

Jämförelsetabell för DPP-leverantörer

Endast befintliga, verifierbara funktioner markeras med en bock – inga tillkännagivanden eller avsiktsförklaringar. Kolumnen "Transpareo" är ifylld i förväg; de två tomma kolumnerna fyller du i när du granskar andra leverantörer. Förklaringar och källor till varje kriterium finns i slutet av dokumentet.

Senaste uppdatering: 10.09.2026

Lagligt obligatoriskt

Kriterium	Transpareo		
Datautbyte i ett öppet, standardiserat format Passdata är tillgängliga via öppna standarder – de kan läsas av alla behöriga system, inte bara av en enskild leverantörs programvara. EN 18216	☒	☐	☐
Unikt, portabelt identifieringsnummer utan bindning till någon leverantör Produktens identifieringskod hör till produkten, inte till plattformen – vid byte av leverantör behåller passet sin identitet. EN 18219	☒	☐	☐
Fysisk datamedie, som kan läsas på lång sikt QR-koden på produkten leder till passet i vilken webbläsare som helst – utan app, utan konto, med vilken smartphone som helst. EN 18220	☒	☐	☐
Lagring och arkivering under den minimala giltighetstiden Varje publicerad version förblir tillgänglig under den tidsperiod som föreskrivs i lag – även äldre versioner, inte bara den aktuella. EN 18221	☒	☐	☐

Kriterium	Transpareo		
API för livscykelhantering och sökbarhet Ett programmeringsgränssnitt läser in, skapar och söker igenom pass - det är inte bara ett webbgränssnitt där man klickar. EN 18222	☒	☐	☐
Interoperabel datamodell Passuppgifterna följer en gemensam modell som andra system kan läsa utan att behöva omformatera dem. EN 18223	☒	☐	☐
En åtkomsträttsmodell i tre nivåer Offentliga, auktoriserade och myndighetsrelaterade uppgifter är tydligt åtskilda - var och en ser exakt det som hen har behörighet till. EN 18239	☒	☐	☐
Verifierbar dataautenticitet och integritet Varje version är dubbelsignerad och kan verifieras i webbläsaren - utan att man behöver lita på oss, enbart utifrån uppgifterna. EN 18246	☒	☐	☐
Anslutning till EU-kommissionens register Registrering inklusive officiellt intyg - så snart EU offentliggör det tekniska gränssnittet. Det finns ännu inte tillgängligt, vilket innebär att ingen leverantör kan uppfylla detta krav i dagsläget.	☐	☐	☐
Lagring av registreringsuppgifterna utöver den lagstadgade tidsfristen Ett oföränderligt tioårigt arkiv - varken tillverkaren eller Transpareo kan ändra en version i efterhand.	☒	☐	☐
Produktinformation på de officiella språken på varje målmarknad Den obligatoriska informationen ska anges på de officiella språken i varje land där produkten säljs - vid försäljning inom hela EU innebär detta alltså på alla 24 officiella språk, inte bara på hemmamarknaden.	☒	☐	☐

Användbart för drift av en DPP-databas

Kriterium	Transpareo		
Språk utanför EU 16 ytterligare språk utöver EU:s 24 officiella språk - totalt 40, för målmarknader utanför unionen.	☒	☐	☐
Versionshantering och ändringshistorik Varje ändring genererar en ny, spårbar version med tidpunkt och upphovsman - under hela produktens livscykel.	☒	☐	☐
Skalbar massproduktionsanläggning för produktfamiljer Ladda upp produktdata via Excel eller CSV och koppla dem till de obligatoriska fälten - för stora volymer finns dessutom ett Bulk-API.	☒	☐	☐
Rollbaserad intern behörighetshantering Det finns regler för vem inom företaget som får hantera eller dela vilka uppgifter - inklusive strikt begränsade, tidsbegränsade åtkomsträttigheter för externa personer.	☒	☐	☐
Förvaring efter avtalets utgång Om du säger upp ditt medlemskap förblir dina publicerade pass tillgängliga i det oföränderliga tioåriga arkivet.	☒	☐	☐
Signatur med egen kryptografisk nyckel Bring Your Own Key: Ni förvarar den privata nyckeln själva, vi lägger bara till en oberoende medsignatur.	☒	☐	☐
Utställarens identitet är oberoende av plattformen Din utställaridentitet finns som DID:webb på din egen domän, inte på vår - ett byte av leverantör innebär en DNS-flytt.	☒	☐	☐
Möjlighet för tredje part att granska, helt utan leverantörens inblandning En renderare med öppen källkod kontrollerar hashvärden och signaturer direkt i webbläsaren - utan att kontakta någon av våra servrar.	☒	☐	☐

