

Sammenligningsskema for DPP-udbydere

Kun allerede eksisterende, verificerbare funktioner markeres med et flueben - ingen løfter eller hensigtserklæringer. Kolonnen »Transpareo« er udfyldt på forhånd; de to tomme kolonner udfylder du, når du vurderer andre udbydere. Forklaringer og kilder til hvert kriterium finder du i slutningen af dokumentet.

Stand: 10.09.2026

Lovmæssigt obligatorisk

Kriterium	Transpareo		
Dataudveksling i et åbent, standardiseret format Passdataene er tilgængelige via åbne standarder - de kan læses af ethvert autoriseret system, ikke kun af en enkelt udbyders software. EN 18216	☒	☐	☐
Unik, bærbar identifikator uden tilknytning til en bestemt udbyder Produktkoden hører til produktet, ikke til platformen - ved skift af udbyder bevarer passet sin identitet. EN 18219	☒	☐	☐
Fysisk datamedie, der kan læses på lang sigt QR-koden på produktet fører til Pass i enhver browser - uden app, uden konto, med enhver smartphone. EN 18220	☒	☐	☐
Opbevaring og arkivering ud over den minimale løbetid Hver offentliggjort version forbliver tilgængelig i den lovbestemte periode - også ældre versioner, ikke kun den aktuelle. EN 18221	☒	☐	☐

Kriterium	Transpareo		
API til livscyklusstyring og søgefunktioner Et programmeringsgrænseflade læser, opretter og søger i pas - det er ikke blot en webgrænseflade, hvor man klikker sig frem. EN 18222	☒	☐	☐
Interoperabel datamodel Passoplysningerne følger en fælles model, som andre systemer kan læse uden at skulle omformatere dem. EN 18223	☒	☐	☐
Tre-trins model for adgangsrettigheder Offentlige, autoriserede og myndighedsrelaterede data er tydeligt adskilt - hver enkelt bruger ser kun det, som vedkommende har adgang til. EN 18239	☒	☐	☐
Påviselig dataautenticitet og -integritet Hver version er dobbeltsigneret og kan verificeres i browseren - uden at man behøver at stole på os, udelukkende på baggrund af dataene. EN 18246	☒	☐	☐
Forbindelse til EU-Kommissionens register Registrering inklusive officiel dokumentation - så snart EU offentliggør den tekniske grænseflade. Den er endnu ikke tilgængelig, og ingen udbyder kan i dag opfylde dette krav.	☐	☐	☐
Opbevaring af registreringsdata ud over den lovbestemte frist Et uændeligt tiårigt arkiv - hverken producenten eller Transpareo kan ændre en version efterfølgende.	☒	☐	☐
Produktoplysninger på de officielle sprog i hvert målmarked De obligatoriske oplysninger skal fremgå på de officielle sprog i hvert land, hvor produktet sælges - ved salg i hele EU altså på alle 24 officielle sprog, ikke kun på hjemmemarkedet.	☒	☐	☐

Anbefalet til drift af en DPP-database

Kriterium	Transpareo		
Sprog uden for EU 16 yderligere sprog ud over de 24 officielle EU-sprog - i alt 40 - til målmarkeder uden for Unionen.	☒	☐	☐
Versionsstyring og ændringshistorik Hver ændring genererer en ny, sporbar version med angivelse af tidspunkt og ophavsmand - gennem hele produktets livscyklus.	☒	☐	☐
Skalerbar masseproduktionsanlæg til produktfamilier Upload produktdata via Excel eller CSV og tilknyt dem til de obligatoriske felter - til store mængder findes der desuden en bulk-API.	☒	☐	☐
Rollebaseret intern rettighedsstyring Det er fastlagt, hvem i virksomheden der må vedligeholde eller frigive hvilke data - herunder strengt begrænsede, tidsbegrænsede adgangsrettigheder for eksterne.	☒	☐	☐
Opbevaring efter kontraktens udløb Hvis du opsiger dit medlemskab, forbliver dine offentliggjorte pass tilgængelige i det uændrelige tiårige arkiv.	☒	☐	☐
Signatur med egen kryptografisk nøgle Bring Your Own Key: Du opbevarer selv den private nøgle, vi tilføjer blot en uafhængig medunderskrift.	☒	☐	☐
Udstillerens identitet uafhængigt af platformen Din udstilleridentitet findes som DID:web på dit eget domæne, ikke på vores - et skift af udbyder bliver dermed til en DNS-flytning.	☒	☐	☐
Mulighed for tredjepartskontrol, helt uden udbyderen En open source-renderer kontrollerer hashværdier og signaturer i browseren - uden at kontakte en af vores servere.	☒	☐	☐

