

Sammenligningsskjema for DPP-leverandører

Bare eksisterende, verifiserbare funksjoner merkes av – ingen kunngjøringer eller intensjonserklæringer.

Kolonnen «Transpareo» er forhåndsutfylt; de to tomme kolonnene fyller du ut når du vurderer andre leverandører. Forklaringer og kilder til hvert kriterium finner du på slutten av dokumentet.

Per: 10.09.2026

Lovpålagt

Kriterium	Transpareo		
Datautveksling i et åpent, standardisert format Passdataene er tilgjengelige via åpne standarder – og kan leses av alle systemer med tilgang, ikke bare av programvaren til én enkelt leverandør. EN 18216	☒	☐	☐
Unik, portabel identifikator uten tilknytning til en bestemt leverandør Produktkoden tilhører produktet, ikke plattformen – ved bytte av leverandør beholder passet sin identitet. EN 18219	☒	☐	☐
Fysisk datamedium, kan leses på lang sikt QR-koden på produktet fører til passet i alle nettlesere – uten app, uten konto, med hvilken som helst smarttelefon. EN 18220	☒	☐	☐
Lagring og arkivering utover minimumsperioden Hver publisert versjon forblir tilgjengelig i den lovbestemte perioden – også eldre versjoner, ikke bare den gjeldende. EN 18221	☒	☐	☐

Kriterium	Transpareo		
API for livssyklusadministrasjon og søkbarhet Et programmeringsgrensesnitt leser, oppretter og søker i pass – ikke bare et nettgrensesnitt man klikker seg gjennom. EN 18222	☒	☐	☐
Interoperabel datamodell Passdataene følger en felles modell som andre systemer kan lese uten å måtte omformatere dem. EN 18223	☒	☐	☐
Et tre-trinns modell for tilgangsrettigheter Offentlige, autoriserte og myndighetsrelaterte data er tydelig adskilt – hver enkelt ser nøyaktig det han eller hun har tilgang til. EN 18239	☒	☐	☐
Påvisbar dataautentisitet og integritet Hver versjon er dobbeltsignert og kan verifiseres i nettleseren – uten at du trenger å stole på oss, utelukkende på grunnlag av dataene. EN 18246	☒	☐	☐
Kobling til EU-kommisjonens register Registrering med offisiell bekreftelse – så snart EU offentliggjør det tekniske grensesnittet. Dette foreligger ikke ennå, og ingen leverandør kan oppfylle dette kravet i dag.	☐	☐	☐
Oppbevaring av registreringsdata utover den lovbestemte fristen Et uforanderlig tiårig arkiv – verken produsenten eller Transpareo kan endre en versjon i etterkant.	☒	☐	☐
Produktdata på de offisielle språkene i hvert målmarked Det obligatoriske innholdet skal vises på de offisielle språkene i hvert land der produktet selges – ved salg i hele EU altså på alle 24 offisielle språk, ikke bare på hjemmemarkedet.	☒	☐	☐

Nyttig for drift av en DPP-database

Kriterium	Transpareo		
Språk utenfor EU 16 språk i tillegg til de 24 offisielle EU-språkene - 40 i alt, for målmarkeder utenfor Unionen.	☒	☐	☐
Versjonering og endringshistorikk Hver endring genererer en ny, sporbar versjon med tidspunkt og opphavsperson - gjennom hele produktets livssyklus.	☒	☐	☐
Skalerbar masseproduksjonsanlegg for produktfamilier Last opp produktdata via Excel eller CSV og tilordne dem til de obligatoriske feltene - for store mengder finnes det i tillegg en bulk-API.	☒	☐	☐
Rollebasert intern rettighetsadministrasjon Det er fastsatt hvem i bedriften som har lov til å vedlikeholde eller dele hvilke data - inkludert strengt begrenset, tidsbegrenset tilgang for eksterne.	☒	☐	☐
Oppbevaring utover avtaleperiodens utløp Hvis du sier opp abonnementet, vil de publiserte passene dine fortsatt være tilgjengelige i det uendrerbare tiårsarkivet.	☒	☐	☐
Signatur med egen kryptografisk nøkkel Bring Your Own Key: Du oppbevarer den private nøkkelen selv, vi legger bare til en uavhengig motsignatur.	☒	☐	☐
Utstilleridentitet uavhengig av plattform Utstilleridentiteten din ligger som DID:web på ditt eget domene, ikke på vårt - et bytte av leverandør innebærer en DNS-flytting.	☒	☐	☐
Mulighet for tredjepartsverifisering, helt uten leverandøren En åpen kildekode-renderer sjekker hashverdier og signaturer i nettleseren - uten å kontakte en av våre servere.	☒	☐	☐