Önskvärda tilläggsfunktioner

Kriterium	Transpareo		
Byta leverantör utan att förlora data Vid bytet tar ni med er hela passbeståndet i öppna format – signerade och självkontrollerade; när avtalet löper ut förblir de obligatoriska passen tillgängliga i ett oföränderligt tioårigt arkiv, utan dataförlust.	☒	☐	☐
Integration med befintliga system istället för dataskator Signerade webhooks och ett bulk-API kopplar samman Pass med era system – det finns ingen färdig koppling för ett specifikt ERP-system.	☒	☐	☐
Batchimport och –export utöver de rena EU-kraven Större datamängder kan flyttas i båda riktningarna – inte bara de obligatoriska fälten.	☒	☐	☐

Säkerhet och integritet

Kriterium	Transpareo		
Separat databas och egen nyckel Dina uppgifter lagras i en egen databas, krypterade med en egen nyckel – separat på databas- och krypteringsnivå.	☒	☐	☐
Kryptering och säkerhetskopiering TLS för alla anslutningar, AES-kryptering av känsliga data och krypterade säkerhetskopior med nyckelrotation.	☒	☐	☐
Säkerheshändelseprotokoll Inloggningsförsök, MFA-utmaningar och aktivitet kopplad till API-nycklar loggas och sparas i ett år.	☒	☐	☐
Flerfaktorautentisering Autentiseringsapp, passnyckel eller hårdvarunyckel för alla användare, med reservkoder om nyckeln skulle gå förlorad.	☒	☐	☐

Kriterium	Transpareo	_____	_____
ISO 27001–certifierad webbhotellstjänst i Tyskland Server i Tyskland med strikta fysiska och organisatoriska säkerhetsåtgärder.	☒	☐	☐

Ekonomiska och organisatoriska frågor

Kriterium	Transpareo	_____	_____
Sköter leverantören EU-registreringen åt dig? Vi sköter registreringen inklusive det officiella intyget så snart EU offentliggör gränssnittet – det innebär ingen extra arbetsbörda för er.	☒	☐	☐
Tydliga regler för supportinsatser och supportkostnader Support ingår i priset hos Transpareo – inget separat supportavtal, inga extra kostnader.	☒	☐	☐
Transparent prisstruktur Fyra offentliga prisplaner för företag av alla storlekar, kostnadsfri provperiod, kan sägas upp när som helst – utan dolda tilläggskostnader per språk, produkt eller API-anrop.	☒	☐	☐

Förklaringar och källor

Datautbyte i ett öppet, standardiserat format **EN 18216**

Standarden kräver att digitala produktpass ska vara tillgängliga via öppna, standardiserade protokoll – så att myndigheter, samarbetspartner och era egna system kan läsa uppgifterna utan att vara bundna till en viss leverantörs programvara. Ett proprietärt format skulle utgöra en isolerad ö: utan leverantören skulle ni inte längre kunna komma åt era egna uppgifter. Standarden har varit publicerad i EU:s officiella tidning sedan den 15 juli 2026 (genomförandebeslut (EU) 2026/1736) och omfattas därmed av presumptionen om överensstämmelse med ESPR.