Ønskelige ekstrafunktioner

Kriterium	Transpareo		
Skift af udbyder uden tab af data Ved skiftet tager De hele pasbestanden med i åbne formater – signeret og med mulighed for selvkontrol; ved kontraktens udløb forbliver de obligatoriske pas tilgængelige i et uændret tiårigt arkiv uden tab af data.	☒	☐	☐
Integration med eksisterende systemer i stedet for en datø Signede webhooks og en bulk-API integrerer Pass med jeres systemer – der er ingen færdigudviklet konektor til et bestemt ERP-system.	☒	☐	☐
Batch-import og -eksport ud over de rene EU-krav Større datamængder kan flyttes i begge retninger – ikke kun de obligatoriske felter.	☒	☐	☐

Sikkerhed og databeskyttelse

Kriterium	Transpareo		
Separat database og egen nøgle Dine data opbevares i en separat database, krypteret med en egen nøgle – adskilt på både database- og krypteringsniveau.	☒	☐	☐
Kryptering og sikkerhedskopiering TLS for alle forbindelser, AES-kryptering af følsomme data og krypterede sikkerhedskopier med nøglerotation.	☒	☐	☐
Sikkerhedshændelseslog Loginforsøg, MFA-udfordringer og aktivitet vedrørende API-nøgler logges og opbevares i et år.	☒	☐	☐
Flerfaktorautentificering Autentificeringsapp, adgangsnøgle eller hardwarenøgle til alle brugere, med sikkerhedskoder i tilfælde af tab.	☒	☐	☐

Kriterium	Transpareo		
ISO 27001–certificeret hosting i Tyskland Server i Tyskland med strenge fysiske og organisatoriske sikkerhedsforanstaltninger.	☒	☐	☐

Økonomiske og organisatoriske spørgsmål

Kriterium	Transpareo		
Tager udbyderen sig af EU–registreringen for dig? Vi tager os af registreringen, herunder den officielle attest, så snart EU offentliggør grænsefladen – det kræver ingen indsats fra Deres side.	☒	☐	☐
Tydelige regler for supportindsats og supportomkostninger Supporten er inkluderet i prisen hos Transpareo – ingen separat supportaftale, ingen ekstra omkostninger.	☒	☐	☐
Gennemsigtig prisstruktur Fire offentlige prisplaner til virksomheder af alle størrelser, gratis prøveperiode, kan opsiges når som helst – uden skjulte ekstraomkostninger pr. sprog, produkt eller API-kald.	☒	☐	☐

Forklaringer og kilder

Dataudveksling i et åbent, standardiseret format **EN 18216**

Standarden kræver, at digitale produktpas skal være tilgængelige via åbne, standardiserede protokoller – så myndigheder, partnere og Deres egne systemer kan læse dataene uden at være bundet til en bestemt udbyders software. Et proprietært format ville være en ø: Uden udbyderen ville De ikke længere have adgang til Deres egne data. Standarden er siden den 15. juli 2026 offentliggjort i EU–Tidende (gennemførelsesafgørelse (EU) 2026/1736) og er dermed omfattet af formodningen om overensstemmelse med ESPR.