Ønskelige tilleggskfunksjoner

Kriterium	Transpareo		
Bytt leverandør uten tap av data Ved overgangen tar du med deg hele passbestanden i åpne formater – signert og med mulighet for selvkontroll; ved kontraktens utløp forblir de obligatoriske passene tilgjengelige i et uendringsbart tiårig arkiv, uten tap av data.	☒	☐	☐
Integrasjon med eksisterende systemer i stedet for dataklo Signerte webhooks og en bulk-API integrerer Pass med systemene dine – ingen ferdiglagd kobling for et bestemt ERP-system.	☒	☐	☐
Batch-import og –eksport utover det som er strengt nødvendig i henhold til EU-regelverket Større datamengder kan flyttes i begge retninger – ikke bare de obligatoriske feltene.	☒	☐	☐

Sikkerhet og personvern

Kriterium	Transpareo		
Separat database og egen nøkkel Opplysningene dine lagres i en egen database, kryptert med en egen nøkkel – adskilt på både database- og krypteringsnivå.	☒	☐	☐
Kryptering og sikkerhetskopiering TLS for alle tilkoblinger, AES-kryptering av sensitive data og krypterte sikkerhetskopier med nøkkelrotasjon.	☒	☐	☐
Sikkerhetshendelseslogg Innloggingsforsøk, MFA-utfordringer og aktivitet knyttet til API-nøkler loggføres og oppbevares i ett år.	☒	☐	☐
Flerfaktoraутentisering Autentiseringsapp, passordnøkkel eller maskinvarenøkkel for alle brukere, med reservekoder i tilfelle tap.	☒	☐	☐

Kriterium	Transpareo	_____	_____
ISO 27001-sertifisert hosting i Tyskland Server i Tyskland med strenge fysiske og organisatoriske sikkerhetstiltak.	☒	☐	☐

Økonomiske og organisatoriske spørsmål

Kriterium	Transpareo	_____	_____
Tar leverandøren seg av EU-registreringen for deg? Vi tar oss av registreringen, inkludert offisiell bekreftelse, så snart EU offentliggjør grensesnittet - det medfører ingen ekstra arbeidsbelastning for deg.	☒	☐	☐
Tydelige regler for supportarbeid og supportkostnader Kundestøtte er inkludert i prisen hos Transpareo - ingen separat supportavtale, ingen tilleggskostnader.	☒	☐	☐
Gjennomsiktig prisstruktur Fire offentlige prisplaner for alle bedriftsstørrelser, gratis prøveperiode, kan sies opp når som helst - uten skjulte tilleggskostnader per språk, produkt eller API-kall.	☒	☐	☐

Forklaringer og kilder

Datautveksling i et åpent, standardisert format **EN 18216**

Standarden krever at digitale produktpass skal være tilgjengelige via åpne, standardiserte protokoller - slik at myndigheter, samarbeidspartnere og deres egne systemer kan lese dataene uten å være bundet til en bestemt leverandørs programvare. Et proprietært format ville være en «Ø»: Uten leverandøren ville dere ikke lenger ha tilgang til deres egne data. Standarden er sitert i EUs offisielle tidsskrift siden 15. juli 2026 (gjennomføringsbeslutning (EU) 2026/1736) og er dermed underlagt formodningen om samsvar med ESPR.

