

DPP-Anbieter-Vergleichsbogen

Nur bereits vorhandene, nachprüfbare Funktionen erhalten einen Haken – keine Ankündigungen oder Absichtserklärungen. Die Spalte «Transpareo» ist vorausgefüllt; die beiden leeren Spalten füllen Sie beim Prüfen anderer Anbieter aus. Erläuterungen und Quellen zu jedem Kriterium finden Sie am Ende des Dokuments.

Stand: 10.09.2026

Gesetzlich zwingend vorgeschrieben

Kriterium	Transpareo		
Datenaustausch in offenem, standardisiertem Format Die Passdaten sind über offene Standards abrufbar – lesbar für jedes berechnigte System, nicht nur für die Software eines einzelnen Anbieters. EN 18216	☒	☐	☐
Eindeutige, portable Kennung ohne Anbieterbindung Die Kennung des Produkts gehört zum Produkt, nicht zur Plattform – bei einem Anbieterwechsel behält der Pass seine Identität. EN 18219	☒	☐	☐
Physischer Datenträger, dauerhaft lesbar Der QR-Code am Produkt führt in jedem Browser zum Pass – ohne App, ohne Konto, mit jedem Smartphone. EN 18220	☒	☐	☐
Speicherung & Archivierung über die Mindestlaufzeit Jede veröffentlichte Version bleibt über die gesetzlich vorgeschriebene Dauer abrufbar – auch ältere Stände, nicht nur der aktuelle. EN 18221	☒	☐	☐

Kriterium	Transpareo		
API für Lifecycle-Management & Durchsuchbarkeit Eine Programmierschnittstelle liest, erstellt und durchsucht Pässe – nicht nur eine Weboberfläche zum Anklicken. EN 18222	☒	☐	☐
Interoperables Datenmodell Die Passdaten folgen einem gemeinsamen Modell, das andere Systeme ohne Umformatierung lesen können. EN 18223	☒	☐	☐
Dreistufiges Zugriffsrechtmodell Öffentliche, autorisierte und behördliche Daten sind sauber getrennt – jeder sieht genau das, wozu er berechtigt ist. EN 18239	☒	☐	☐
Nachweisbare Datenauthentizität & Integrität Jede Version ist doppelt signiert und lässt sich im Browser prüfen – ohne Vertrauen in uns, allein aus den Daten. EN 18246	☒	☐	☐
Anbindung an das EU-Kommissionsregister Registrierung samt amtlichem Nachweis – sobald die EU die technische Schnittstelle veröffentlicht. Sie liegt noch nicht vor, das kann heute kein Anbieter erfüllen.	☐	☐	☐
Aufbewahrung der Registrierungsdaten über die gesetzliche Frist Ein unveränderbares Zehn-Jahres-Archiv – weder Hersteller noch Transpareo können eine Version nachträglich ändern.	☒	☐	☐
Produktdaten in den Amtssprachen jedes Zielmarkts Der Pflichtinhalt erscheint in den Amtssprachen jedes Landes, in dem das Produkt verkauft wird – beim EU-weiten Vertrieb also in allen 24 Amtssprachen, nicht nur im Heimatmarkt.	☒	☐	☐

Sinnvoll für den Betrieb einer DPP-Datenbank

Kriterium	Transpareo		
Sprachen über die EU hinaus 16 weitere Sprachen über die 24 EU-Amtssprachen hinaus – 40 insgesamt, für Zielmärkte ausserhalb der Union.	☒	☐	☐
Versionierung & Änderungshistorie Jede Änderung erzeugt eine neue, nachvollziehbare Version mit Zeitpunkt und Urheber – über den gesamten Produktlebenszyklus.	☒	☐	☐
Skalierbare Massenanlage für Produktfamilien Produktdaten per Excel oder CSV hochladen und den Pflichtfeldern zuordnen – für grosse Mengen zusätzlich eine Bulk-API.	☒	☐	☐
Rollenbasierte interne Rechteverwaltung Wer im Unternehmen welche Daten pflegen oder freigeben darf, ist geregelt – inklusive eng begrenzter, befristeter Zugänge für Externe.	☒	☐	☐
Aufbewahrung über das Vertragsende hinaus Kündigen Sie, bleiben Ihre veröffentlichten Pässe im unveränderbaren Zehn-Jahres-Archiv erreichbar.	☒	☐	☐
Signatur mit eigenem kryptografischen Schlüssel Bring Your Own Key: Sie halten den privaten Schlüssel selbst, wir ergänzen nur eine unabhängige Gegensignatur.	☒	☐	☐
Ausstelleridentität unabhängig von der Plattform Ihre Ausstelleridentität steht als DID:web auf Ihrer eigenen Domain, nicht auf unserer – ein Anbieterwechsel wird zum DNS-Umzug.	☒	☐	☐
Prüfbarkeit durch Dritte, ganz ohne den Anbieter Ein quelloffener Renderer prüft Hash und Signaturen im Browser – ohne einen Server von uns zu kontaktieren.	☒	☐	☐