Transpareo leverer alle passdata og grænseflader via standard-HTTPS i struktureret, maskinlæsbar form – uden specialsoftware og uden proprietære protokoller. Hver offentliggjort version er desuden signeret, så en modtager ikke kun kan læse, men også kontrollere, at dataene er uændrede. Det, du ser

i brugergrænsefladen, er det samme datasæt, som ethvert autoriseret system henter via de åbne grænseflader.

Kilde: EN 18216, Krav til dataudvekslingsprotokoller: »Til standardiseret DPP-adgang skal de fastlagte dataudvekslingsprotokoller anvendes.«

Unik, bærbar identifikator uden tilknytning til en bestemt udbyder EN 18219

Hvert produktpas skal have en entydig identifikator, der permanent henviser til det samme produkt og ikke er afhængig af en bestemt udbyder. Hvis en udbyder knytter identifikatoren til sin egen infrastruktur, mister De identiteten af Deres pas, hvis De skifter udbyder – hver eneste udskrevne kode og hver eneste registrering vil da ikke længere have nogen betydning. Standarden er blevet offentliggjort i EU-Tidende den 15. juli 2026.

Transpareo tildeler identifikatoren som en GS1 Digital Link med jeres GTIN – en åben industristandard, der tilhører produktet, ikke platformen – og kontrollerer hver identifikator i forhold til de godkendte standardskemaer. Signaturidentiteten ligger som DID:web på jeres eget domæne, ikke på vores. Identifikatoren forbliver gyldig, selv hvis et system går ned: En permanent fallback-adresse løser den fortsat, og passet bevarer sin identitet uanset udbyderskift.

Kilde: EN 18219, afsnit 4.6.2(3): »Den entydige identifikator må ikke medføre en binding til en bestemt udbyder.«

Fysisk datamedie, der kan læses på lang sigt EN 18220

Passet skal være tilgængeligt via et maskinlæsbart datamedie på produktet, som alle kan få adgang til uden specialsoftware – og som forbliver læsbart gennem hele produktets levetid, også efter brug og reparation. Et datamedie, der kræver en bestemt app eller en konto, udelukker en del af offentligheden. Standarden er blevet offentliggjort i EU-Tidende den 15. juli 2026.

Transpareo genererer en QR-kode i henhold til ISO/IEC 18004, der indeholder en GS1 Digital Link-adresse og fører direkte til passet i enhver browser – ingen login, ingen download, på enhver smartphone. Model, batch og artikel er allerede indeholdt i den kodede adresse, så en scanning fører direkte til det rette niveau. Da adressen forbliver stabil via en permanent fallback-opløsning, forbliver en kode, der er udskrevet én gang, gyldig i hele produktets levetid.

Kilde: EN 18220, Krav til datamedier (afsnit 5): Symbolik, kodning, udskriftskvalitet og holdbarhed; datamediet skal forblive læsbart, selv efter flere brugs- og reparationscyklusser.

Opbevaring og arkivering ud over den minimale løbetid EN 18221

Standarden kræver, at en standard samt dens versionshistorik opbevares i den lovmæssigt foreskrevne periode og forbliver tilgængelig i uændret form. Hvis kun den aktuelle version opbevares, går sporbarheden af tidligere oplysninger tabt – og det er netop disse oplysninger, som en erhvervsaktør skal

kunne dokumentere over for myndighederne. Opbevaringsfristen afhænger af den pågældende sektorlovgivning, men er dog mindst ti år. Standarden er blevet offentliggjort i EU-Tidende siden den 15. juli 2026.

Transpareo gemmer hver offentliggørelse som en fastfrosset, signeret version i et uændeligt arkiv, hvor ingen senere kan ændre eller slette den – hverken du eller vi. Ældre versioner forbliver tilgængelige ved siden af den aktuelle, og hver version er forsynet med tidsstempel og signatur. På den måde kan det for ethvert tidspunkt dokumenteres, hvad passet viste på det pågældende tidspunkt.