Transpareo leverer alle passdata og grensesnitt via standard HTTPS i strukturert, maskinlesbar form - uten spesialprogramvare, uten proprietære protokoller. Hver publiserte versjon er i tillegg signert, slik at en mottaker ikke bare kan lese, men også kontrollere at dataene er uendret. Det du ser i grensesnittet, er det samme datasettet som ethvert autorisert system henter via de åpne grensesnittene.

Kilde: EN 18216, Krav til datautvekslingsprotokoller: «For standardisert DPP-tilgang skal de fastsatte datautvekslingsprotokollene benyttes.»

Unik, portabel identifikator uten tilknytning til en bestemt leverandør EN 18219

Hvert produktpass må ha en entydig identifikator som permanent henviser til det samme produktet og ikke er avhengig av en bestemt leverandør. Hvis en leverandør knytter identifikatoren til sin egen infrastruktur, mister du identiteten til passene dine ved et bytte – hver utskrevne kode og hver registrering vil da peke mot ingenting. Standarden er publisert i EUs offisielle tidsskrift siden 15. juli 2026.

Transpareo tildeler identifikatoren som en GS1 Digital Link med din GTIN – en åpen industristandard som tilhører produktet, ikke plattformen – og sjekker hver identifikator mot de godkjente standardskjemaene. Signaturidentiteten ligger som DID:web på ditt eget domene, ikke på vårt. Identifikatoren forblir gyldig, selv om et system svikter: En permanent reserveadresse løser den videre, og passet beholder sin identitet uavhengig av leverandørskifte.

Kilde: EN 18219, avsnitt 4.6.2(3): «Den entydige identifikatoren må ikke føre til en leverandørbinding.»

Fysisk datamedium, kan leses på lang sikt EN 18220

Passet må være tilgjengelig via et maskinlesbart datamedium på produktet, som alle kan få tilgang til uten spesialprogramvare – og som forblir lesbart gjennom hele produktets levetid, også etter bruk og reparasjon. Et datamedium som krever en bestemt app eller en konto, utelukker en del av allmennheten. Standarden er sitert i EUs offisielle tidsskrift siden 15. juli 2026.

Transpareo genererer en QR-kode i henhold til ISO/IEC 18004, som inneholder en GS1 Digital Link-adresse og fører direkte til passet i enhver nettleser – uten pålogging, uten nedlasting, på alle smarttelefoner. Modell, batch og artikkel er allerede innebygd i den kodede adressen, slik at en skanning fører direkte til riktig nivå. Fordi adressen forblir stabil gjennom en permanent fallback-oppløsning, forblir en kode som er skrevet ut én gang gyldig gjennom hele produktets levetid.

Kilde: EN 18220, Krav til datamedier (avsnitt 5): Symbolikk, koding, utskriftskvalitet og holdbarhet; datamediet skal forbli lesbart også etter flere bruks- og reparasjonssykluser.

Lagring og arkivering utover minimumsperioden EN 18221

Standarden krever at en standard, sammen med versjonshistorikken, lagres i den tidsperioden som er foreskrevet i regelverket, og at den forblir tilgjengelig uten endringer. Hvis man kun oppbevarer den gjeldende versjonen, går sporbarheten av tidligere opplysninger tapt – og det er nettopp dette en næringsaktør må kunne dokumentere overfor myndighetene. Oppbevaringsfristen fastsettes i henhold til gjeldende sektorlovgivning, men er på minst ti år. Standarden er sitert i EUs offisielle tidsskrift siden 15. juli 2026.

Transpareo lagrer hver publisering som en fastfrosset, signert versjon i et uforanderlig arkiv, der ingen senere kan endre eller slette den – verken du eller vi. Eldre versjoner forblir tilgjengelige ved siden av den aktuelle, og hver versjon er utstyrt med tidsstempel og signatur. På denne måten kan det for ethvert tidspunkt dokumenteres hva passet viste på det aktuelle tidspunktet.

Kilde: EN 18221: «Det digitale produktpasset skal være tilgjengelig for autoriserte brukere gjennom hele produktets levetid.»

