

Vergelijkingsformulier voor DPP-aanbieders

Alleen reeds bestaande, controleerbare functies worden aangevinkt – geen aankondigingen of intentieverklaringen. De kolom ‘Transpareo’ is vooraf ingevuld; de twee lege kolommen vult u in wanneer u andere aanbieders beoordeelt. Toelichtingen en bronnen bij elk criterium vindt u aan het einde van het document.

Stand: 10.09.2026

Wettelijk verplicht

Criterium	Transpareo		
Gegevensuitwisseling in een open, gestandaardiseerd formaat De paspoortgegevens zijn via open standaarden toegankelijk – leesbaar voor elk bevoegd systeem, niet alleen voor de software van één enkele aanbieder. EN 18216	☒	☐	☐
Unieke, draagbare identificatiecode zonder binding aan een provider De productcode hoort bij het product, niet bij het platform – bij een verandering van aanbieder behoudt de pas zijn identiteit. EN 18219	☒	☐	☐
Fysieke gegevensdrager, blijvend leesbaar De QR-code op het product leidt in elke browser naar de pas – zonder app, zonder account, met elke smartphone. EN 18220	☒	☐	☐

Criterium	Transpareo		
Opslag en archivering gedurende de minimale looptijd Elke gepubliceerde versie blijft gedurende de wettelijk voorgeschreven termijn beschikbaar – ook oudere versies, niet alleen de huidige. EN 18221	☒	☐	☐
API voor levenscyclusbeheer en doorzoekbaarheid Een programmeerinterface leest, maakt en doorzoekt paspoorten – het is niet zomaar een webinterface waar je op kunt klikken. EN 18222	☒	☐	☐
Interoperabel gegevensmodel De paspoortgegevens volgen een gemeenschappelijk model dat door andere systemen kan worden gelezen zonder dat de opmaak hoeft te worden aangepast. EN 18223	☒	☐	☐
Toegangsrechtenmodel met drie niveaus Openbare, geautoriseerde en officiële gegevens zijn duidelijk gescheiden – iedereen ziet precies datgene waarvoor hij bevoegd is. EN 18239	☒	☐	☐
Aantoonbare authenticiteit en integriteit van gegevens Elke versie is dubbel ondertekend en kan in de browser worden gecontroleerd – zonder dat je ons hoeft te vertrouwen, uitsluitend op basis van de gegevens. EN 18246	☒	☐	☐
Koppeling met het register van de Europese Commissie Registratie inclusief officieel bewijs – zodra de EU de technische interface publiceert. Die is nog niet beschikbaar; geen enkele aanbieder kan hier op dit moment aan voldoen.	☐	☐	☐
Bewaring van de registratiegegevens na afloop van de wettelijke termijn Een onwijzigbaar archief van tien jaar – noch de fabrikant, noch Transpareo kan een versie achteraf wijzigen.	☒	☐	☐

Criterium	Transpareo		
Productgegevens in de officiële talen van elke doelmarkt De verplichte informatie wordt weergegeven in de officiële talen van elk land waar het product wordt verkocht - bij verkoop in de hele EU dus in alle 24 officiële talen, niet alleen op de thuismarkt.	☒	☐	☐

Nuttig voor het beheer van een DPP-database

Criterium	Transpareo		
Talen buiten de EU 16 extra talen naast de 24 officiële EU-talen - 40 in totaal, voor doelmarkten buiten de Unie.	☒	☐	☐
Versiebeheer & wijzigingsgeschiedenis Elke wijziging leidt tot een nieuwe, traceerbare versie met vermelding van het tijdstip en de auteur - gedurende de gehele levenscyclus van het product.	☒	☐	☐
Schaalbare massaproductie-installatie voor product-families Productgegevens uploaden via Excel of CSV en toewijzen aan de verplichte velden - voor grote hoeveelheden is er bovendien een bulk-API beschikbaar.	☒	☐	☐
Op rollen gebaseerd intern rechtenbeheer Er zijn regels vastgelegd over wie binnen het bedrijf welke gegevens mag bijwerken of vrijgeven - inclusief strikt beperkte, tijdelijke toegangsrechten voor externen.	☒	☐	☐
Bewaring na afloop van de overeenkomst Als u uw lidmaatschap opzegt, blijven uw gepubliceerde pasjes toegankelijk in het onwijzigbare tienjarige archief.	☒	☐	☐
Ondertekening met een eigen cryptografische sleutel Bring Your Own Key: U bewaart de privésleutel zelf; wij voegen alleen een onafhankelijke tegenhandtekening toe.	☒	☐	☐

