis afslutningstidspunktet er observerbart.

**Semantik og uddybning:** sluttidspunkt kan anvendes til at beskrive varigheden af en hændelse. Elementet er valgfrit, fordi ikke alle hændelser har et observerbart eller meningsfuldt sluttidspunkt.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Hvis elementet angives, SKAL værdien være en string med formatet date-time.
- Hvis elementet angives, SKAL værdien angives med tidszone.

**Afsenderkrav:**

- Afsender KAN angive sluttidspunkt, når afslutningstidspunktet er observerbart.
- Afsender SKAL angive værdien i gyldigt date-time-format med tidszone, hvis elementet angives.
- Afsender BØR sikre, at sluttidspunkt ikke ligger før starttidspunkt.

**Modtagerkrav:**

- Modtager SKAL kunne modtage records uden sluttidspunkt.
- Hvis sluttidspunkt er angivet, SKAL modtager validere formatet.
- Modtager BØR kunne anvende sluttidspunkt sammen med starttidspunkt til varighed og analyse.

**Eksempel:** "sluttidspunkt": "2026-03-12T11:18:07+01:00"

**Eksempel:** "sluttidspunkt": "2026-03-12T10:18:07Z"

**Typiske faldgruber:**

- sluttidspunkt angives uden tidszone.
- sluttidspunkt ligger før starttidspunkt.
- sluttidspunkt forveksles med leverance.til.

**2.2.5. logregistrering.operation**

**Formål:** Angiver hvilken operation eller handling logregistreringen vedrører.

**Semantik og uddybning:** operation beskriver den overordnede handlingstype for den loggede hændelse. operation beskriver hvad der blev forsøgt eller udført; udfaldet beskrives i operationTilstand.

**Normative krav:**

- Elementet SKAL angives.
- Elementet er obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Værdien SKAL være en string.
- Værdien BØR følge operation-kataloget.

**Afsenderkrav:**

- Afsender SKAL angive operation.
- Afsender BØR anvende en værdi fra operation-kataloget, når en dækkende værdi findes.
- Afsender BØR anvende andet, hvis ingen anbefalet værdi er dækkende.
- Afsender BØR anvende værdierne konsistent.

**Modtagerkrav:**

- Modtager SKAL validere, at operation er til stede og er en string.
- Modtager BØR kunne anvende operation til filtrering, rapportering, statistik og audit.
- Modtager BØR kunne håndtere andet og eventuelle lokale værdier efter fast politik.

**Eksempel:** "operation": "soeg"

**Eksempel:** "operation": "laes"

**Typiske faldgruber:**

- operation bruges til teknisk metode i stedet for revisionsmæssig handlingstype.
- operation blandes sammen med operationTilstand.
- Lokale værdier anvendes inkonsistent.

## 2.2.6. logregistrering.operationTilstand

**Formål:** Angiver det overordnede udfald af operationen.

**Semantik og uddybning:** operationTilstand beskriver, om operationen blev gennemført, fejlede, blev afvist eller blev afbrudt. Elementet er ikke beregnet til tekniske statuskoder, HTTP-koder, applikationsfejlkode, exception-typer eller debug-information. Tekniske status- og fejloplysninger KAN angives i teknCtx.

**Normative krav:**

- Elementet SKAL angives.
- Elementet er obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Værdien SKAL være en string.
- Værdien SKAL være én af: Gennemført, Fejlet, Afvist eller Afbrudt.
- operationTilstand MÅ IKKE anvendes til tekniske statuskoder, HTTP-koder, applikationsfejlkode eller debug-information.

**Afsenderkrav:**

- Afsender SKAL angive operationTilstand.
- Afsender SKAL mappe interne udfald, statusser og fejlkode til én af de fire overordnede værdier.
- Afsender KAN angive tekniske status- og fejloplysninger i teknCtx.
- Afsender MÅ IKKE udvide operationTilstand med lokale fejlkode.

**Modtagerkrav:**

- Modtager SKAL validere, at operationTilstand er til stede og har en tilladt enum-værdi.
- Modtager SKAL kunne anvende operationTilstand som overordnet udfaldskategori.
- Modtager BØR anvende teknCtx til tekniske status- og fejloplysninger.
- Modtager BØR markere eller afvise records med værdier uden for enum-listen.

**Eksempel:** "operationTilstand": "Gennemført"

**Eksempel:** "operationTilstand": "Afvist", "teknCtx": ["api.statuskode|403", "fejl.kode|AUTHZ\_DENIED"]

**Typiske faldgruber:**

- HTTP-statuskode angives i operationTilstand.
- Applikationsfejlkode angives i operationTilstand.
- operationTilstand udvides med lokale værdier.

### 2.2.7. logregistrering.initItSystemID

**Formål:** Angiver ID for det it-system, der initierede den loggede hændelse.

**Semantik og uddybning:** initItSystemID identificerer det system, hvorfra handlingen blev initieret. Elementet beskriver hvor hændelsen blev initieret, mens execItSystemID beskriver hvilket system der udførte behandlingen.

**Normative krav:**

- Elementet SKAL angives.
- Elementet er obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Værdien SKAL være en string.
- Værdien MÅ IKKE indeholde CPR-numre, brugeroplysninger, tokens, nøgler, passwords eller andre hemmeligheder.