API for livssyklusadministrasjon og søkbarhet EN 18222

I tillegg til visning i nettleseren krever standarden et programmeringsgrensesnitt som gjør det mulig å opprette, lese, oppdatere og søke i passene ved hjelp av produktidentifikatorer. Uten et slikt grensesnitt må all massebehandling utføres manuelt, og andre systemer kan ikke utnytte passdatabasen automatisk. Standarden er publisert i EUs offisielle tidsskrift siden 15. juli 2026.

Transpareo støtter de foreskrevne standardmetodene via et versjonert, standardisert grensesnitt: Pass kan opprettes, leses, oppdateres og søkes gjennom side for side ved hjelp av produktidentifikatorer på en programstyrt måte. Det signerte passet leveres uendret – grensesnittet leverer nøyaktig de byte-ene som en kontrollør kan verifisere signaturen på.

Kilde: EN 18222: standardisert programmeringsgrensesnitt (API) for livssyklusadministrasjon og søkbarhet i DPP, slik det kreves i ESPR.

Interoperabel datamodell EN 18223

For at passene skal passe sammen på tvers av systemer og forsyningskjeder, foreskriver standarden en felles datamodell med enhetlig betydning av feltene. En leverandørspesifikk modell tvinger hver partner til å lage sin egen oversettelse – og hver oversettelse er en feilkilde. Standarden er sitert i EUs offisielle tidsskrift siden 15. juli 2026.

Transpareo bygger på et horisontalt vokabularlag med parallelle, anerkjente fagvokabularer (GS1, EPCIS og andre) og beskriver hvert datapunkt med henvisning til dets ordbok og datatype. Dermed får et mottakende system ikke bare vite hva et felt heter, men også hva det betyr – passet forblir lesbart uten omformatering.

Kilde: EN 18223: felles semantisk datamodell for systeminteroperabilitet i DPP.

Et tre-trinns modell for tilgangsrettigheter EN 18239

Et produktpass inneholder offentlige opplysninger, data for autoriserte aktører i næringslivet og data som kun er tilgjengelige for myndigheter; standarden krever at disse nivåene holdes adskilt og reguleres for hvert enkelt datafelt. Offentlige data må være tilgjengelige uten pålogging, mens alt annet kun er tilgjengelig etter godkjenning. EN 18239 er i ferd med å bli endelig vedtatt.

Transpareo håndterer synligheten som en egenskap for hvert enkelt datafelt: Det offentlige nivået leveres uten autentisering, de høyere nivåene er beskyttet via et eget, loggført grensesnitt for myndigheter med utelukkende lesetilgang, og hver tilgang til beskyttede data registreres i revisjonsloggen. Standardens tretrinnsmodell er dermed allerede i dag integrert i arkitekturen, ikke lagt til i etterkant.

Kilde: EN 18239 (utkast, i ferd med å bli endelig vedtatt): «Tilgang til offentlige data må være mulig for aktører både innenfor og utenfor EU uten ytterligere autentisering»; kontrollerte data krever autentisert, sporbar tilgang.

Påvisbar dataautentisitet og integritet EN 18246

Standarden krever at et pass' ekthet og integritet kan påvises, og at det skal være mulig å foreta en kontroll fritt og uten begrensninger. Tilliten må ikke være avhengig av leverandørens fortsatte eksistens, men må være knyttet til selve datasettet – ellers ville hvert pass bare være like troverdig som selskapet som til enhver tid drifter det. EN 18246 er i ferd med å bli endelig vedtatt.

Transpareo signerer hver publiserte versjon med to uavhengige nøkler (utsteder og Transpareo) og kobler versjonene sammen via deres hash, slik at heller ikke historikken kan omskrives uten at det blir lagt merke til. En åpen kildekode-renderer sjekker begge signaturene direkte i nettleseren, uten å kontakte en av våre servere – det påkrevde signerte, selvkontrollerbare beviset er dermed allerede implementert.

Kilde: EN 18246 (utkast, i ferd med å bli endelig vedtatt): Autentisiteten, påliteligheten og integriteten til DPP-dataene må kunne påvises.