Criterium	Transpareo	_____	_____
Identiteit van de exposant, onafhankelijk van het platform Uw exposantenidentiteit staat als DID:web op uw eigen domein, niet op het onze - een overstap naar een andere provider komt neer op een DNS-verhuizing.	☒	☐	☐
Controleerbaarheid door derden, geheel zonder tussenkomst van de aanbieder Een open-source-renderer controleert hashes en handtekeningen in de browser - zonder contact op te nemen met een van onze servers.	☒	☐	☐

Gewenste extra functies

Criterium	Transpareo	_____	_____
Overstappen naar een andere provider zonder gegevensverlies Bij de overstap neemt u de volledige paspoortdatabase mee in open formaten - ondertekend en zelfcontroleerbaar; aan het einde van het contract blijven de verplichte paspoorten toegankelijk in het onwijzigbare tienjarige archief, zonder gegevensverlies.	☒	☐	☐
Koppeling met bestaande systemen in plaats van een data-eiland Met gesigndeerde webhooks en een bulk-API kunt u de Pass aan uw systemen koppelen - er is geen kant-en-klare connector voor een specifiek ERP-systeem.	☒	☐	☐
Batch-import en -export die verder gaan dan de strikte EU-verplichtingen Grote hoeveelheden gegevens kunnen in beide richtingen worden verplaatst - niet alleen de verplichte velden.	☒	☐	☐

Veiligheid en gegevensbescherming

Criterium	Transpareo		
Aparte database en eigen sleutel Uw gegevens worden opgeslagen in een eigen database, versleuteld met een eigen sleutel - gescheiden op database- en versleutelingsniveau.	☒	☐	☐
Versleuteling en back-ups TLS voor alle verbindingen, AES-versleuteling van gevoelige gegevens en versleutelde back-ups met sleutelrotatie.	☒	☐	☐
Beveiligingslogboek Inlogpogingen, MFA-verificaties en activiteiten met API-sleutels worden geregistreerd en een jaar bewaard.	☒	☐	☐
Meervoudige authenticatie Authenticator-app, passkey of hardware sleutel voor alle gebruikers, met back-upcodes voor het geval deze verloren gaan.	☒	☐	☐
ISO 27001-gecertificeerde hosting in Duitsland Servers in Duitsland met strenge fysieke en organisatorische beveiligingsmaatregelen.	☒	☐	☐

Economische en organisatorische kwesties

Criterium	Transpareo		
Regelt de aanbieder de EU-registratie voor u? Zodra de EU de interface publiceert, zorgen wij voor de registratie, inclusief het officiële bewijs - u hoeft er dus niets voor te doen.	☒	☐	☐
Duidelijke regeling voor ondersteuningsinspanningen en ondersteuningskosten Bij Transparéo is de ondersteuning bij de prijs inbegrepen - geen apart ondersteuningscontract, geen extra kosten.	☒	☐	☐

Criterium	Transpareo		
Transparante prijsstructuur Vier openbare tariefplannen voor bedrijven van elke omvang, gratis proefperiode, op elk moment opzegbaar – zonder verborgen extra kosten per taal, product of API-aanroep.	☒	☐	☐

Toelichtingen en bronnen

Gegevensuitwisseling in een open, gestandaardiseerd formaat **EN 18216**

De norm schrijft voor dat digitale productpaspoorten toegankelijk moeten zijn via open, gestandaardiseerde protocollen – zodat overheidsinstanties, partners en uw eigen systemen de gegevens kunnen lezen zonder gebonden te zijn aan de software van een bepaalde aanbieder. Een eigen formaat zou een eiland zijn: zonder de aanbieder zou u geen toegang meer hebben tot uw eigen gegevens. De norm is sinds 15 juli 2026 opgenomen in het Publicatieblad van de EU (Uitvoeringsbesluit (EU) 2026/1736) en geniet daarmee het vermoeden van conformiteit met de ESPR.

Transpareo levert alle passgegevens en interfaces via standaard-HTTPS in gestructureerde, machinaal leesbare vorm – zonder speciale software, zonder propriëtaire protocollen. Elke gepubliceerde versie is bovendien ondertekend, zodat een ontvanger de gegevens niet alleen kan lezen, maar ook kan controleren of ze ongewijzigd zijn. Wat u in de interface ziet, is dezelfde dataset die elk bevoegd systeem via de open interfaces opvraagt.