**Afsenderkrav:**

- Afsender SKAL angive initItSystemID.
- Afsender SKAL anvende en stabil systemidentifikator.
- Afsender BØR anvende samme initItSystemID på tværs af hændelser fra samme system.
- Afsender MÅ IKKE anvende initItSystemNavn som erstatning for initItSystemID.

**Modtagerkrav:**

- Modtager SKAL validere, at initItSystemID er til stede og er en string.
- Modtager BØR anvende initItSystemID til audit, filtrering, rapportering, fejlhåndtering og korrelation.
- Modtager BØR kunne sammenholde initItSystemID med execItSystemID.

**Databeskyttelse og sikkerhed:** initItSystemID bør være en teknisk systemnøgle og MÅ IKKE indeholde personhenførbare oplysninger eller hemmeligheder.

**Eksempel:** "initItSystemID": "HR-PORTAL-01"

**Typiske faldgruber:**

- initItSystemID ændres ved versionsopdateringer.
- Systemnavn anvendes som teknisk nøgle.
- Elementet udfyldes med bruger-id eller CPR-nummer.
- initItSystemID og execItSystemID forveksles.

### 2.2.8. logregistrering.initItSystemNavn

**Formål:** Angiver et læsevenligt navn for det it-system, der initierede den loggede hændelse.

**Semantik og uddybning:** initItSystemNavn er et visnings- og driftsvenligt supplement til initItSystemID og er ikke den autoritative systemidentifikation.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Hvis elementet angives, SKAL værdien være en string.

**Afsenderkrav:**

- Afsender KAN angive initItSystemNavn for læsbarhed.
- Afsender BØR anvende et stabilt og genkendeligt systemnavn.
- Afsender MÅ IKKE anvende initItSystemNavn som erstatning for initItSystemID.
- Afsender BØR undgå miljø-, bruger-, person- eller sagsoplysninger i systemnavnet.

**Modtagerkrav:**

- Modtager SKAL kunne modtage records uden initItSystemNavn.
- Modtager MÅ IKKE basere audit, korrelation, autorisation eller teknisk sammenstilling på initItSystemNavn alene.
- Modtager KAN anvende initItSystemNavn til visning, rapportering og manuel fejlsøgning.

**Databeskyttelse og sikkerhed:** initItSystemNavn bør ikke indeholde personoplysninger, bruger-id'er, CPR-numre, sagsoplysninger eller hemmeligheder.

**Eksempel:** "initItSystemNavn": "HR-portal"

**Typiske faldgruber:**

- Navnet anvendes som teknisk nøgle.
- Navnet varierer mellem logregistreringer.
- Navnet indeholder person- eller sagsoplysninger.

---

### 2.2.9. logregistrering.initBruger

**Formål:** Angiver bruger-id for den identificerbare bruger, der initierede persondatabehandlingen, når hændelsen er brugerinitieret.

**Semantik og uddybning:** initBruger anvendes til at identificere den bruger eller tekniske brugerreference, som initierede handlingen. Ved systeminitierede hændelser, batchkørsler, automatiske processer eller andre hændelser uden identificerbar bruger kan initBruger udelades. I sådanne tilfælde identificeres det initierende system fortsat via initItSystemID.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Hvis persondatabehandlingen er initieret af en identificerbar bruger, og brugeridentifikationen er tilgængelig for det initierende system, SKAL initBruger angives.
- Hvis elementet angives, SKAL værdien være en string.
- Elementet MÅ IKKE indeholde CPR-numre, tokens, nøgler, passwords eller andre hemmeligheder.

**Afsenderkrav:**

- Afsender SKAL angive initBruger, når persondatabehandlingen er initieret af en identificerbar bruger, og brugeridentifikationen er tilgængelig.
- Afsender KAN udelade initBruger ved systeminitierede hændelser uden identificerbar bruger.
- Afsender BØR anvende en stabil brugeridentifikator frem for brugerens navn.
- Afsender MÅ IKKE anvende initBruger til hemmeligheder eller autentifikationsmateriale.

**Modtagerkrav:**

- Modtager SKAL kunne modtage records uden initBruger.
- Hvis initBruger er angivet, SKAL modtager kunne behandle værdien som en brugeridentifikator.
- Modtager BØR anvende initBruger til audit, filtrering, rapportering og kontrol.
- Modtager BØR beskytte initBruger som personhenførbare eller potentielt personhenførbare oplysninger.

**Databeskyttelse og sikkerhed:** initBruger kan være personhenførbart. Adgang bør begrænses efter princippet om mindst mulig adgang.

**Eksempel:** "initBruger": "jd123"

**Typiske faldgruber:**

- initBruger udelades ved brugerinitieret persondatabehandling.
- initBruger udfyldes med fuldt navn eller CPR.
- initBruger udfyldes med session-token eller password.
- Elementet udfyldes mekanisk ved systeminitierede hændelser uden identificerbar bruger.

---

### 2.2.10. logregistrering.initOrgEnhedID

**Formål:** Angiver ID for den organisatoriske enhed, som den initierende bruger eller proces er knyttet til, når dette er relevant for audit og ansvarssporing.