Kobling til EU-kommisjonens register

Alle pass som er underlagt registreringsplikt, må i fremtiden være registrert i det sentrale EU-registeret, som utsteder en permanent registrerings-ID og et offisielt registreringsbevis. EU har ennå ikke offentliggjort det tekniske grensesnittet for dette – derfor kan ingen leverandør i dag dokumentere denne tilkoblingen; hvis en leverandør hevder dette, bør du spørre nærmere.

Transpareo har forberedt tilkoblingen så langt det er mulig uten grensesnittet: De nødvendige feltene (registrerings-ID, stabil backup-adresse, versjons-hash) er allerede opprettet i datamodellen. Så snart EU offentliggjør grensesnittet, aktiverer vi registreringen uten at du trenger å endre passene dine. Inntil da forblir denne avmerkingsboksen uavmerket – både hos oss og hos alle andre seriøse leverandører.

Kilde: Utkast til gjennomføringsforordning for DPP-registeret (Ares(2026)4424976).

Oppbevaring av registreringsdata utover den lovbestemte fristen

Registrerte passdata må forbli tilgjengelige uten endringer utover den lovbestemte fristen – som regel ti år fra registreringstidspunktet – selv i tilfelle produsentens konkurs eller nedleggelse av virksomheten. Plikten gjelder altså lenger enn både din avtale med en leverandør og selve leverandøren.

Transpareo opprettholder et uforanderlig arkiv for dette formålet, der ingen – verken produsenten eller vi – kan endre eller slette en versjon som en gang er lagret. Arkivet trer automatisk i kraft ved EU-registreringen. Og for å sikre at det forblir tilgjengelig selv om Transpareo en dag skulle opphøre å eksistere, er dets videre eksistens sikret gjennom en notarial deponering i Sveits.

Kilde: Gjennomføringsforordningen til DPP-registeret, art. 10(3) (oppbevaring i ti år).

Produktdata på de offisielle språkene i hvert målmarked

De obligatoriske opplysningene i et pass må være tilgjengelige på de offisielle språkene i hver medlemsstat der produktet markedsføres – ikke bare på språket der produsenten har sitt hovedkontor. Den som kun betjener hjemmemarkedet, oppfyller ikke kravet for alle andre målmarkeder.

Transpareo vedlikeholder hvert pass på flere språk og leverer det obligatoriske innholdet på alle 24 offisielle EU-språk. Dere legger inn innholdet én gang; språkversjonene genereres automatisk uten at dere må betale ekstra per språk eller vedlikeholde separate pass. Passet er dermed lesbart i samsvar med regelverket i hvert målmarked.

Kilde: Batteriforordningen (EU) 2023/1542: Opplysninger på de offisielle språkene i de medlemsstatene hvor produktet markedsføres.

Språk utenfor EU

Utover den lovpålagte plikten er det en fordel at et pass også dekker språk utenfor EU – for eksportmarkeder, internasjonale handelspartnere og forbrukere som ikke snakker et av EUs offisielle språk.

Transpareo vedlikeholder totalt 40 språkversjoner, inkludert de 24 offisielle EU-språkene. Du registrerer innholdet én gang og kan deretter vise det på hvilket som helst ønsket språk, uten å måtte betale ekstra per språk. Også grensesnittet der du vedlikeholder passene dine (Applikasjonsmanageren) er oversatt til alle 40 språkene, og du kan legge inn informasjon på hvilket som helst av de tilgjengelige språkene.

Versjonering og endringshistorikk

Et pass endres i løpet av produktets levetid; uten en fullstendig versjonshistorikk vil det senere ikke være mulig å dokumentere hvilken versjon som gjaldt når. Standarden krever derfor at alle endringer i passet arkiveres.

Transpareo lagrer hver utgivelse som en egen, signert versjon og registrerer hvem som har opprettet den, når den ble opprettet og hvilke felt som er endret. På denne måten kan alle opplysninger kontrolleres i ettertid, og en senere korreksjon overskriver ikke historikken, men fortsetter den.

Kilde: EN 18221: «Alle endringer i det digitale produktpasset skal arkiveres.»