Bron: EN 18216, Eisen aan protocollen voor gegevensuitwisseling: „Voor de gestandaardiseerde DPP-toegang moeten de vastgestelde protocollen voor gegevensuitwisseling worden gebruikt.”

Unieke, draagbare identificatiecode zonder binding aan een provider **EN 18219**

Elk productpaspoort moet een unieke identificatiecode hebben die permanent naar hetzelfde product verwijst en niet aan een bepaalde aanbieder gebonden is. Als een aanbieder de identificatiecode aan zijn eigen infrastructuur koppelt, verliezen uw paspoorten bij een overstap hun identiteit – elke afgedrukte code en elke registratie zou dan nergens meer naar verwijzen. De norm is sinds 15 juli 2026 gepubliceerd in het Publicatieblad van de EU.

Transpareo kent de identificatiecode toe als GS1 Digital Link met uw GTIN – een open industriestandaard die bij het product hoort, niet bij het platform – en controleert elke identificatiecode aan de hand van de goedgekeurde normschema's. De signatuuridentiteit staat als DID:web op uw eigen domein,

niet op het onze. De identificatiecode blijft geldig, zelfs als een systeem uitvalt: een permanent fallback-adres blijft deze omzetten, en de pas behoudt zijn identiteit bij elke verandering van aanbieder.

Bron: EN 18219, paragraaf 4.6.2(3): „De unieke identificatiecode mag niet leiden tot een binding aan een bepaalde aanbieder.”

Fysieke gegevensdrager, blijvend leesbaar EN 18220

De pas moet via een machinaal leesbaar gegevensdrager op het product toegankelijk zijn, die iedereen zonder speciale software kan raadplegen – en die gedurende de gehele levensduur van het product leesbaar blijft, ook na gebruik en reparatie. Een gegevensdrager die een bepaalde app of een account vereist, sluit een deel van het publiek uit. De norm is sinds 15 juli 2026 opgenomen in het Publicatieblad van de EU.

Transpareo genereert een QR-code volgens ISO/IEC 18004, die een GS1 Digital Link-adres bevat en in elke browser direct naar het paspoort leidt – geen inloggen, geen download, op elke smartphone. Model, batch en artikel zijn al in het gecodeerde adres opgenomen, zodat een scan direct op het juiste niveau terechtkomt. Omdat het adres stabiel blijft dankzij een permanente fallback-resolutie, blijft een eenmaal afgedrukte code gedurende de gehele levensduur van het product geldig.

Bron: EN 18220, Eisen aan gegevensdragers (paragraaf 5): symbolen, codering, afdrukkwaliteit en duurzaamheid; de gegevensdrager moet ook na meerdere gebruiks- en reparatiecycli leesbaar blijven.

Opslag en archivering gedurende de minimale looptijd EN 18221

De norm schrijft voor dat een norm, inclusief de versiegeschiedenis ervan, gedurende de wettelijk voorgeschreven termijn moet worden bewaard en ongewijzigd toegankelijk moet blijven. Als alleen de actuele versie wordt bewaard, gaat de traceerbaarheid van eerdere gegevens verloren – en juist die moet een marktdeelnemer aan de autoriteiten kunnen aantonen. De bewaartermijn is afhankelijk van de betreffende sectorale wetgeving, maar bedraagt minimaal tien jaar. De norm is sinds 15 juli 2026 opgenomen in het Publicatieblad van de EU.

Transpareo slaat elke publicatie op als een bevroren, ondertekende versie in een onveranderbaar archief, waarin niemand deze later nog kan wijzigen of verwijderen – noch u, noch wij. Oudere versies blijven naast de huidige versie beschikbaar, en elke versie is voorzien van een tijdstempel en een handtekening. Zo kan voor elk moment worden aangetoond wat er destijds in het paspoort stond vermeld.

Bron: EN 18221: „Het digitale productpaspoort moet gedurende de gehele levensduur beschikbaar blijven voor geautoriseerde gebruikers.”