**Semantik og uddybning:** initOrgEnhedID kan anvendes til at beskrive organisatorisk kontekst, fx afdeling, team eller enhed. Elementet er et supplement til initBruger og initOrgID.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Hvis elementet angives, SKAL værdien være en string.
- Elementet MÅ IKKE indeholde hemmeligheder.

**Afsenderkrav:**

- Afsender KAN angive elementet, når organisatorisk kontekst er relevant for revisionssporet.
- Afsender BØR anvende stabile og genkendelige værdier.
- Afsender MÅ IKKE anvende navnelementer som erstatning for ID-elementer, hvis stabile ID'er findes.

**Modtagerkrav:**

- Modtager SKAL kunne modtage records, hvor elementet ikke er angivet.
- Modtager KAN anvende elementet til audit, rapportering, filtrering og organisatorisk analyse.
- Modtager MÅ IKKE basere teknisk identifikation af bruger eller system på elementet alene.

**Databeskyttelse og sikkerhed:** Elementet bør ikke indeholde personoplysninger, CPR-numre, tokens, nøgler, passwords, sagsoplysninger eller hemmeligheder.

**Eksempel:** "initOrgEnhedID": "AFD-42"

**Typiske faldgruber:**

- Elementet anvendes som teknisk nøgle uden stabilitet.
- Elementet bruges som erstatning for initBruger eller initSystemID.
- Elementet indeholder fritext, personoplysninger eller lokale bemærkninger.

---

### 2.2.11. logregistrering.initOrgEnhedNavn

**Formål:** Angiver et læsevenligt navn for den organisatoriske enhed, som den initierende bruger eller proces er knyttet til.

**Semantik og uddybning:** initOrgEnhedNavn er et visnings- og rapporteringsvenligt supplement til initOrgEnhedID og er ikke den autoritative identifikation af enheden.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Logregistrering.

- Hvis elementet angives, SKAL værdien være en string.
- Elementet MÅ IKKE indeholde hemmeligheder.

**Afsenderkrav:**

- Afsender KAN angive elementet, når organisatorisk kontekst er relevant for revisionssporet.
- Afsender BØR anvende stabile og genkendelige værdier.
- Afsender MÅ IKKE anvende navnelementer som erstatning for ID-elementer, hvis stabile ID'er findes.

**Modtagerkrav:**

- Modtager SKAL kunne modtage records, hvor elementet ikke er angivet.
- Modtager KAN anvende elementet til audit, rapportering, filtrering og organisatorisk analyse.
- Modtager MÅ IKKE basere teknisk identifikation af bruger eller system på elementet alene.

**Databeskyttelse og sikkerhed:** Elementet bør ikke indeholde personoplysninger, CPR-numre, tokens, nøgler, passwords, sagsoplysninger eller hemmeligheder.

**Eksempel:** "initOrgEnhedsNavn": "Kundeservice"

**Typiske faldgruber:**

- Elementet anvendes som teknisk nøgle uden stabilitet.
- Elementet bruges som erstatning for initBruger eller initItSystemID.
- Elementet indeholder fritext, personoplysninger eller lokale bemærkninger.

**2.2.12. logregistrering.initOrgID**

**Formål:** Angiver ID for den organisation, som den initierende bruger, proces eller organisatoriske kontekst er knyttet til.

**Semantik og uddybning:** initOrgID kan anvendes til organisatorisk kontekst på organisationsniveau og er et valgfrit supplement til initItSystemID, initBruger og initOrgEnhedsID.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Hvis elementet angives, SKAL værdien være en string.
- Elementet MÅ IKKE indeholde hemmeligheder.

**Afsenderkrav:**

- Afsender KAN angive elementet, når organisatorisk kontekst er relevant for revisionssporet.
- Afsender BØR anvende stabile og genkendelige værdier.
- Afsender MÅ IKKE anvende navnelementer som erstatning for ID-elementer, hvis stabile ID'er findes.

**Modtagerkrav:**

- Modtager SKAL kunne modtage records, hvor elementet ikke er angivet.
- Modtager KAN anvende elementet til audit, rapportering, filtrering og organisatorisk analyse.
- Modtager MÅ IKKE basere teknisk identifikation af bruger eller system på elementet alene.

**Databeskyttelse og sikkerhed:** Elementet bør ikke indeholde personoplysninger, CPR-numre, tokens, nøgler, passwords, sagsoplysninger eller hemmeligheder.

**Eksempel:** "initOrgID": "ORG-123"

**Typiske faldgruber:**

- Elementet anvendes som teknisk nøgle uden stabilitet.
- Elementet bruges som erstatning for initBruger eller initItSystemID.
- Elementet indeholder fritext, personoplysninger eller lokale bemærkninger.

---

### 2.2.13. logregistrering.initOrgNavn

**Formål:** Angiver et læsevenligt navn for den organisation, som den initierende bruger, proces eller organisatoriske kontekst er knyttet til.

**Semantik og uddybning:** initOrgNavn er et visnings- og rapporteringsvenligt supplement til initOrgID og er ikke den autoritative identifikation af organisationen.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Hvis elementet angives, SKAL værdien være en string.
- Elementet MÅ IKKE indeholde hemmeligheder.

**Afsenderkrav:**

- Afsender KAN angive elementet, når organisatorisk kontekst er relevant for revisionssporet.
- Afsender BØR anvende stabile og genkendelige værdier.
- Afsender MÅ IKKE anvende navnelementer som erstatning for ID-elementer, hvis stabile ID'er findes.