Skalerbar masseproduksjonsanlegg for produktfamilier

De som har mange lignende produkter, kan ikke opprette hver enkelt produktprofil manuelt; et bærekraftig system trenger en måte å registrere hele produktfamilier på én gang.

Transpareo lar deg laste opp produktdata via Excel eller CSV og tilordne dem til de obligatoriske feltene; for svært store mengder er det i tillegg en bulk-API tilgjengelig som oppretter produktkortene programstyrt. Dermed kan opprettelsen skaleres fra et dusin til titusenvis av produktkort.

Rollebasert intern rettighetsadministrasjon

Ikke alle i bedriften skal ha rett til å redigere eller godkjenne innholdet i hvert pass; standarden krever en rollebasert rettighetsadministrasjon med loggført tilgang.

Transpareo tildeler rettigheter etter rolle og brukergruppe og loggfører hver endring. Også eksterne aktører som verksteder eller gjenvinningsbedrifter får kun svært begrenset, tidsbegrenset tilgang; myndigheter får tilgang via et separat grensesnitt med utelukkende lesetilgang, som merker hvert tilgangstilfelle i revisjonsloggen.

Kilde: EN 18239 (utkast), Administrasjon av tilgangsrettigheter: regulerer hvilke aktører som har lov til å vedlikeholde og dele DPP-data.

Oppbevaring utover avtaleperiodens utløp

Oppbevaringsplikten opphører ikke med kontrakten: Et registrert pass må forbli i kraft utover den lovbestemte fristen, selv om du slutter å bruke tjenesteleverandøren. En tjenesteleverandør som deaktiverer passene ved oppsigelse, etterlater deg et problem med regelverksetterlevelse.

Transpareo håndterer dette gjennom det samme uforanderlige tiårige arkivet som registreringsdataene – etter en oppsigelse leverer en permanent fallback-adresse passene videre, og myndighetsgrensesnittet henter den samme datasetten fra arkivet etter avtalens utløp. QR-koder som allerede er trykket, forblir gyldige.

Kilde: EN 18221: Arkivversjoner lagres også hos leverandøren av sikkerhetskopitjenester.

Signatur med egen kryptografisk nøkkel

Den som har den private signaturnøkkelen, kan utstede pass i utstederens navn; derfor er det tryggere at utstederen selv oppbevarer denne nøkkelen, i stedet for å overlate den til leverandøren.

Med «Bring Your Own Key» driver bedriften din sitt eget signaturendepunkt – Transpareo oppbevarer aldri den private nøkkelen og legger bare til en uavhengig motsignatur. Dermed har hver versjon to uavhengige signaturer, og utstederens signatur er en som Transpareo selv ikke kan generere.

Utstilleridentitet uavhengig av plattform

For at en verifikator skal kunne finne dine offentlige nøkler, må passet ha en offentliggjort utstederidentitet. Hvis denne ligger på leverandørens domene, binder den deg til denne leverandøren: Et bytte ville gjøre alle allerede utskrevne koder ugyldige.

Transpareo publiserer identiteten din som DID: på nettet på ditt eget domene, ikke på vårt – et bytte av leverandør blir dermed en DNS-flytting, og allerede utskrevne koder samt verifisering av dem forblir gyldige. I tillegg speiler vi hver offentlig nøkkel til en permanent adresse på tidspunktet for publiseringen, slik at hver versjon forblir verifiserbar, selv om den opprinnelige verten forsvinner.

Kilde: EN 18219, avsnitt 4.2.2 (Varighet): Identifikatorer forblir gyldige gjennom hele livssyklusen; nettdomenene kan overføres eller omdirigeres.

Mulighet for tredjepartsverifisering, helt uten leverandøren

Den avgjørende testen for tillit er om en tredjepart kan verifisere passet uten å benytte leverandørens infrastruktur. Standarden krever at verifisering av gyldighet og integritet skal være kostnadsfri og uten begrensninger for den som utfører verifiseringen.