API voor levenscyclusbeheer en doorzoekbaarheid EN 18222

Naast de weergave in de browser vereist de norm een programmeerinterface waarmee paspoorten kunnen worden aangemaakt, gelezen, bijgewerkt en doorzocht op productcodes. Zonder een dergelijke interface blijft elke massaverwerking handmatig werk, en kunnen andere systemen de paspoort-database niet geautomatiseerd gebruiken. De norm is sinds 15 juli 2026 gepubliceerd in het Publicatieblad van de EU.

Transpareo ondersteunt de voorgeschreven normmethoden via een versiebeheerde, gestandaardiseerde interface: Paspoorten kunnen programmeerbaar worden aangemaakt, gelezen, bijgewerkt en pagina voor pagina worden doorzocht op productcodes. Het ondertekende paspoort wordt daarbij ongewijzigd geleverd – de interface geeft precies de bytes weer waarvan een controleur de handtekening kan narekenen.

Bron: EN 18222: gestandaardiseerde programmeerinterface (API) voor levenscyclusbeheer en doorzoekbaarheid van het DPP, zoals vereist door de ESPR.

Interoperabel gegevensmodel EN 18223

Om ervoor te zorgen dat paspoorten tussen systemen en binnen toeleveringsketens op elkaar aansluiten, schrijft de norm een gemeenschappelijk gegevensmodel voor met een uniforme betekenis van de velden. Een leveranciersspecifiek model dwingt elke partner tot een eigen vertaling – en elke vertaling is een bron van fouten. De norm is sinds 15 juli 2026 opgenomen in het Publicatieblad van de EU.

Transpareo is gebaseerd op een horizontale vocabulairelaag met parallelle, erkende vakvocabulaires (GS1, EPCIS en andere) en beschrijft elk gegevenspunt met een verwijzing naar het bijbehorende woordenboek en het gegevenstype. Een ontvangend systeem komt daardoor niet alleen te weten hoe een veld heet, maar ook wat het betekent – de pas blijft leesbaar zonder herformattering.

Bron: EN 18223: gemeenschappelijk semantisch gegevensmodel voor de interoperabiliteit van het DPP-systeem.

Toegangsrechtenmodel met drie niveaus EN 18239

Een productpas bevat openbare gegevens, gegevens voor geautoriseerde marktdeelnemers en gegevens die uitsluitend bestemd zijn voor overheidsinstanties; de norm schrijft voor dat deze niveaus gescheiden moeten worden gehouden en per gegevensveld worden geregeld. Openbare gegevens moeten zonder aanmelding toegankelijk zijn, alle overige gegevens alleen na controle. EN 18239 bevindt zich in de laatste fase van goedkeuring.

Transpareo hanteert zichtbaarheid als een eigenschap per gegevensveld: het openbare niveau wordt zonder authenticatie aangeboden, de hogere niveaus worden beschermd via een eigen, gelogde overheidsinterface met uitsluitend leestoeegang, en elke toegang tot beschermde gegevens wordt

vastgelegd in het auditlogboek. Het driedelige model van de norm is daarmee vandaag de dag al in de architectuur geïntegreerd en niet achteraf toegevoegd.

Bron: EN 18239 (ontwerp, in de laatste fase van goedkeuring): „Toegang tot openbare gegevens moet mogelijk zijn voor zowel EU- als niet-EU-actoren zonder aanvullende authenticatie”; voor gecontroleerde gegevens is geauthenticeerde, aantoonbare toegang vereist.

Aantoonbare authenticiteit en integriteit van gegevens EN 18246

De norm schrijft voor dat de authenticiteit en integriteit van een paspoort aantoonbaar moeten zijn en dat controle vrij en onbeperkt mogelijk moet zijn. Het vertrouwen mag niet afhangen van het voortbestaan van de aanbieder, maar moet verbonden zijn aan het gegevensbestand zelf – anders zou elk paspoort slechts zo geloofwaardig zijn als het bedrijf dat het op dat moment host. EN 18246 bevindt zich in de laatste fase van goedkeuring.

Transpareo ondertekent elke gepubliceerde versie met twee onafhankelijke sleutels (uitgever en Transpareo) en koppelt de versies aan elkaar via hun hash, zodat ook de geschiedenis niet onopgemerkt kan worden herschreven. Een open-source-renderer controleert beide handtekeningen rechtstreeks in de browser, zonder contact op te nemen met een van onze servers – het vereiste, ondertekende en zelfcontroleerbare bewijs is daarmee al geïmplementeerd.

Bron: EN 18246 (ontwerp, in de laatste fase van goedkeuring): De authenticiteit, betrouwbaarheid en integriteit van de DPP-gegevens moeten aantoonbaar zijn.