**Modtagerkrav:**

- Modtager SKAL kunne modtage records, hvor elementet ikke er angivet.
- Modtager KAN anvende elementet til audit, rapportering, filtrering og organisatorisk analyse.
- Modtager MÅ IKKE basere teknisk identifikation af bruger eller system på elementet alene.

**Databeskyttelse og sikkerhed:** Elementet bør ikke indeholde personoplysninger, CPR-numre, tokens, nøgler, passwords, sagsoplysninger eller hemmeligheder.

**Eksempel:** "initOrgNavn": "Korsbæk Kommune"

**Typiske faldgruber:**

- Elementet anvendes som teknisk nøgle uden stabilitet.
- Elementet bruges som erstatning for initBruger eller initItSystemID.
- Elementet indeholder fritext, personoplysninger eller lokale bemærkninger.

---

### 2.2.14. logregistrering.execItSystemID

**Formål:** Angiver ID for det it-system, der udførte den loggede behandling eller operation.

**Semantik og uddybning:** execItSystemID identificerer det system, der udfører behandlingen eller er ansvarligt for den konkrete logregistrerede aktivitet. I simple scenarier kan initItSystemID og execItSystemID have samme værdi.

**Normative krav:**

- Elementet SKAL angives.
- Elementet er obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Værdien SKAL være en string.
- Værdien MÅ IKKE indeholde CPR-numre, brugeroplysninger, tokens, nøgler, passwords eller hemmeligheder.

**Afsenderkrav:**

- Afsender SKAL angive execItSystemID.
- Afsender SKAL anvende en stabil systemidentifikator.
- Afsender BØR anvende samme execItSystemID på tværs af hændelser fra samme system.
- Afsender MÅ IKKE anvende execItSystemNavn som erstatning for execItSystemID.

**Modtagerkrav:**

- Modtager SKAL validere, at execItSystemID er til stede og er en string.

- Modtager BØR anvende execItSystemID til audit, filtrering, rapportering, fejlhåndtering og korrelation.
- Modtager BØR kunne sammenholde execItSystemID med initItSystemID.

**Databeskyttelse og sikkerhed:** execItSystemID bør være en teknisk systemnøgle og MÅ IKKE indeholde personhenførbare oplysninger eller hemmeligheder.

**Eksempel:** "execItSystemID": "HR-KERNE-01"

**Typiske faldgruber:**

- execItSystemID ændres ved versionsopdateringer.
- Systemnavn anvendes som teknisk nøgle.
- initItSystemID og execItSystemID forveksles.

## 2.2.15. logregistrering.execItSystemNavn

**Formål:** Angiver et læsevenligt navn for det it-system, der udførte den loggede behandling eller operation.

**Semantik og uddybning:** execItSystemNavn er et visnings- og driftsvenligt supplement til execItSystemID og er ikke den autoritative systemidentifikation.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Hvis elementet angives, SKAL værdien være en string.

**Afsenderkrav:**

- Afsender KAN angive execItSystemNavn for læsbarhed.
- Afsender BØR anvende et stabilt og genkendeligt systemnavn.
- Afsender MÅ IKKE anvende execItSystemNavn som erstatning for execItSystemID.

**Modtagerkrav:**

- Modtager SKAL kunne modtage records uden execItSystemNavn.
- Modtager MÅ IKKE basere audit, korrelation, autorisation eller teknisk sammenstilling på execItSystemNavn alene.
- Modtager KAN anvende execItSystemNavn til visning, rapportering og manuel fejlsøgning.

**Databeskyttelse og sikkerhed:** execItSystemNavn bør ikke indeholde personoplysninger, bruger-id'er, CPR-numre, sagsoplysninger eller hemmeligheder.

**Eksempel:** "execItSystemNavn": "HR-kernesystem"

**Typiske faldgruber:**

- Navnet anvendes som teknisk nøgle.
- Navnet varierer mellem logregistreringer.
- Navnet indeholder person- eller sagsoplysninger.

## 2.2.16. logregistrering.srcGdprBehandlKat

**Formål:** Angiver afsenders vurdering af GDPR-behandlingskategori for den loggede hændelse.

**Semantik og uddybning:** srcGdprBehandlKat er afsenders best-effort-klassifikation. Modtager, pipeline eller SIEM kan normalisere eller omklassificere værdien i dstGdprBehandlKat, men den oprindelige src-værdi bør bevares af hensyn til sporbarhed.

**Normative krav:**

- Elementet KAN angives.

- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Hvis elementet angives, SKAL værdien være en string.
- Værdien BØR følge relevant GDPR-katalog.

**Afsenderkrav:**

- Afsender KAN angive src-elementer som best-effort.
- Afsender KAN undlade dst-elementer, hvis de først fastsættes af modtager, pipeline eller SIEM.
- Afsender BØR anvende værdier fra kataloget, når dækkende værdier findes.
- Afsender MÅ IKKE overskrive src-værdier med dst-værdier, hvis der er behov for at bevare afsenders oprindelige deklaration.