Transpareo levererar alla passdata och gränssnitt via standard-HTTPS i strukturerad, maskinläsbar form – utan specialprogramvara, utan proprietära protokoll. Varje publicerad version är dessutom signerad,

så att mottagaren inte bara kan läsa utan också kontrollera att uppgifterna är oförändrade. Det du ser i gränssnittet är samma datamängd som varje behörigt system hämtar via de öppna gränssnitten.

Källa: EN 18216, Krav på datautbytesprotokoll: "För standardiserad DPP-åtkomst ska de fastställda datautbytesprotokollen användas."

Unikt, portabelt identifieringsnummer utan bindning till någon leverantör EN 18219

Varje produktpass måste ha en unik identifierare som permanent hänvisar till samma produkt och inte är bunden till någon leverantör. Om en leverantör kopplar identifieraren till sin egen infrastruktur förlorar ni identiteten på era pass vid ett byte – varje utskriven kod och varje registrering skulle då vara meningslös. Standarden har varit publicerad i EU:s officiella tidning sedan den 15 juli 2026.

Transpareo tilldelar identifieraren som en GS1 Digital Link med ditt GTIN – en öppen branschstandard som tillhör produkten, inte plattformen – och kontrollerar varje identifierare mot de godkända standardschemana. Signaturidentiteten finns som DID:web på din egen domän, inte på vår. Identifieraren förblir giltig även om ett system slutar fungera: en permanent reservadress fortsätter att lösa den, och passet behåller sin identitet oavsett leverantörsbyte.

Källa: EN 18219, avsnitt 4.6.2(3): "Den unika identifieraren får inte leda till en bindning till en leverantör."

Fysisk datamedie, som kan läsas på lång sikt EN 18220

Passet måste vara tillgängligt via ett maskinläsbart datamedium på produkten, som vem som helst kan komma åt utan specialprogramvara – och som förblir läsbart under hela produktens livslängd, även efter användning och reparation. Ett datamedium som kräver en viss app eller ett konto utestänger en del av allmänheten. Standarden har varit publicerad i EU:s officiella tidning sedan den 15 juli 2026.

Transpareo genererar en QR-kod enligt ISO/IEC 18004 som innehåller en GS1 Digital Link-adress och som i vilken webbläsare som helst leder direkt till passet – ingen inloggning, ingen nedladdning, fungerar på alla smartphones. Modell, sats och artikel finns redan i den kodade adressen, så att en skanning direkt hamnar på rätt nivå. Eftersom adressen förblir stabil tack vare en permanent fallback-upplösning förblir en kod som en gång har skrivits ut giltig under hela produktens livslängd.

Källa: EN 18220, Krav på datamedier (avsnitt 5): Symbolik, kodning, tryckkvalitet och hållbarhet; datamediet ska förbli läsbart även efter flera användnings- och reparationscykler.

Lagring och arkivering under den minimala giltighetstiden EN 18221

Standarden kräver att en standard, inklusive dess versionshistorik, lagras under den tidsperiod som föreskrivs i lagstiftningen och förblir tillgänglig i oförändrat skick. Om endast den aktuella versionen bevaras går spårbarheten för tidigare uppgifter förlorad – och det är just detta som en ekonomisk aktör

måste kunna styrka gentemot myndigheterna. Bevarandeperioden styrs av den aktuella sektorslagstiftningen, men är minst tio år. Standarden har citerats i EU:s officiella tidning sedan den 15 juli 2026.

Transpareo sparar varje publicering som en låst, signerad version i ett oföränderligt arkiv, där ingen senare kan ändra eller radera den – varken du eller vi. Äldre versioner förblir tillgängliga vid sidan av den aktuella, och varje version är försedd med tidsstämpel och signatur. På så sätt går det att för varje tidpunkt styrka vad passet visade vid den tidpunkten.

Källa: EN 18221: "Det digitala produktpasset ska hållas tillgängligt för behöriga användare under hela dess livslängd."