Koppeling met het register van de Europese Commissie

Elk paspoort dat onder de registratieplicht valt, moet voortaan worden opgenomen in het centrale EU-register, dat een permanent registratienummer en een officieel registratiebewijs verstrekt. De EU heeft de technische interface hiervoor nog niet gepubliceerd – daarom kan geen enkele aanbieder op dit moment aantonen dat deze koppeling bestaat; als een aanbieder dat beweert, moet u daar navraag naar doen.

Transpareo heeft de koppeling zo ver voorbereid als dat zonder de interface mogelijk is: de daarvoor benodigde velden (registratie-ID, stabiel back-upadres, versie-hash) zijn al in het gegevensmodel aangemaakt. Zodra de EU de interface publiceert, activeren wij de registratie, zonder dat u uw pasjes hoeft aan te passen. Tot die tijd blijft dit punt openstaan – bij ons net als bij elke eerlijke aanbieder.

Bron: Ontwerp van de uitvoeringsverordening inzake het DPP-register (Ares(2026)4424976).

Bewaring van de registratiegegevens na afloop van de wettelijke termijn

Geregistreerde pasgegevens moeten na afloop van de wettelijke termijn – doorgaans tien jaar vanaf de registratie – ongewijzigd beschikbaar blijven, zelfs in geval van faillissement of bedrijfsbeëindiging van

de fabrikant. Deze verplichting blijft dus zowel na afloop van uw contract met een aanbieder als na het verdwijnen van de aanbieder zelf van kracht.

Transpareo houdt hiervoor een onveranderbaar archief bij, waarin een eenmaal opgeslagen versie achteraf door niemand kan worden gewijzigd of verwijderd – noch door de fabrikant, noch door ons. Het archief wordt automatisch geactiveerd bij de EU-registratie. En om ervoor te zorgen dat het ook toegankelijk blijft als Transpareo op een dag niet meer zou bestaan, is het voortbestaan ervan gewaarborgd door een notariële deponering in Zwitserland.

Bron: Uitvoeringsverordening DPP-register, art. 10, lid 3 (bewaartermijn van tien jaar).

Productgegevens in de officiële talen van elke doelmarkt

De verplichte vermeldingen op een paspoort moeten beschikbaar zijn in de officiële talen van elke lidstaat waar het product op de markt wordt gebracht – niet alleen in de taal van de vestigingsplaats van de fabrikant. Wie alleen de thuismarkt bedient, voldoet niet aan de verplichting voor alle andere doelmarkten.

Transpareo onderhoudt elk paspoort in meerdere talen en levert de verplichte inhoud in alle 24 officiële EU-talen. U voert de inhoud één keer in; de taalversies worden daaruit gegenereerd, zonder dat u per taal extra hoeft te betalen of afzonderlijke paspoorten hoeft bij te houden. Het paspoort is daarmee in elke doelmarkt conform de voorschriften leesbaar.

Bron: Batterijverordening (EU) 2023/1542: gegevens in de officiële talen van de lidstaten waar het product in de handel wordt gebracht.

Talen buiten de EU

Naast de wettelijke verplichting is het nuttig als een pas ook talen buiten de EU omvat – voor exportmarkten, internationale handelspartners en consumenten die geen officiële taal van de Unie spreken.

Transpareo onderhoudt in totaal 40 taalversies, waaronder de 24 officiële EU-talen. U voert de inhoud één keer in en geeft deze weer in elke gewenste taal, zonder extra te betalen per taal. Ook de interface waarin u uw paspoorten beheert (de Application Manager) is in alle 40 talen vertaald, en u kunt informatie in elk van de beschikbare talen invoeren.

Versiebeheer & wijzigingsgeschiedenis

Een pas verandert gedurende de levensduur van het product; zonder een volledige versiegeschiedenis kan later niet worden aangetoond welke stand op welk moment van kracht was. De norm schrijft daarom voor dat alle wijzigingen aan de pas worden gearchiveerd.

Transpareo legt elke publicatie vast als een afzonderlijke, ondertekende versie en registreert wie deze wanneer heeft aangemaakt en welke velden daarbij zijn gewijzigd. Zo blijft elke vermelding met terug-

werkende kracht controleerbaar, en overschrijft een latere correctie de geschiedenis niet, maar zet deze voort.