Kilde: EN 18221: »Det digitale produktpas skal være tilgængeligt for autoriserede brugere i hele dets levetid.«

API til livscyklusstyring og søgefunktioner EN 18222

Ud over visningen i browseren kræver standarden en programmeringsgrænseflade, hvorigennem pas kan oprettes, læses, opdateres og søges på via produktidentifikatorer. Uden en sådan grænseflade forbliver al massebehandling manuelt arbejde, og andre systemer kan ikke automatisk udnytte pasbestanden. Standarden er blevet offentliggjort i EU-Tidende den 15. juli 2026.

Transpareo understøtter de foreskrevne standardmetoder via en versioneret, standardiseret grænseflade: Pas kan oprettes, læses, opdateres og gennemsøges side for side via produktkoder ved hjælp af et program. Det signerede pas leveres uændret – grænsefladen udleverer nøjagtigt de bytes, hvis signatur en kontrollør kan efterberegne.

Kilde: EN 18222: standardiseret programmeringsgrænseflade (API) til livscyklusstyring og søgefunktioner i DPP, som krævet i ESPR.

Interoperabel datamodel EN 18223

For at passene skal passe sammen på tværs af systemer og forsyningskæder, foreskriver standarden en fælles datamodel med ensartede definitioner af felterne. En leverandørspecifik model tvinger hver partner til at lave sin egen oversættelse – og hver oversættelse er en fejlkilde. Standarden er blevet offentliggjort i EU-Tidende den 15. juli 2026.

Transpareo bygger på et horisontalt vokabularlag med parallelle, anerkendte fagvokabularer (GS1, EPCIS og andre) og beskriver hvert datapunkt med henvisning til dets ordbog og datatype. Et modtagende system får dermed ikke kun at vide, hvad et felt hedder, men også hvad det betyder – passet forbliver læsbart uden omformatering.

Kilde: EN 18223: fælles semantisk datamodel for systeminteroperabilitet i DPP.

Tre-trins model for adgangsrettigheder EN 18239

Et produkt pas indeholder offentlige oplysninger, data til autoriserede erhvervsaktører og data, der udelukkende er beregnet til myndigheder; standarden kræver, at disse niveauer holdes adskilt og reguleres for hvert enkelt datafelt. Offentlige data skal være tilgængelige uden login, mens alt andet kun er tilgængeligt efter godkendelse. EN 18239 er i den afsluttende godkendelsesfase.

Transpareo implementerer synlighed som en egenskab for hvert datafelt: Det offentlige niveau leveres uden autentificering, de højere niveauer er beskyttet via en egen, protokolleret myndighedsgrænseflade med udelukkende læseadgang, og enhver adgang til beskyttede data registreres i auditloggen. Standardens tretrinsmodel er dermed allerede i dag afspejlet i arkitekturen og er ikke blot tilføjet efterfølgende.

Kilde: EN 18239 (udkast, i endelig godkendelse): »Adgang til offentlige data skal være mulig for aktører både inden for og uden for EU uden yderligere autentificering«; kontrollerede data kræver autentificeret og dokumenterbar adgang.

Påviselig dataautenticitet og -integritet EN 18246

Standarden kræver, at et pas' ægthed og integritet kan bevises, og at det skal være muligt at kontrollere det frit og uden begrænsninger. Tilliden må ikke afhænge af udbyderens fortsatte eksistens, men skal være knyttet til selve datasættet – ellers ville hvert pas kun være lige så troværdigt som det firma, der netop nu hoster det. EN 18246 er i den afsluttende godkendelsesfase.

Transpareo signerer hver offentliggjort version med to uafhængige nøgler (udsteder og Transpareo) og sammenkæder versionerne via deres hash, så historikken heller ikke kan omskrives ubemærket. En open source-renderer kontrollerer begge signaturer direkte i browseren uden at kontakte en af vores servere – det krævede signerede, selvkontrollerende bevis er dermed allerede implementeret.

Kilde: EN 18246 (udkast, i endelig godkendelsesfase): DPP-dataenes ægthed, pålidelighed og integritet skal kunne dokumenteres.