API för livscykelhantering och sökbarhet EN 18222

Förutom visningen i webbläsaren kräver standarden ett programmeringsgränssnitt genom vilket pass kan skapas, läsas, uppdateras och sökas fram med hjälp av produktidentifierare. Utan ett sådant gränssnitt måste all massbehandling ske manuellt, och andra system kan inte utnyttja passregistret automatiskt. Standarden har varit publicerad i EU:s officiella tidning sedan den 15 juli 2026.

Transpareo stödjer de föreskrivna standardmetoderna via ett versionshanterat, standardiserat gränssnitt: Pass kan skapas, läsas, uppdateras och sökas igenom sida för sida med hjälp av produktkoderna på ett programstyrt sätt. Det signerade passet levereras oförändrat – gränssnittet lämnar ut exakt de byte vars signatur en granskare kan verifiera.

Källa: EN 18222: standardiserat programmeringsgränssnitt (API) för livscykelhantering och sökbarhet i DPP, i enlighet med kraven i ESPR.

Interoperabel datamodell EN 18223

För att pass ska vara kompatibla mellan olika system och genom hela leveranskedjan föreskriver standarden en gemensam datamodell med enhetliga definitioner av fälten. En leverantörsspecifik modell tvingar varje partner att göra en egen översättning – och varje översättning är en felkälla. Standarden har citerats i EU:s officiella tidning sedan den 15 juli 2026.

Transpareo bygger på ett horisontellt vokabulärlager med parallella, erkända fackvokabulärer (GS1, EPCIS och andra) och beskriver varje datapunkt med hänvisning till dess ordbok och datatyp. Ett mottagande system får därmed inte bara reda på vad ett fält heter, utan också vad det betyder – passet förblir läsbart utan omformatering.

Källa: EN 18223: gemensam semantisk datamodell för systeminteroperabilitet inom DPP.

En åtkomsträttsmodell i tre nivåer EN 18239

Ett produktpass innehåller offentliga uppgifter, data för auktoriserade aktörer på marknaden och data som endast är avsedda för myndigheter; standarden kräver att dessa nivåer hålls åtskilda och regleras

per datafält. Offentliga data måste vara tillgängliga utan inloggning, medan all övrig information endast är tillgänglig efter verifiering. EN 18239 befinner sig i slutfasen av godkännandeprocessen.

Transpareo hanterar synligheten som en egenskap för varje datafält: den offentliga nivån tillhandahålls utan autentisering, de högre nivåerna skyddas via ett eget, loggat myndighetsgränssnitt med uteslutande läsbehörighet, och varje åtkomst till skyddade uppgifter registreras i revisionsloggen. Standardens trestegsmodell återspeglas därmed redan idag i arkitekturen, och har inte lagts till i efterhand.

Källa: EN 18239 (utkast, i slutfasen av godkännandet): "Tillgång till offentliga data måste vara möjlig för aktörer inom och utanför EU utan ytterligare autentisering"; kontrollerade data kräver autentiserad och verifierbar åtkomst.

Verifierbar dataautenticitet och integritet EN 18246

Standarden kräver att ett pass äkthet och integritet kan verifieras och att kontrollen kan utföras fritt och utan begränsningar. Förtroendet får inte vara beroende av leverantörens fortbestånd, utan måste vara knutet till själva datamängden – annars skulle varje pass endast vara lika trovärdigt som det företag som för tillfället lagrar det. EN 18246 befinner sig i slutfasen av godkännandeprocessen.

Transpareo signerar varje publicerad version med två oberoende nycklar (utfärdare och Transpareo) och länkar samman versionerna via deras hash, så att inte heller historiken kan ändras utan att det märks. En öppen källkodsrenderare verifierar båda signaturerna direkt i webbläsaren utan att kontakta någon av våra servrar – det krävda signerade, självverifierbara beviset är därmed redan implementerat.