Bron: EN 18221: „Alle wijzigingen in het digitale productpaspoort moeten worden gearchiveerd.”

Schaalbare massaproductie–installatie voor productfamilies

Wie veel vergelijkbare producten in het assortiment heeft, kan niet elk productblad afzonderlijk met de hand aanmaken; een werkbaar systeem heeft een manier nodig om hele productfamilies in één keer vast te leggen.

Met Transpareo kunt u productgegevens via Excel of CSV uploaden en aan de verplichte velden toewijzen; voor zeer grote hoeveelheden is er bovendien een bulk-API beschikbaar die productpagina's automatisch aanmaakt. Hierdoor is het systeem schaalbaar van een tiental tot tienduizenden productpagina's.

Op rollen gebaseerd intern rechtenbeheer

Niet iedereen binnen het bedrijf mag de inhoud van elk pasje bewerken of vrijgeven; de norm vereist een op rollen gebaseerd rechtenbeheer met gelogde toegangen.

Transpareo kent rechten toe per rol en gebruikersgroep en registreert elke wijziging. Ook externe partijen, zoals werkplaatsen of recyclers, krijgen slechts zeer beperkte, tijdelijke toegangsrechten; overheidsinstanties hebben toegang via een aparte, uitsluitend op leesrechten gebaseerde interface, die elke toegang in het auditlogboek vastlegt.

Bron: EN 18239 (ontwerp), Beheer van toegangsrechten: regelt welke actoren DPP-gegevens mogen bewerken en vrijgeven.

Bewaring na afloop van de overeenkomst

De bewaarplicht houdt niet op bij het einde van het contract: een geregistreerd paspoort moet langer bewaard blijven dan de wettelijke termijn, ook als u de aanbieder verlaat. Een aanbieder die paspoorten bij opzegging deactiveert, bezorgt u een compliance-probleem.

Transpareo bewaart deze in hetzelfde onveranderlijke archief met een looptijd van tien jaar als de registratiegegevens – na een opzegging levert een permanent fallback-adres de pasjes nog steeds uit, en de interface voor de overheid leest hetzelfde gegevensrecord uit het archief dat na afloop van het contract nog steeds beschikbaar is. Reeds afgedrukte QR-codes blijven geldig.

Bron: EN 18221: Archiefversies worden ook opgeslagen bij de back-updienstverlener.

Ondertekening met een eigen cryptografische sleutel

Wie de priv sleutel bezit, kan pasjes aanmaken op naam van de uitgever; daarom is het veiliger als de uitgever deze sleutel zelf bewaart, in plaats van deze aan de aanbieder toe te vertrouwen.

Met 'Bring Your Own Key' beheert uw bedrijf een eigen handtekening-eindpunt – Transpareo bewaart de priv sleutel nooit en voegt alleen een onafhankelijke tegenhandtekening toe. Zo bevat elke versie twee onderling onafhankelijke handtekeningen, en is uw uitgevershandtekening er een die Transpareo zelf niet kan genereren.

Identiteit van de exposant, onafhankelijk van het platform

Om ervoor te zorgen dat een controleur uw openbare sleutels kan vinden, moet het pasje een gepubliceerde identiteit van de uitgever bevatten. Als deze op het domein van de aanbieder staat, bent u aan hem gebonden: een overstap zou elke reeds afgedrukte code ongeldig maken.

Transpareo publiceert uw identiteit als DID: op uw eigen domein, niet op het onze – een overstap naar een andere aanbieder wordt zo een DNS-verhuizing, en reeds afgedrukte codes blijven samen met hun verificatie geldig. Bovendien spiegelen we elke openbare sleutel op het moment van publicatie naar een permanent adres, zodat elke versie verifieerbaar blijft, zelfs als de oorspronkelijke host verdwijnt.

Bron: EN 18219, paragraaf 4.2.2 (Duurzaamheid): identificatiecodes blijven gedurende de gehele levenscyclus behouden; webdomeinen zijn overdraagbaar of kunnen worden omgeleid.

Controleerbaarheid door derden, geheel zonder tussenkomst van de aanbieder

De doorslaggevende test voor vertrouwen is of een derde partij het certificaat kan controleren zonder gebruik te maken van de infrastructuur van de aanbieder. De norm schrijft voor dat de controle van de geldigheid en integriteit voor de controleur kosteloos en zonder beperkingen mogelijk moet zijn.