Forbindelse til EU-Kommissionens register

Alle pas, der er omfattet af registreringspligten, skal fremover være registreret i det centrale EU-register, som udsteder et permanent registrerings-ID og et officielt registreringsbevis. EU har endnu ikke offentliggjort den tekniske grænseflade hertil – derfor kan ingen udbyder i dag dokumentere denne tilkobling; hvis en udbyder hævder det, bør du spørge nærmere ind til det.

Transpareo har forberedt tilkoblingen så langt, som det er muligt uden grænsefladen: De nødvendige felter (registrerings-ID, stabil backup-adresse, versions-hash) er allerede oprettet i datamodellen. Så snart EU offentliggør grænsefladen, aktiverer vi registreringen, uden at du behøver at ændre dine pas. Indtil da forbliver dette punkt uafklaret – både hos os og hos enhver seriøs udbyder.

Kilde: Udkast til gennemførelsesforordning om DPP-registret (Ares(2026)4424976).

Opbevaring af registreringsdata ud over den lovbestemte frist

Registrerede pasdata skal forblive tilgængelige uændret ud over den lovbestemte frist – som regel ti år fra registreringen – selv i tilfælde af producentens konkurs eller ophør af virksomheden. Forpligtelsen gælder altså længere end både din kontrakt med en udbyder og udbyderen selv.

Transpareo opbevarer derfor et uændeligt arkiv, hvor en version, der først er gemt, ikke kan ændres eller slettes efterfølgende af nogen – hverken producenten eller os. Arkivet træder automatisk i kraft ved EU-registreringen. Og for at sikre, at det forbliver tilgængeligt, selv hvis Transpareo en dag ikke længere eksisterer, er dets fortsatte eksistens sikret gennem en notariel deponering i Schweiz.

Kilde: Gennemførelsesforordningen til DPP-registret, artikel 10, stk. 3 (opbevaring i ti år).

Produktoplysninger på de officielle sprog i hvert målmarked

De obligatoriske oplysninger på et pas skal foreligge på de officielle sprog i hver enkelt medlemsstat, hvor produktet markedsføres – ikke kun på sproget i det land, hvor producenten har hjemsted. Hvis man kun betjener hjemmemarkedet, opfylder man ikke kravet for alle andre målmarkeder.

Transpareo vedligeholder hvert pas på flere sprog og leverer det obligatoriske indhold på alle 24 officielle EU-sprog. I indtaster indholdet én gang; sprogversionerne genereres ud fra dette, uden at I skal betale ekstra pr. sprog eller vedligeholde separate pas. Passet er dermed læsbart i overensstemmelse med reglerne på hvert målmarked.

Kilde: Batteriforordningen (EU) 2023/1542: Oplysninger på de officielle sprog i de medlemsstater, hvor produktet markedsføres.

Sprog uden for EU

Ud over den lovmæssige forpligtelse er det en fordel, hvis et pas også dækker sprog uden for EU – til eksportmarkeder, internationale handelspartnere og forbrugere, der ikke taler et af Unionens officielle sprog.

Transpareo vedligeholder i alt 40 sprogversioner, herunder de 24 officielle EU-sprog. De indtaster indholdet én gang og udgiver det på ethvert ønsket sprog uden at skulle betale ekstra pr. sprog. Også brugergrænsefladen, hvor De vedligeholder Deres pas (Applikationsmanageren), er oversat til alle 40 sprog, og De kan indtaste oplysninger på ethvert af de tilgængelige sprog.

Versionsstyring og ændringshistorik

Et certifikat ændrer sig i løbet af produktets levetid; uden en fuldstændig versionshistorik kan man senere ikke dokumentere, hvilken version der var gældende på hvilket tidspunkt. Standarden kræver derfor, at alle ændringer af certifikatet arkiveres.

Transpareo gemmer hver udgivelse som en separat, signeret version og registrerer, hvem der har oprettet den, hvornår og med hvilke ændrede felter. På den måde kan alle oplysninger kontrolleres med tilbagevirkende kraft, og en senere rettelse overskriver ikke historikken, men fortsætter den.