Källa: EN 18246 (utkast, i slutfasen av godkännandet): Äktheten, tillförlitligheten och integriteten hos DPP-uppgifterna måste kunna styrkas.

Anslutning till EU-kommissionens register

Alla pass som omfattas av registreringskravet måste i framtiden registreras i EU:s centrala register, som utfärdar ett permanent registrerings-ID och ett officiellt registreringsbevis. EU har ännu inte offentliggjort det tekniska gränssnittet för detta – därför kan ingen leverantör i dagsläget styrka att de har denna anslutning; om en leverantör hävdar detta bör du ställa frågor.

Transpareo har förberett anslutningen så långt det är möjligt utan gränssnittet: De nödvändiga fälten (registrerings-ID, stabil backup-adress, versionshash) finns redan skapade i datamodellen. Så snart EU offentliggör gränssnittet aktiverar vi registreringen utan att du behöver ändra dina pass. Fram till dess förblir denna punkt öppen – hos oss liksom hos alla seriösa leverantörer.

Källa: Utkast till genomförandeförordning om DPP-registret (Ares(2026)4424976).

Lagring av registreringsuppgifterna utöver den lagstadgade tidsfristen

Registrerade passuppgifter måste förbli tillgängliga utan ändringar under den lagstadgade tidsfristen – vanligtvis tio år från registreringen – även vid tillverkarens konkurs eller nedläggning av verksamheten.

Skyldigheten gäller alltså längre än både ditt avtal med en leverantör och leverantören själv.

Transpareo förvarar därför uppgifterna i ett oföränderligt arkiv, där ingen – varken tillverkaren eller vi – i efterhand kan ändra eller radera en version som en gång har lagts in. Arkivet aktiveras automatiskt i samband med EU-registreringen. Och för att det ska förbli tillgängligt även om Transpareo en dag skulle upphöra att existera, säkerställs dess fortbestånd genom en notariell deponering i Schweiz.

Källa: Förordningen om tillämpning av DPP-registret, artikel 10.3 (bevarande i tio år).

Produktinformation på de officiella språken på varje målmarknad

De obligatoriska uppgifterna i ett pass måste finnas på de officiella språken i varje medlemsstat där produkten släpps ut på marknaden – inte bara på språket i det land där tillverkaren har sitt säte. Den som endast riktar sig till hemmamarknaden uppfyller inte kraven för alla andra målmarknader.

Transpareo hanterar varje pass på flera språk och levererar det obligatoriska innehållet på alla 24 officiella EU-språk. Ni matar in innehållet en gång; språkversionerna skapas automatiskt utan att ni behöver betala extra per språk eller hantera separata pass. Passet är därmed läsbart och uppfyller gällande regler på varje målmarknad.

Källa: Batteriförordningen (EU) 2023/1542: Uppgifter på de officiella språken i de medlemsstater där produkten släpps ut på marknaden.

Språk utanför EU

Utöver den lagstadgade skyldigheten är det en fördel om ett pass även omfattar språk utanför EU – för exportmarknader, internationella handelspartner och konsumenter som inte talar något av unionens officiella språk.

Transpareo underhåller totalt 40 språkversioner, inklusive de 24 officiella EU-språken. Ni matar in innehållet en gång och kan sedan visa det på vilket språk ni vill, utan att behöva betala extra per språk. Även gränssnittet där ni hanterar era pass (Applikationshanteraren) är översatt till alla 40 språk, och ni kan mata in information på vilket som helst av de tillgängliga språken.

Versionshantering och ändringshistorik

Ett pass förändras under produktens livslängd; utan en fullständig versionshistorik går det inte att senare styrka vilken version som gällde vid vilken tidpunkt. Standarden kräver därför att alla ändringar av passet arkiveras.

Transpareo spärrar varje publicering som en egen, signerad version och registrerar vem som skapade den, när och med vilka ändrade fält. På så sätt förblir varje uppgift retroaktivt verifierbar, och en senare korrigering skriver inte över historiken utan fortsätter den.