Transpareo publiceert hiervoor een open-source renderer die de bytes van een versie uit een willekeurige bron laadt, de hash opnieuw berekent en beide handtekeningen controleert aan de hand van de openbare sleutels die in het pasje worden vermeld – geen login, geen telefoontje naar ons, geen afhankelijkheid van een actief platform. Wie wantrouwig is, kan de broncode lezen.

Bron: EN 18246 (ontwerp): „De controle van de geldigheid en integriteit van de DPP-gegevens moet voor de controleur kosteloos en zonder beperkingen mogelijk zijn.”

Overstappen naar een andere provider zonder gegevensverlies

Een aanbieder die de overstap bemoeilijkt, houdt u vast aan de hand van uw eigen gegevens – en wat er aan het einde van het contract met die gegevens gebeurt, bepaalt of u vrij kunt overstappen. De norm schrijft daarom voor dat de gegevens via een open, interoperabel netwerk kunnen worden overgedragen zonder dat u aan een aanbieder gebonden bent.

Transpareo slaat de wettelijk vereiste documenten vanaf het begin op in een open, openbaar spiegelbare omgeving: een eenvoudige synchronisatie genereert een volledige, ondertekende kopie die zichzelf controleert aan de hand van de gepubliceerde sleutels, zonder tussenkomst van ons. Het volledige gebeurtenissenarchief verstrekken wij via een ondertekend, tijdelijk downloadadres aan u of uw nieuwe aanbieder; de bijbehorende productcatalogus wordt bovendien als JSON-LD en CSV aangeleverd. Aan het einde van het contract blijven de geregistreerde verplichte gegevens via het onveranderlijke tienjarige archief toegankelijk: De openbare mirror en het archief blijven gesynchroniseerd en leveren dezelfde dataset aan; reeds afgedrukte QR-codes kunnen nog steeds worden ingelezen via het permanente fallback-adres, en de registerverwijzing verwijst naar het nieuwe adres. Zo loopt het contract af zonder gegevensverlies en zonder dat de wettelijke bewaarplicht wordt geschonden.

Bron: EN 18216: Gegevens moeten „via een open, interoperabel netwerk zonder binding aan een bepaalde aanbieder kunnen worden overgedragen”.

Koppeling met bestaande systemen in plaats van een data-eiland

Een pas die alleen in de interface van de aanbieder bestaat, wordt een data-eiland naast uw overige systemen – elke wijziging moet dan dubbel worden bijgewerkt.

Transpareo meldt gebeurtenissen via gesigndeerde webhooks en maakt het mogelijk om gegevens via een bulk-API in en uit te lezen, zodat u de pas aan uw eigen systeemlandschap kunt koppelen. We leveren bewust geen kant-en-klare connector voor een specifiek ERP-systeem – de open, gesigndeerde interfaces zijn geschikt voor elk systeem, in plaats van de voorkeur te geven aan één bepaald systeem.

Batch-import en -export die verder gaan dan de strikte EU-verplichtingen

Wie de geregistreerde gegevens ook buiten het paspoort wil gebruiken, heeft import- en exportfuncties nodig voor meer dan alleen de wettelijk verplichte velden.

Transpareo neemt grotere hoeveelheden gegevens aan via Excel, CSV en de bulk-API en geeft deze in dezelfde omvang weer uit. Zo dient het systeem niet alleen om aan de EU-verplichting te voldoen, maar ook voor uw eigen gegevensbeheer.

Aparte database en eigen sleutel

In een gedeelde database zijn uw gegevens gekoppeld aan die van andere klanten; een duidelijke, aantoonbare scheiding is dan nauwelijks mogelijk – en het recht op verwijdering op grond van artikel 17 van de AVG is moeilijk aan te tonen.

Bij Transpareo staat elke klant in een eigen database, versleuteld met een eigen sleutel – de scheiding vindt plaats op zowel databaseniveau als versleutelingsniveau. Dit voldoet aan het recht op verwijdering door middel van verifieerbare verwijdering; de hosting vindt plaats in Duitsland en de verwerkersovereenkomst (AVV) is inbegrepen.

Bron: AVG, artikel 17 (recht op verwijdering), waaraan wordt voldaan door middel van een afzonderlijke database, een eigen sleutel en een verifieerbare verwijdering.

Versleuteling en back-ups

Een aanbieder moet gegevens tijdens de overdracht en in rust beschermen en beveiligen tegen uitval; de AVG vereist hiervoor maatregelen die in overeenstemming zijn met de stand van de techniek.