Kilde: EN 18221: »Alle ændringer i det digitale produktpas skal arkiveres.«

Skalerbar masseproduktionsanlæg til produktfamilier

Hvis man fører mange lignende produkter, kan man ikke oprette hver enkelt produktprofil manuelt; et velfungerende system kræver en måde at registrere hele produktfamilier på én gang.

Med Transpareo kan du uploade produktdata via Excel eller CSV og tilknytte dem til de obligatoriske felter; til meget store mængder findes der desuden en bulk-API, der opretter produktkort programstyret. Dermed kan oprettelsen skales fra et dusin til titusinder af produktkort.

Rollebaseret intern rettighedsstyring

Det er ikke meningen, at alle i virksomheden skal have lov til at redigere eller godkende indholdet i hvert pas; standarden kræver en rollebaseret rettighedsstyring med logført adgang.

Transpareo tildeler rettigheder efter rolle og brugergruppe og logfører enhver ændring. Også eksterne parter som værksteder eller genvindingsvirksomheder får kun meget begrænset og tidsbegrænset adgang; myndighederne får adgang via en separat, udelukkende læseadgangsbaseret grænseflade, der markerer hver adgang i auditloggen.

Kilde: EN 18239 (udkast), Administration af adgangsrettigheder: fastlægger, hvilke aktører der må vedligeholde og frigive DPP-data.

Opbevaring efter kontraktens udløb

Opbevaringspligten ophører ikke med kontraktens udløb: Et registreret pas skal fortsat eksistere ud over den lovbestemte frist, selvom du forlader udbyderen. En udbyder, der deaktiverer pas ved opsigelse, efterlader dig med et compliance-problem.

Transpareo løser dette ved hjælp af det samme uforanderlige tiårige arkiv som registreringsdataene – efter en opsigelse leverer en permanent fallback-adresse fortsat pasene, og myndighedsgrænsefladen læser det samme datasæt fra arkivet efter aftalens ophør. Allerede udskrevne QR-koder forbliver gyldige.

Kilde: EN 18221: Arkivversioner gemmes også hos udbyderen af backup-tjenester.

Signatur med egen kryptografisk nøgle

Den, der er i besiddelse af den private signaturnøgle, kan udstede certifikater i udstederens navn; derfor er det sikrere, hvis udstederen selv opbevarer denne nøgle i stedet for at overlade den til

udbyderen.

Med »Bring Your Own Key« driver din virksomhed sin egen signaturendepunkt – Transpareo opbevarer aldrig den private nøgle og tilføjer kun en uafhængig modsignatur. På den måde bærer hver version to uafhængige signaturer, og din udsteder-signatur er en, som Transpareo ikke selv kan generere.

Udstillerens identitet uafhængigt af platformen

For at en verificator kan finde dine offentlige nøgler, skal certifikatet indeholde en offentliggjort udstederidentitet. Hvis denne findes på udbyderens domæne, binder den dig til udbyderen: Et skift ville gøre alle allerede udskrevne koder ugyldige.

Transpareo offentliggør din identitet som DID: på dit eget domæne, ikke på vores – et skift af udbyder bliver dermed blot en DNS-flytning, og allerede udskrevne koder samt deres verifikation forbliver gyldige. Derudover spejler vi hver offentlig nøgle på tidspunktet for offentliggørelsen til en permanent adresse, så hver version forbliver verificerbar, selvom den oprindelige host forsvinder.

Kilde: EN 18219, afsnit 4.2.2 (Varighed): Identifikatorer forbliver uændrede gennem hele livscyklussen; webdomæner kan overdrages eller omdirigeres.

Mulighed for tredjepartskontrol, helt uden udbyderen

Den afgørende test for tillid er, om en tredjepart kan kontrollere passet uden at benytte udbyderens infrastruktur. Standarden kræver, at kontrollen af gyldighed og integritet skal være gratis og ubegrænset for den, der foretager kontrollen.