Källa: EN 18221: "Alla ändringar i det digitala produktpasset ska arkiveras."

Skalbar massproduktionsanläggning för produktfamiljer

Den som hanterar många liknande produkter kan inte skapa varje produktkort manuellt ett och ett; ett hållbart system kräver ett sätt att registrera hela produktfamiljer på en gång.

Med Transpareo kan du ladda upp produktdata via Excel eller CSV och koppla dem till de obligatoriska fälten; för mycket stora volymer finns dessutom ett bulk-API tillgängligt som skapar produktkort programstyrt. På så sätt kan systemet skala från ett dussin till tiotusentals produktkort.

Rollbaserad intern behörighetshantering

Det är inte meningen att alla inom företaget ska kunna redigera eller godkänna allt innehåll i passet; standarden kräver en rollbaserad behörighetshantering med loggförda åtkomsthändelser.

Transpareo tilldelar behörigheter per roll och användargrupp och loggar varje ändring. Även externa aktörer, såsom verkstäder eller återvinningsföretag, får endast mycket begränsad och tidsbegränsad åtkomst; myndigheter får åtkomst via ett separat gränssnitt med enbart läsbehörighet, som markerar varje åtkomst i revisionsloggen.

Källa: EN 18239 (utkast), Hantering av åtkomsträttigheter: reglerar vilka aktörer som får underhålla och dela DPP-data.

Förvaring efter avtalets utgång

Bevaringsskyldigheten upphör inte i och med att avtalet upphör: Ett registrerat pass måste finnas kvar längre än den lagstadgade tidsfristen, även om du lämnar leverantören. En leverantör som inaktiverar pass vid uppsägning lämnar ett efterlevnadsproblem åt dig.

Transpareo hanterar detta genom samma oföränderliga tioåriga arkiv som registreringsuppgifterna - efter en uppsägning levererar en permanent reservadress passet vidare, och myndighetsgränssnittet läser samma datapost från arkivet efter avtalets upphörande. Redan utskrivna QR-koder förblir giltiga.

Källa: EN 18221: Arkivversioner lagras även hos leverantören av säkerhetskopieringstjänster.

Signatur med egen kryptografisk nyckel

Den som innehar den privata signaturnyckeln kan skapa pass i utfärdarens namn; därför är det säkrare om utfärdaren själv behåller denna nyckel istället för att anförtro den till leverantören.

Med Bring Your Own Key driver ert företag en egen signaturterminal - Transpareo förvarar aldrig den privata nyckeln och lägger endast till en oberoende motsignatur. På så sätt har varje version två oberoende signaturer, och er utfärdarsignatur är en som Transpareo inte själv kan skapa.

Utställarens identitet är oberoende av plattformen

För att en granskare ska kunna hitta dina offentliga nycklar måste passet ha en publicerad utfärdaridentitet. Om denna finns på leverantörens domän binder den dig till denne: ett byte skulle göra alla redan utskrivna koder ogiltiga.

Transpareo publicerar din identitet som DID: på webben på din egen domän, inte på vår – ett byte av leverantör blir därmed en DNS-flytt, och redan utskrivna koder samt deras verifiering förblir giltiga. Dessutom speglar vi varje offentlig nyckel vid tidpunkten för publiceringen till en permanent adress, så att varje version förblir verifierbar, även om den ursprungliga värden försvinner.

Källa: EN 18219, avsnitt 4.2.2 (Beständighet): Identifierare kvarstår under hela livscykeln; webbdomäner kan överlåtas eller omdirigeras.

Möjlighet för tredje part att granska, helt utan leverantörens inblandning

Det avgörande testet för förtroende är om en tredje part kan verifiera passet utan att använda leverantörens infrastruktur. Standarden kräver att kontrollen av giltighet och integritet ska vara kostnadsfri för den som utför kontrollen och kunna genomföras utan begränsningar.