Transpareo versleutelt alle verbindingen met TLS en gevoelige applicatiegegevens met AES. De back-ups zijn GPG-versleuteld, worden vernieuwd met regelmatige sleutelrotatie, worden om de vier uur gemaakt en twaalf maanden lang op een aparte server bewaard.

Bron: AVG, artikel 32 (Beveiliging van de verwerking): TLS, AES en versleutelde back-ups met rotatie.

Beveiligingslogboek

Beveiligingsgerelateerde gebeurtenissen moeten traceerbaar blijven: wie zich wanneer heeft aangemeld en hoe sleutels zijn gebruikt. De NIS-2-richtlijn vereist dat er hiervoor auditlogs worden bijgehouden.

Transpareo houdt een beveiligingslogboek bij van inlogpogingen, MFA-uitdagingen en API-sleutelactiviteit en bewaart dit gedurende één jaar. Hiermee wordt voldaan aan de NIS-2-vereisten voor auditlogs.

Bron: NIS-2-richtlijn (eisen inzake auditlogs): geregistreerde beveiligingsgebeurtenissen, bewaartermijn van één jaar.

Meervoudige authenticatie

Een enkel wachtwoord biedt slechts een zwakke beveiliging; de NIS-2-richtlijn vereist toegangscontrole met meervoudige authenticatie.

Transpareo biedt meervoudige authenticatie voor alle gebruikers van de Application Manager - via een authenticator-app, een passkey of een hardware-sleutel - inclusief back-upcodes voor het geval deze verloren gaan. De MFA-verplichting kan voor uw account worden afgedwongen.

Bron: NIS-2-richtlijn (toegangscontrole en meervoudige authenticatie).

ISO 27001-gecertificeerde hosting in Duitsland

De locatie van de servers en de beveiliging van het datacenter zijn bepalend voor de fysieke veiligheid van uw gegevens - en voor de wetgeving waaronder deze vallen.

Transpareo host op ISO 27001-gecertificeerde servers in Duitsland, met strenge fysieke en organisatorische beveiligingsmaatregelen. Door de locatie in Duitsland vallen uw gegevens bovendien volledig onder het Europese recht.

Bron: ISO/IEC 27001 (informatiebeveiligingsmanagement), gecertificeerd datacenter in Duitsland.

Regelt de aanbieder de EU-registratie voor u?

De inschrijving in het EU-register, inclusief het verkrijgen van het officiële bewijs, is een terugkerende taak die een dienstverlener voor u kan uitvoeren. De registerverordening voorziet hier uitdrukkelijk in: een dienstverlener mag de registratie in opdracht uitvoeren, maar de juridische verantwoordelijkheid blijft bij de marktdeelnemer.

Transpareo registreert uw paspoorten namens u zodra de EU de technische interface publiceert – u blijft de juridisch verantwoordelijke marktdeelnemer, maar draagt niet de operationele lasten. Totdat de interface beschikbaar is, kan niemand deze dienst verlenen; wij hebben de daarvoor benodigde gegevens al voorbereid.

Bron: Uitvoeringsverordening DPP-register (ontwerp), art. 19: De registratie kan door een dienstverlener in opdracht worden uitgevoerd; de verantwoordelijkheid blijft bij de marktdeelnemer.

Duidelijke regeling voor ondersteuningsinspanningen en ondersteuningskosten

Sommige aanbieders maken een onderscheid tussen het gebruik en de ondersteuning en brengen hulp apart in rekening; uiteindelijk maakt dit de samenwerking moeilijk te begroten.

Bij Transpareo is de ondersteuning inbegrepen in het tarief – geen apart ondersteuningscontract, geen extra uren die op basis van de gewerkte uren worden gefactureerd. Wat u aan ondersteuning nodig hebt, is al inbegrepen in de vermelde prijs.

Transparante prijsstructuur

Een prijsstructuur die pas tijdens het verkoopgesprek duidelijk wordt of die achteraf per taal, product en interface-oproep wordt berekend, maakt de werkelijke kosten onvoorspelbaar.

Transpareo publiceert vier tarieven voor elke bedrijfsgrootte openlijk op de website, met een gratis proefperiode en opzegging op elk moment. Er zijn geen verborgen extra kosten per taal, product of interface-oproep – de vermelde prijs is de prijs.