**Modtagerkrav:**

- Modtager SKAL kunne modtage records, hvor elementet ikke er angivet.
- Modtager KAN danne dst-elementer som led i normalisering, berigelse, rapportering eller SIEM-behandling.
- Modtager BØR bevare src-værdier som afsenders oprindelige deklaration.
- Modtager BØR anvende en dokumenteret og konsistent klassifikationspraksis.

**Eksempel:** "srcGdprBehandlKat": "soegning"

**Eksempel:** "srcGdprBehandlKat": "ukendt"

**Typiske faldgruber:**

- src-værdier overskrives ved modtagers omklassificering.
- Lokale værdier anvendes inkonsistent.
- dst-værdier antages at være angivet af afsender.

## 2.2.17. logregistrering.dstGdprBehandlKat

**Formål:** Angiver modtagers, pipelines eller SIEM-systemets normaliserede GDPR-behandlingskategori.

**Semantik og uddybning:** dstGdprBehandlKat kan anvendes, når modtager, pipeline eller SIEM ønsker at normalisere, supplere eller omklassificere afsenders deklaration i srcGdprBehandlKat.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Hvis elementet angives, SKAL værdien være en string.
- Værdien BØR følge relevant GDPR-katalog.

**Afsenderkrav:**

- Afsender KAN angive src-elementer som best-effort.
- Afsender KAN undlade dst-elementer, hvis de først fastsættes af modtager, pipeline eller SIEM.
- Afsender BØR anvende værdier fra kataloget, når dækkende værdier findes.
- Afsender MÅ IKKE overskrive src-værdier med dst-værdier, hvis der er behov for at bevare afsenders oprindelige deklaration.

**Modtagerkrav:**

- Modtager SKAL kunne modtage records, hvor elementet ikke er angivet.
- Modtager KAN danne dst-elementer som led i normalisering, berigelse, rapportering eller SIEM-behandling.
- Modtager BØR bevare src-værdier som afsenders oprindelige deklaration.
- Modtager BØR anvende en dokumenteret og konsistent klassifikationspraksis.

**Eksempel:** "dstGdprBehandlKat": "soegning"

**Typiske faldgruber:**

- src-værdier overskrives ved modtagers omklassificering.
- Lokale værdier anvendes inkonsistent.
- dst-værdier antages at være angivet af afsender.

**2.2.18. logregistrering.srcGdprDataKat**

**Formål:** Angiver afsenders vurdering af GDPR-datakategori for de oplysninger, som hændelsen vedrører.

**Semantik og uddybning:** srcGdprDataKat er afsenders best-effort-klassifikation af datakategorien, fx Almindelige, Særlige\_art9, Strafbare\_art10, Blandede eller Ukendt. Den oprindelige src-værdi bør bevares af hensyn til sporbarhed.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Hvis elementet angives, SKAL værdien være en string.
- Værdien BØR følge relevant GDPR-katalog.

**Afsenderkrav:**

- Afsender KAN angive src-elementer som best-effort.
- Afsender KAN undlade dst-elementer, hvis de først fastsættes af modtager, pipeline eller SIEM.
- Afsender BØR anvende værdier fra kataloget, når dækkende værdier findes.
- Afsender MÅ IKKE overskrive src-værdier med dst-værdier, hvis der er behov for at bevare afsenders oprindelige deklaration.

**Modtagerkrav:**

- Modtager SKAL kunne modtage records, hvor elementet ikke er angivet.
- Modtager KAN danne dst-elementer som led i normalisering, berigelse, rapportering eller SIEM-behandling.
- Modtager BØR bevare src-værdier som afsenders oprindelige deklaration.
- Modtager BØR anvende en dokumenteret og konsistent klassifikationspraksis.

**Eksempel:** "srcGdprDataKat": "Almindelige"

**Eksempel:** "srcGdprDataKat": "Ukendt"

**Typiske faldgruber:**

- src-værdier overskrives ved modtagers omklassificering.
- Lokale værdier anvendes inkonsistent.
- dst-værdier antages at være angivet af afsender.

**2.2.19. logregistrering.dstGdprDataKat**

**Formål:** Angiver modtagers, pipelines eller SIEM-systemets normaliserede GDPR-datakategori.

**Semantik og uddybning:** dstGdprDataKat kan anvendes, når modtager, pipeline eller SIEM ønsker at normalisere, supplere eller omklassificere afsenders deklaration i srcGdprDataKat.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Hvis elementet angives, SKAL værdien være en string.
- Værdien BØR følge relevant GDPR-katalog.

**Afsenderkrav:**

- Afsender KAN angive src-elementer som best-effort.
- Afsender KAN undlade dst-elementer, hvis de først fastsættes af modtager, pipeline eller SIEM.
- Afsender BØR anvende værdier fra kataloget, når dækkende værdier findes.
- Afsender MÅ IKKE overskrive src-værdier med dst-værdier, hvis der er behov for at bevare afsenders oprindelige deklaration.

**Modtagerkrav:**

- Modtager SKAL kunne modtage records, hvor elementet ikke er angivet.
- Modtager KAN danne dst-elementer som led i normalisering, berigelse, rapportering eller SIEM-behandling.
- Modtager BØR bevare src-værdier som afsenders oprindelige deklaration.
- Modtager BØR anvende en dokumenteret og konsistent klassifikationspraksis.