Transpareo publicerar därför en öppen källkodsbasead renderare som laddar in byten från en version från valfri källa, beräknar hashvärdet på nytt och kontrollerar båda signaturerna mot de offentliga nycklarna som anges i passet – ingen inloggning, inget samtal till oss, inget beroende av en igångvarande plattform. Den som är misstänksam kan läsa källkoden.

Källa: EN 18246 (utkast): "Kontrollen av DPP-uppgifternas giltighet och integritet måste kunna utföras av kontrollanten utan kostnad och utan begränsningar."

Byta leverantör utan att förlora data

En leverantör som försvårar bytet håller dig bunden till dina egna data – och vad som händer med uppgifterna när avtalet löper ut avgör om du fritt kan byta leverantör. Standarden kräver därför att uppgifterna ska kunna överföras via ett öppet, interoperabelt nätverk utan bindning till någon leverantör.

Transpareo lagrar från början de regleringsmässiga passartefakterna i ett öppet område som kan speglas offentligt: En enkel synkronisering skapar en fullständig, signerad kopia som själv kontrollerar mot de publicerade nycklarna, utan någon inblandning från vår sida. Vi tillhandahåller det fullständiga händelsearkivet via en signerad, tidsbegränsad nedladdningsadress till dig eller din nya leverantör, och den tidigare produktkatalogen dessutom i formatet JSON-LD och CSV. När avtalet löper ut förblir de registrerade obligatoriska uppgifterna tillgängliga via det oföränderliga tioåriga arkivet: Den offentliga speglingen och arkivet förblir synkroniserade och överför samma datamängd, redan utskrivna QR-koder kan fortfarande lösas in via den permanenta fallback-adressen, och registerhänvisningen pekar på den nya adressen. På så sätt avslutas avtalet utan dataförlust och utan att de lagstadgade arkiveringskraven bryts.

Källa: EN 18216: Data måste kunna "överföras via ett öppet, interoperabelt nätverk utan leverantörsberoende".

Integration med befintliga system istället för dataskator

Ett pass som endast finns i leverantörens gränssnitt blir en dataö i förhållande till era övriga system – varje ändring måste då uppdateras två gånger.

Transpareo rapporterar händelser via signerade webhooks och gör det möjligt att läsa in och läsa ut data via ett bulk-API, så att du kan integrera passet med din egen systemmiljö. Vi tillhandahåller medvetet ingen färdigkoppling för ett specifikt ERP-system – de öppna, signerade gränssnitten passar alla system, istället för att gynna ett enda.

Batchimport och –export utöver de rena EU-kraven

Den som vill använda de insamlade uppgifterna även utanför passet behöver import- och exportfunktioner för mer än bara de lagstadgade obligatoriska fälten.

Transpareo tar emot större datamängder via Excel, CSV och Bulk-API och exporterar dem i samma omfattning. På så sätt uppfyller systemet inte bara EU:s krav, utan underlättar även er egen datahantering.

Separat databas och egen nyckel

I en delad databas är dina uppgifter kopplade till andra kunders uppgifter; en tydlig och verifierbar åtskillnad är då knappast möjlig – och rätten till radering enligt artikel 17 i GDPR är svår att styrka.

Hos Transparero finns varje kund i en egen databas, krypterad med en egen nyckel – åtskillnaden sker både på databas- och krypteringsnivå. Detta uppfyller rätten till radering genom verifierbar radering; serverutrymmet finns i Tyskland och avtalet om uppdragshantering (AVV) ingår.

Källa: GDPR artikel 17 (rätten till radering), uppfylls genom en separat databas, egen nyckel och verifierbar radering.

Kryptering och säkerhetskopiering

En leverantör måste skydda data både under överföring och i viloläge samt säkerställa att de skyddas mot driftstopp; GDPR kräver att åtgärder i enlighet med den senaste tekniken vidtas för detta.