Transpareo offentliggør til dette formål en open source-renderer, der indlæser bytes fra en version fra en vilkårlig kilde, genberegner hashværdien og kontrollerer begge signaturer mod de offentlige nøgler, der er angivet i passet – ingen login, intet opkald til os, ingen afhængighed af en kørende platform. Den, der er mistroisk, kan læse kildekoden.

Kilde: EN 18246 (udkast): »Kontrollen af DPP-dataenes gyldighed og integritet skal være mulig for kontrolløren uden omkostninger og uden begrænsninger.«

Skift af udbyder uden tab af data

En udbyder, der gør det vanskeligt at skifte, holder dig fast ved hjælp af dine egne data – og hvad der sker med dataene ved kontraktens udløb, afgør, om du frit kan skifte udbyder. Standarden kræver derfor, at dataene kan overføres via et åbent, interoperabelt netværk uden binding til en bestemt udbyder.

Transpareo gemmer de lovmæssige passartefakter fra starten i et åbent område, der kan spejles offentligt: En simpel synkronisering genererer en komplet, signeret kopi, der selv kontrollerer sig mod de offentliggjorte nøgler uden indgriben fra vores side. Vi leverer det komplette hændelsesarkiv via en signeret, tidsbegrænset download-adresse til dig eller din nye udbyder, og det overordnede produkt-katalog leveres desuden som JSON-LD og CSV. Ved kontraktens udløb forbliver de registrerede

obligatoriske pass-data tilgængelige via det uforanderlige tiårige arkiv: Den offentlige spejling og arkivet forbliver synkroniseret og videregiver den samme datamængde, allerede udskrevne QR-koder kan fortsat indløses via den permanente fallback-adresse, og registerhenvisningen peger på den nye adresse. På denne måde afsluttes kontrakten uden tab af data og uden at bryde de lovmæssige opbevaringskrav.

Kilde: EN 18216: Data skal kunne »overføres via et åbent, interoperabelt netværk uden leverandørbinding«.

Integration med eksisterende systemer i stedet for en datø

Et pass, der kun findes i udbyderens brugergrænseflade, bliver en dataø i forhold til dine øvrige systemer – hver ændring skal derfor opdateres to gange.

Transpareo rapporterer hændelser via signerede webhooks og gør det muligt at indlæse og udlæse data via en bulk-API, så du kan integrere Passet i dit eget systemlandskab. Vi leverer bevidst ikke en færdiglavet konektor til et bestemt ERP-system – de åbne, signerede grænseflader passer til ethvert system i stedet for at favorisere ét bestemt.

Batch-import og -eksport ud over de rene EU-krav

Hvis man ønsker at anvende de indsamlede data også uden for Pass-systemet, er det nødvendigt med import- og eksportfunktioner, der dækker mere end blot de lovpligtige felter.

Transpareo modtager større datamængder via Excel, CSV og Bulk-API og udleverer dem i samme omfang. På den måde tjener systemet ikke kun til at opfylde EU-kravene, men også til din egen datahåndtering.

Separat database og egen nøgle

I en delt database er dine data sammenkædet med andre kunders data; en klar og dokumenterbar adskillelse er i så fald næsten umulig – og retten til sletning i henhold til artikel 17 i GDPR er svær at dokumentere.

Hos Transpareo ligger hver kunde i sin egen database, krypteret med sin egen nøgle – adskillelsen findes både på database- og krypteringsniveau. Dette opfylder retten til sletning gennem verificerbar sletning; hosting foregår i Tyskland, og databehandleraftalen (AVV) er inkluderet.

Kilde: GDPR, artikel 17 (ret til sletning), opfyldt gennem en separat database, egen nøgle og verificerbar sletning.

Kryptering og sikkerhedskopiering

En udbyder skal beskytte data under overførsel og i hvile og sikre dem mod nedbrud; GDPR kræver i den forbindelse foranstaltninger, der er i overensstemmelse med den aktuelle tekniske udvikling.

Transpareo krypterer alle forbindelser med TLS og følsomme applikationsdata med AES. Sikkerhedskopierne er GPG-krypterede, opdateres med regelmæssig nøglerotation, oprettes hver fjerde time og opbevares i tolv måneder på en separat server.