**Eksempel:** "dstGdprDataKat": "Almindelige"

**Eksempel:** "dstGdprDataKat": "Blandede"

**Typiske faldgruber:**

- src-værdier overskrives ved modtagers omklassificering.
- Lokale værdier anvendes inkonsistent.
- dst-værdier antages at være angivet af afsender.

## 2.2.20. logregistrering.visteOpl

**Formål:** Angiver hvilke typer oplysninger der er vist eller behandlet i forbindelse med den loggede hændelse.

**Semantik og uddybning:** visteOpl beskriver oplysningstyper på klassifikationsniveau og ikke konkrete oplysningsværdier. Elementet er en flad liste af strenge i formatet gdprDataKat|oplysningstype. person.identitet.cpr i visteOpl betyder alene, at CPR som oplysningstype er vist eller behandlet.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Hvis elementet angives, SKAL værdien være et array.
- Hvert element SKAL være en string i formatet gdprDataKat|oplysningstype.
- Arrayet MÅ IKKE indeholde objekter eller nestede arrays.
- Elementet MÅ IKKE indeholde konkrete oplysningsværdier.

**Afsenderkrav:**

- Afsender KAN angive visteOpl som best-effort.
- Afsender BØR anvende oplysningstyper fra datakataloget.
- Afsender BØR anvende passende gdprDataKat for hver oplysningstype.
- Afsender MÅ IKKE angive konkrete oplysningsværdier.
- Afsender BØR undgå meget store arrays og kan opdele hændelser og sammenkæde via teknCtx.

**Modtagerkrav:**

- Modtager SKAL kunne modtage records uden visteOpl.
- Hvis visteOpl er angivet, SKAL modtager kunne behandle elementet som en flad liste.
- Modtager BØR validere formatet for hvert element.
- Modtager MÅ IKKE fortolke person.identitet.cpr som selve CPR-nummeret.

**Databeskyttelse og sikkerhed:** visteOpl kan afsløre hvilke typer oplysninger der er behandlet og bør beskyttes efter behov.

**Eksempel:** "visteOpl": ["Almindelige|person.identitet.cpr",  
"Almindelige|person.identitet.navn\_fuldt"]

**Typiske faldgruber:**

- Konkrete værdier angives i visteOpl.
- person.identitet.cpr misforstås som CPR-værdi.
- visteOpl udfyldes som objekter.
- Arrayet bliver meget stort.

### 2.2.21. logregistrering.visteOpl.element

**Formål:** Angiver én oplysningstype, der er vist eller behandlet.

**Semantik og uddybning:** Et visteOpl-element er en enkelt string i formatet gdprDataKat|oplysningstype. Hvis gdprDataKat eller oplysningstype indeholder separatoren | eller escape-tegnet \, SKAL tegnene escapes efter den fælles escape-regel.

**Normative krav:**

- Elementet KAN forekomme 0..\* gange i visteOpl.
- Hvis elementet forekommer, SKAL det være en string.
- Elementet SKAL følge formatet gdprDataKat|oplysningstype.
- gdprDataKat-delen og oplysningstype-delen SKAL være angivet.
- Elementet MÅ IKKE indeholde konkrete oplysningsværdier eller objekter.

**Afsenderkrav:**

- Afsender SKAL danne hvert element som gdprDataKat|oplysningstype.
- Afsender BØR anvende værdier fra datakataloget.
- Afsender MÅ IKKE placere konkrete personoplysninger eller dokumentindhold i elementet.
- Afsender BØR escape separator-tegn efter den fælles escape-regel.

**Modtagerkrav:**

- Modtager SKAL kunne parse elementer efter formatet.
- Modtager BØR anvende delene til indeksering, filtrering, analyse og rapportering.
- Modtager MÅ IKKE fortolke oplysningstype-delen som en konkret oplysningsværdi.

**Eksempel:** "Almindelige|person.identitet.cpr"

**Eksempel:** "Saerlige\_art9|person.helbred.diagnose"

**Typiske faldgruber:**

- Separatoren | udelades.
- Elementet angives som JSON-objekt.
- CPR-nummer eller navn angives som værdi.
- gdprDataKat og oplysningstype byttes om.

### 2.2.22. logregistrering.personCpr

**Formål:** Angiver CPR-nummer for den fysiske person, som logregistreringen vedrører, når der er én entydigt identificeret person.

**Semantik og uddybning:** personCpr er et valgfrit, søgbart personreferenceelement. Det kan anvendes, når logregistreringen vedrører én entydigt identificeret fysisk person, og CPR-nummeret er nødvendigt som søge- eller sammenstillingsnøgle. Ved flere personer anvendes personCpr ikke; i stedet kan personerne angives i behandlObj. personCpr skal adskilles fra visteOpl, hvor person.identitet.cpr kun angiver CPR som oplysningstype.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Hvis elementet angives, SKAL værdien være en string.
- Elementet KAN angives, når logregistreringen vedrører én entydigt identificeret fysisk person, og CPR-nummeret er nødvendigt.
- Ved logregistreringer, der vedrører flere personer, anvendes `personCpr` ikke som enkeltreference. `personCpr` MÅ IKKE anvendes til kun at angive én af flere personer.