Transpareo publiserer derfor en åpen kildekode-renderer som laster inn byteene fra en versjon fra en hvilken som helst kilde, beregner hashen på nytt og sjekker begge signaturene mot de offentlige nøklene som er oppgitt i passet – uten pålogging, uten å ringe oss, uten avhengighet av en aktiv plattform. Den som er skeptisk, kan lese kildekode.

Kilde: EN 18246 (utkast): «Kontrollen av gyldigheten og integriteten til DPP-dataene må kunne utføres av kontrolløren uten kostnader og uten begrensninger.»

Bytt leverandør uten tap av data

En leverandør som gjør det vanskelig å bytte, holder deg fast gjennom dine egne data – og hva som skjer med dataene når kontrakten utløper, avgjør om du fritt kan bytte leverandør. Standarden krever derfor at dataene kan overføres via et åpent, interoperabelt nettverk uten binding til en bestemt leverandør.

Transpareo lagrer de regulatoriske passartefaktene fra starten av i et åpent område som kan speiles offentlig: En enkel synkronisering genererer en fullstendig, signert kopi som selv sjekker seg mot de publiserte nøklene, uten at vi trenger å gjøre noe. Vi overleverer det fullstendige hendelsesarkivet via en signert, tidsbegrenset nedlastingsadresse til deg eller din nye leverandør, og den tilhørende produktkatalogen i tillegg som JSON-LD og CSV. Ved kontraktens utløp forblir de registrerte obligatoriske passene tilgjengelige via det uforanderlige tiårsarkivet: Den offentlige speilingen og arkivet forblir synkronisert og overfører det samme datasettet, allerede utskrevne QR-koder kan fortsatt løses opp via den permanente fallback-adressen, og registerhenvisningen peker mot den nye adressen. På denne måten avsluttes avtalen uten tap av data og uten brudd på lovbestemte oppbevaringskrav.

Kilde: EN 18216: Data må kunne «overføres via et åpent, interoperabelt nettverk uten leverandørbinding».

Integrasjon med eksisterende systemer i stedet for dataklo

Et pass som kun finnes i leverandørens grensesnitt, blir en dataøy i forhold til de øvrige systemene dine – hver endring må da oppdateres to ganger.

Transpareo rapporterer hendelser via signerte webhooks og lar deg importere og eksportere data via en bulk-API, slik at du kan integrere Passet med ditt eget systemlandskap. Vi leverer bevisst ikke en ferdiglaget kobling for et bestemt ERP-system – de åpne, signerte grensesnittene passer til alle systemer, i stedet for å favorisere ett bestemt.

Batch-import og -eksport utover det som er strengt nødvendig i henhold til EU-regelverket

De som ønsker å bruke de registrerte dataene også utenfor passet, trenger import- og eksportfunksjoner for mer enn bare de lovpålagte feltene.

Transpareo mottar store datamengder via Excel, CSV og Bulk-API og eksporterer dem i samme omfang. Dermed tjener systemet ikke bare til å oppfylle EU-kravene, men også til din egen datahåndtering.

Separat database og egen nøkkel

I en delt database er opplysningene dine knyttet til opplysningene til andre kunder; en klar og påvisbar adskillelse er da nesten umulig – og retten til sletting i henhold til GDPR artikkel 17 er vanskelig å dokumentere.

Hos Transpareo ligger hver kunde i sin egen database, kryptert med en egen nøkkel – adskillelsen skjer både på databasenivå og på krypteringsnivå. Dette oppfyller retten til sletting gjennom verifiserbar sletting; hosting skjer i Tyskland, og avtalen om databehandling (AVV) er inkludert.

Kilde: GDPR art. 17 (rett til sletting), oppfylt gjennom separat database, egen nøkkel og verifiserbar sletting.

Kryptering og sikkerhetskopiering

En leverandør må beskytte data både under overføring og i hvile, samt sikre dem mot svikt; GDPR krever at det treffes tiltak i samsvar med dagens tekniske standard.

Transpareo krypterer alle tilkoblinger med TLS og sensitive applikasjonsdata med AES. Sikkerhetskopiene er GPG-kryptert, oppdateres med regelmessig nøkkelrotasjon, lages hver fjerde time og oppbevares i tolv måneder på en separat server.