Transpareo krypterar alla anslutningar med TLS och känsliga applikationsdata med AES. Säkerhetskopiorna är GPG-krypterade, förnyas med regelbunden nyckelrotation, skapas var fjärde timme och lagras i tolv månader på en separat server.

Källa: GDPR artikel 32 (säkerhet vid behandling): TLS, AES och krypterade säkerhetskopior med rotationsschema.

Säkerhetshändelseprotokoll

Säkerhetsrelaterade händelser måste kunna spåras – vem som har loggat in, när detta skedde och hur nycklarna har använts. NIS-2-direktivet kräver motsvarande revisionsloggar.

Transpareo för en säkerhetshändelselogg över inloggningsförsök, MFA-utmaningar och API-nyckelaktivitet och sparar den i ett år. Därmed uppfylls NIS 2-kraven på revisionsloggar.

Källa: NIS 2-direktivet (krav på revisionsloggar): loggade säkerhetshändelser, lagringstid på ett år.

Flerfaktorautentisering

Ett enda lösenord ger endast ett svagt skydd för åtkomst; NIS-2-direktivet kräver åtkomstkontroll med multifaktorautentisering.

Transpareo erbjuder multifaktorautentisering för alla användare av Applikationshanteraren – via Authenticator-appen, passnyckel eller hårdvarunyckel – inklusive reservkoder för den händelse att nyckeln skulle gå förlorad. Kravet på multifaktorautentisering kan aktiveras för ditt konto.

Källa: NIS 2-direktivet (åtkomstkontroll och multifaktorautentisering).

ISO 27001–certifierad webbhotellstjänst i Tyskland

Var serverna är placerade och hur datacentret är säkrat avgör den fysiska säkerheten för dina uppgifter – och vilken lagstiftning de omfattas av.

Transpareo använder ISO 27001–certifierade servrar i Tyskland, med strikta fysiska och organisatoriska säkerhetsåtgärder. Genom att vara beläget i Tyskland omfattas dina uppgifter dessutom helt av europeisk lagstiftning.

Källa: ISO/IEC 27001 (informationssäkerhetsledning), certifierat datacenter i Tyskland.

Sköter leverantören EU-registreringen åt dig?

Registreringen i EU-registret samt inhämtandet av det officiella intyget är en återkommande uppgift som en leverantör kan sköta åt er. Registerförordningen föreskriver detta uttryckligen: En tjänsteleverantör får sköta registreringen på uppdrag, men det juridiska ansvaret ligger kvar hos den ekonomiska aktören.

Transpareo registrerar era pass på era vägnar så snart EU offentliggör det tekniska gränssnittet – ni förblir den juridiskt ansvariga aktören, men slipper den operativa arbetsbördan. Innan gränssnittet finns tillgängligt kan ingen tillhandahålla denna tjänst; vi har redan förberett de uppgifter som krävs för detta.

Källa: Förordningen om genomförande av DPP-registret (utkast), artikel 19: Registreringen kan utföras av en tjänsteleverantör på uppdrag av den ekonomiska aktören; ansvaret ligger dock kvar hos den ekonomiska aktören.

Tydliga regler för supportinsatser och supportkostnader

Vissa leverantörer skiljer användningen från supporten och fakturerar hjälpen separat; i slutändan blir samarbetet därmed svårt att beräkna kostnaderna för.

Hos Transpareo ingår supporten i priset – inget separat supportavtal, inga extra timmar som faktureras efter tidsåtgång. All den support du behöver ingår redan i det angivna priset.

Transparent prisstruktur

En prisstruktur som först blir tydlig under säljsamtalet eller som debiteras i efterhand per språk, produkt och gränssnittsanrop gör de faktiska kostnaderna oförutsägbara.

Transpareo publicerar öppet fyra prisplaner för alla företagsstorlekar på sin webbplats, med en kostnadsfri provperiod och möjlighet att säga upp abonnemanget när som helst. Det finns inga dolda tilläggskostnader per språk, produkt eller gränssnittsanrop – det angivna priset är det pris du betalar.