**Afsenderkrav:**

- Afsender KAN angive personCpr ved én entydigt identificeret fysisk person.
- Afsender BØR kun angive personCpr, hvis det er nødvendigt og proportionalt.
- Afsender MÅ IKKE angive personCpr ved listervisninger eller flerpersone-scenarier.
- Afsender BØR anvende behandlObj ved flere personer eller andre behandlingsobjekter.

**Modtagerkrav:**

- Modtager SKAL kunne modtage records uden personCpr.
- Hvis personCpr er angivet, SKAL modtager kunne behandle værdien som personreference.
- Modtager BØR beskytte personCpr efter princippet om mindst mulig adgang.
- Modtager MÅ IKKE fortolke person.identitet.cpr i visteOpl som CPR-nummeret.

**Databeskyttelse og sikkerhed:** personCpr er en direkte personidentifikator og bør kun anvendes, når det er nødvendigt og proportionalt.

**Eksempel:** "personCpr": "0101701234"

**Typiske faldgruber:**

- personCpr anvendes ved listervisninger med flere personer.
- personCpr udfyldes, selvom en mindre følsom identifikator er tilstrækkelig.
- personCpr anvendes som generel personliste.

**2.2.23. logregistrering.behandlObj**

**Formål:** Angiver et eller flere behandlingsobjekter, som den loggede hændelse vedrører.

**Semantik og uddybning:** behandlObj er en flad liste af strengværdier. Hvert element angives som type|værdi eller kun type ved dataminimering. Ved flere personer anvendes behandlObj i stedet for personCpr.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Hvis elementet angives, SKAL værdien være et array.
- Hvert element SKAL være en string.
- Hvert element SKAL følge formatet type|værdi eller type.
- Arrayet MÅ IKKE indeholde objekter eller nestede arrays.

**Afsenderkrav:**

- Afsender KAN angive behandlObj, når det er relevant for revisionsformålet.
- Afsender BØR anvende objekttyper fra datakataloget.
- Afsender BØR kun angive værdi-delen, når konkret identifikation er nødvendig og proportional.
- Afsender BØR anvende type uden værdi ved dataminimering.
- Afsender BØR undgå meget store arrays og kan opdele hændelser og sammenkæde via teknCtx.

**Modtagerkrav:**

- Modtager SKAL kunne modtage records uden behandlObj.
- Hvis behandlObj er angivet, SKAL modtager kunne behandle elementet som en flad liste.

- Modtager BØR kunne parse type|værdi eller type uden værdi.
- Modtager BØR kunne anvende behandlObj til audit, søgning, filtrering, rapportering og analyse.

**Databeskyttelse og sikkerhed:** behandlObj kan indeholde personhenførbare eller forretningskritiske identifikatorer. Værdi-delen bør kun anvendes, når den er nødvendig.

**Eksempel:** "behandlObj": ["Person|0101701234", "Sag|SAG-12345"]

**Eksempel:** "behandlObj": ["Person"]

**Typiske faldgruber:**

- behandlObj udfyldes som objekter.
- Der angives konkrete personidentifikatorer unødigt.
- behandlObj bruges til oplysningstyper.
- Arrayet bliver meget stort.

## 2.2.24. logregistrering.behandlObj.element

**Formål:** Angiver ét behandlingsobjekt, som den loggede hændelse vedrører.

**Semantik og uddybning:** Et behandlObj-element er en enkelt string, der enten angives som type|værdi eller kun som type. Hvis type eller værdi indeholder separatoren | eller escape-tegnet \, SKAL tegnene escapes efter den fælles escape-regel.

**Normative krav:**

- Elementet KAN forekomme 0..\* gange i behandlObj.
- Hvis elementet forekommer, SKAL det være en string.
- Elementet SKAL følge formatet type|værdi eller type.
- type-delen SKAL være angivet.
- værdi-delen KAN udelades ved dataminimering.
- Elementet MÅ IKKE indeholde objekter eller nestede strukturer.

**Afsenderkrav:**

- Afsender SKAL danne hvert element som en string.
- Afsender BØR anvende objekttyper fra datakataloget.
- Afsender BØR kun angive værdi-delen, når konkret identifikation er nødvendig og proportional.
- Afsender BØR anvende type uden værdi ved dataminimering.
- Afsender BØR escape separator-tegn efter den fælles escape-regel.

**Modtagerkrav:**

- Modtager SKAL kunne parse elementer som type|værdi eller type.
- Modtager BØR kunne anvende type-delen til filtrering, analyse og rapportering.
- Modtager BØR kunne anvende værdi-delen til søgning og sammenstilling, når den er angivet.
- Modtager SKAL kunne håndtere elementer uden værdi-del.

**Eksempel:** "Person|0101701234"

**Eksempel:** "Sag|SAG-12345"

**Eksempel:** "Person"

**Typiske faldgruber:**

- Separatoren | udelades.
- Elementet angives som JSON-objekt.
- type og værdi byttes om.
- Værdi angives, selvom type alene er tilstrækkeligt.

### 2.2.25. logregistrering.teknCtx

**Formål:** Angiver supplerende teknisk kontekst for logregistreringen, fx til korrelation, fejlsøgning, tekniske statuskoder, fejlkoder, sporbarhed og drift.