Kilde: GDPR art. 32 (Sikkerhet ved behandling): TLS, AES og krypterte sikkerhetskopier med rotasjon.

Sikkerhetshendelseslogg

Sikkerhetsrelevante hendelser må kunne spores – hvem som har logget seg på, når det skjedde, og hvordan nøklene ble brukt. NIS-2-direktivet krever tilsvarende revisjonslogger.

Transpareo fører en sikkerhetshendelseslogg over påloggingsforsøk, MFA-utfordringer og API-nøkkelaktivitet, og oppbevarer den i ett år. Dermed oppfylles NIS-2-kravene til revisjonslogger.

Kilde: NIS-2-direktivet (krav til revisjonslogger): loggførte sikkerhetshendelser, oppbevaring i ett år.

Flerfaktorautentisering

Et enkelt passord gir kun svak beskyttelse av tilgangen; NIS-2-retningslinjen krever tilgangskontroll med multifaktorautentisering.

Transpareo tilbyr multifaktorautentisering for alle brukere av Application Manager – via Authenticator-appen, passnøkkel eller maskinvarenøkkel – inkludert reservekoder i tilfelle tap. Kravet om multifaktorautentisering kan aktiveres for din konto.

Kilde: NIS-2-direktivet (tilgangskontroll og multifaktorautentisering).

ISO 27001–sertifisert hosting i Tyskland

Hvor serverne står og hvordan datasenteret er sikret, avgjør den fysiske sikkerheten til dataene dine – og hvilken lovgivning de er underlagt.

Transpareo drifter sine tjenester på ISO 27001–sertifiserte servere i Tyskland, med strenge fysiske og organisatoriske sikkerhetstiltak. Med Tyskland som lokalisering er dataene dine dessuten fullt ut underlagt europeisk lovgivning.

Kilde: ISO/IEC 27001 (informasjonssikkerhetsstyring), sertifisert datasenter i Tyskland.

Tar leverandøren seg av EU-registreringen for deg?

Registrering i EU-registeret, inkludert innhenting av offisiell bekreftelse, er en gjentakende oppgave som en tjenesteleverandør kan ta seg av på dine vegne. Registerforordningen fastsetter dette uttrykkelig: En tjenesteleverandør kan utføre registreringen på vegne av deg, men det juridiske ansvaret ligger fortsatt hos den økonomiske aktøren.

Transpareo registrerer passene dine på dine vegne så snart EU offentliggjør det tekniske grensesnittet – du forblir den juridisk ansvarlige næringsaktøren, men slipper den operative arbeidsbelastningen. Inn-til grensesnittet er tilgjengelig, kan ingen tilby denne tjenesten; vi har allerede forberedt de nødvendige dataene for dette.

Kilde: Gjennomføringsforordning for DPP-registeret (utkast), art. 19: Registreringen kan utføres av en tjenesteleverandør på vegne av den økonomiske aktøren; ansvaret ligger fortsatt hos den økonomiske aktøren.

Tydelige regler for supportarbeid og supportkostnader

Noen leverandører skiller bruk fra support og fakturerer hjelp separat; i det store og hele gjør dette samarbeidet vanskelig å beregne kostnadene for.

Hos Transpareo er supporten en del av abonnementet – ingen separat supportavtale, ingen tilleggstermer som faktureres etter tidsforbruk. Alt du trenger av support er allerede inkludert i den oppgitte prisen.

Gjennomsiktig prisstruktur

En prisstruktur som først blir synlig under salgssamtalen, eller som beregnes i etterkant per språk, produkt og grensesnittkall, gjør de faktiske kostnadene uforutsigbare.

Transpareo publiserer fire prisplaner for alle bedriftsstørrelser åpent på nettstedet, med gratis prøveperiode og mulighet for oppsigelse når som helst. Det er ingen skjulte tilleggskostnader per språk, produkt eller grensesnittkall – den oppgitte prisen er den endelige prisen.