Kilde: GDPR, artikel 32 (sikkerhed i forbindelse med databehandlingen): TLS, AES og krypterede sikkerhedskopier med rotationsordning.

Sikkerhedshændelseslog

Sikkerhedsrelevante hændelser skal kunne spores – hvem der har logget ind, hvornår det skete, og hvordan nøglerne blev brugt. NIS-2-direktivet kræver, at der føres relevante revisionslogfiler.

Transpareo fører en sikkerhedshændelseslog over loginforsøg, MFA-udfordringer og API-nøgleaktivitet og opbevarer den i et år. Dermed opfyldes NIS-2-kravene til auditlogs.

Kilde: NIS 2-direktivet (krav til revisionslogfiler): registrerede sikkerhedshændelser, opbevaring i et år.

Flerfaktorautentificering

En enkelt adgangskode giver kun ringe beskyttelse af adgangen; NIS-2-direktivet kræver adgangskontrol med multifaktor-autentificering.

Transpareo tilbyder multifaktor-autentificering til alle brugere af Applikations-Manager – via Authenticator-app, passkey eller hardwarenøgle – inklusive backup-koder i tilfælde af tab. Kravet om multifaktor-autentificering kan gøres obligatorisk for din konto.

Kilde: NIS 2-direktivet (adgangskontrol og multifaktor-autentificering).

ISO 27001-certificeret hosting i Tyskland

Hvor serverne er placeret, og hvordan datacentret er sikret, er afgørende for den fysiske sikkerhed af dine data – og for, hvilken lovgivning de er underlagt.

Transpareo hoster på ISO 27001-certificerede servere i Tyskland med strenge fysiske og organisatoriske sikkerhedsforanstaltninger. Placeringen i Tyskland betyder desuden, at dine data fuldt ud er underlagt europæisk lovgivning.

Kilde: ISO/IEC 27001 (informationssikkerhedsstyring), certificeret datacenter i Tyskland.

Tager udbyderen sig af EU-registreringen for dig?

Registreringen i EU-registret samt indhentning af det officielle bevis er en tilbagevendende opgave, som en udbyder kan varetage for Dem. Registerforordningen fastsætter dette udtrykkeligt: En tjenesteudbyder må varetage registreringen på Deres vegne, men det juridiske ansvar forbliver hos den økonomiske aktør.

Transpareo registrerer dine certifikater på dine vegne, så snart EU offentliggør den tekniske grænseflade – du forbliver den juridisk ansvarlige erhvervsaktør, men bærer ikke den operationelle byrde. Indtil grænsefladen er tilgængelig, kan ingen levere denne tjeneste; vi har allerede forberedt de nødvendige data hertil.

Kilde: Gennemførelsesforordning om DPP-registret (udkast), artikel 19: Registreringen kan foretages af en tjenesteudbyder på vegne af den økonomiske aktør; ansvaret påhviler dog fortsat den økonomiske aktør.

Tydelige regler for supportindsats og supportomkostninger

Nogle udbydere adskiller brugen fra supporten og fakturerer hjælp separat; alt i alt gør det samarbejdet svært at beregne omkostningerne for.

Hos Transpareo er supporten en del af abonnementsprisen – ingen separat supportaftale, ingen ekstra timer, der faktureres efter tidsforbrug. Alt den support, du har brug for, er allerede inkluderet i den angivne pris.

Gennemsigtig prisstruktur

En prisstruktur, der først bliver synlig under salgssamtalen eller beregnes efter hvert sprog, produkt og grænsefladeopkald, gør de faktiske omkostninger uforudsigelige.

Transpareo offentliggør åbent fire prisplaner for alle virksomhedsstørrelser på sin hjemmeside, med en gratis prøveperiode og mulighed for opsigelse når som helst. Der er ingen skjulte ekstraomkostninger pr. sprog, produkt eller grænsefladeopkald – den angivne pris er den pris, du betaler.