**Semantik og uddybning:** teknCtx er en flad liste af tekniske kontekstelementer. Hvert element angives som en streng i formatet type|værdi. Tekniske statuskoder, HTTP-koder, applikationsfejlkoder og debug-relaterede oplysninger angives ikke i operationTilstand, men KAN angives i teknCtx.

**Normative krav:**

- Elementet KAN angives.
- Elementet er ikke obligatorisk i JSON-schemaets required-liste for Logregistrering.
- Hvis elementet angives, SKAL værdien være et array.
- Hvert element SKAL være en string i formatet type|værdi.
- Arrayet MÅ IKKE indeholde objekter eller nestede arrays.
- teknCtx MÅ IKKE indeholde hemmeligheder.

**Afsenderkrav:**

- Afsender KAN angive teknCtx ved behov for teknisk kontekst, korrelation, fejlsøgning eller driftsspor.
- Afsender SKAL sikre, at hvert teknCtx-element følger formatet type|værdi.
- Afsender BØR anvende relevante teknCtx-typer fra datakataloget, når de er tilgængelige.
- Ved teknisk korrelation og fejlsøgning BØR udvikler som udgangspunkt anvende en relevant kernegruppe af teknCtx-typer, fx korrelationsId, requestId, traceId, transaktionsId, api.statuskode og fejl.kode. Ved fejlscenarier kan fejl.type desuden angives, hvis det er relevant.
- Afsender MÅ IKKE placere hemmeligheder i teknCtx.
- Afsender BØR undgå personhenførbare oplysninger i teknCtx, medmindre der er et klart og dokumenteret revisions- eller driftsbehov.
- Afsender BØR undgå meget store arrays og kan opdele hændelser og sammenkæde via korrelationsId, traceId eller transaktionsId.

**Modtagerkrav:**

- Modtager SKAL kunne modtage records uden teknCtx.
- Hvis teknCtx er angivet, SKAL modtager kunne behandle elementet som en flad liste af type|værdi-streng.
- Modtager BØR kunne parse type-delen og værdi-delen til indeksering, filtrering, analyse, fejlsøgning og korrelation.
- Modtager SKAL kunne håndtere ukendte type-værdier uden at afvise alene af den grund, hvis formatet er gyldigt.
- Modtager BØR beskytte værdier i teknCtx som driftsdata og begrænse adgang efter behov.

**Databeskyttelse og sikkerhed:** teknCtx er beregnet til teknisk metadata og MÅ IKKE indeholde tokens, nøgler, passwords eller andre hemmeligheder.

**Eksempel:** "teknCtx": ["requestId|REQ-c117", "korrelationsId|CORR-20260312-000043", "api.statuskode|403", "fejl.kode|AUTHZ\_DENIED"]

**Typiske faldgruber:**

- teknCtx udfyldes som objekter.
- Tekniske fejlkoder angives i operationTilstand.
- teknCtx indeholder hemmeligheder.
- teknCtx anvendes til forretningsdata eller konkrete personoplysninger.
- Arrayet bliver meget stort.

## 2.2.26. logregistrering.teknCtx.element

**Formål:** Angiver ét teknisk kontekstelement i teknCtx.

**Semantik og uddybning:** Et teknCtx-element er en enkelt string i formatet type|værdi. type angiver den tekniske oplysning, fx requestId, korrelationsId, traceId, transaktionId, api.statuskode, fejl.kode eller fejl.type. Hvis type eller værdi indeholder separatoren | eller escape-tegnet \, SKAL tegnene escapes efter den fælles escape-regel.

**Normative krav:**

- Elementet KAN forekomme 0..\* gange i teknCtx.
- Hvis elementet forekommer, SKAL det være en string.
- Elementet SKAL følge formatet type|værdi.
- type-delen SKAL være angivet.
- værdi-delen SKAL være angivet.
- Elementet MÅ IKKE indeholde objekter eller nestede strukturer.
- Elementet MÅ IKKE indeholde hemmeligheder.

**Afsenderkrav:**

- Afsender SKAL danne hvert element som en type|værdi-streng.
- Afsender BØR anvende stabile type-navne på tværs af hændelser og systemversioner.
- Afsender BØR anvende relevante typer fra datakataloget.
- Afsender MÅ IKKE placere tokens, nøgler, passwords eller andre hemmeligheder i værdien.
- Afsender BØR escape separator-tegn efter den fælles escape-regel.

**Modtagerkrav:**

- Modtager SKAL kunne parse elementer efter type|værdi-formatet.
- Modtager BØR kunne anvende type-delen til indeksering, filtrering, korrelation og analyse.
- Modtager BØR kunne anvende værdi-delen til teknisk fejlsøgning, sporing og sammenstilling.
- Modtager SKAL kunne håndtere ukendte type-værdier uden at afvise alene af den grund.
- Modtager BØR markere eller afvise elementer, der ikke følger formatet, afhængigt af valideringspolitikken.

**Eksempel:** "requestId|REQ-c117"

**Eksempel:** "api.statuskode|403"

**Eksempel:** "fejl.kode|AUTHZ\_DENIED"

**Typiske faldgruber:**

- Separatoren | udelades.
- Elementet angives som JSON-objekt.
- type-delen ændrer navn mellem hændelser uden begrundelse.
- Værdien indeholder hemmeligheder eller unødvendige personoplysninger.
- Debug-information placeres ukritisk uden dataminimering.