Wünschenswerte Zusatzfunktionen

Kriterium	Transpareo		
Anbieterwechsel ohne Datenverlust Beim Wechsel nehmen Sie den vollständigen Passbestand in offenen Formaten mit – signiert und selbstprüfbar; am Vertragsende bleiben die Pflichtpässe im unveränderbaren Zehn-Jahres-Archiv erreichbar, ohne Datenverlust.	☒	☐	☐
Anbindung an bestehende Systeme statt Dateninsel Signierte Webhooks und eine Bulk-API binden den Pass an Ihre Systeme an – kein vorgefertigter Konnektor für ein bestimmtes ERP.	☒	☐	☐
Batch-Import & -Export über die reine EU-Pflicht hinaus Grössere Datenmengen lassen sich in beide Richtungen bewegen – nicht nur die reinen Pflichtfelder.	☒	☐	☐

Sicherheit & Datenschutz

Kriterium	Transpareo		
Separate Datenbank und eigener Schlüssel Ihre Daten liegen in einer eigenen Datenbank, verschlüsselt mit einem eigenen Schlüssel – getrennt auf Datenbank- und Verschlüsselungsebene.	☒	☐	☐
Verschlüsselung und Backups TLS für alle Verbindungen, AES-Verschlüsselung sensibler Daten und verschlüsselte Backups mit Schlüsselrotation.	☒	☐	☐
Sicherheits-Ereignisprotokoll Login-Versuche, MFA-Challenges und API-Schlüssel-Aktivität werden protokolliert und ein Jahr aufbewahrt.	☒	☐	☐
Mehrfaktor-Authentifizierung Authenticator-App, Passkey oder Hardware-Schlüssel für alle Nutzer, mit Backup-Codes für den Verlustfall.	☒	☐	☐

Kriterium	Transpareo	_____	_____
ISO 27001–zertifiziertes Hosting in Deutschland Server in Deutschland mit strengen physischen und organisatorischen Sicherheitsmassnahmen.	☒	☐	☐

Wirtschaftliche & organisatorische Fragen

Kriterium	Transpareo	_____	_____
Übernimmt der Anbieter die EU–Registrierung für Sie? Wir übernehmen die Registrierung samt amtlichem Nachweis, sobald die EU die Schnittstelle veröffentlicht – Sie haben damit keinen Aufwand.	☒	☐	☐
Klare Regelung für Supportaufwand und Supportkosten Der Support ist bei Transpareo im Preis enthalten – kein getrennter Supportvertrag, keine Zusatzkosten.	☒	☐	☐
Transparente Preisstruktur Vier öffentliche Tarife für jede Unternehmensgrösse, kostenlose Testphase, jederzeit kündbar – ohne versteckte Zusatzkosten pro Sprache, Produkt oder API–Aufruf.	☒	☐	☐

Erläuterungen und Quellen

Datenaustausch in offenem, standardisiertem Format **EN 18216**

Die Norm verlangt, dass Digitale Produktpässe über offene, standardisierte Protokolle zugänglich sind – damit Behörden, Partner und Ihre eigenen Systeme die Daten lesen können, ohne an die Software eines Anbieters gebunden zu sein. Ein proprietäres Format wäre eine Insel: Ohne den Anbieter kämen Sie nicht mehr an Ihre eigenen Daten. Die Norm ist seit dem 15. Juli 2026 im EU–Amtsblatt zitiert (Durchführungsbeschluss (EU) 2026/1736) und trägt damit die Konformitätsvermutung zur ESPR.

Transpareo liefert alle Passdaten und Schnittstellen über Standard-HTTPS in strukturierter, maschinenlesbarer Form aus – ohne Spezialsoftware, ohne proprietäre Protokolle. Jede veröffentlichte Version ist zusätzlich signiert, sodass ein Empfänger nicht nur lesen, sondern auch prüfen kann, dass die Daten

unverändert sind. Was Sie in der Oberfläche sehen, ist derselbe Datensatz, den jedes berechnete System über die offenen Schnittstellen abrufen kann.

Quelle: EN 18216, Anforderung an Datenaustauschprotokolle: «Für den standardisierten DPP-Zugriff sind die festgelegten Datenaustauschprotokolle zu verwenden.»

Eindeutige, portable Kennung ohne Anbieterbindung EN 18219

Jeder Produktpass braucht eine eindeutige Kennung, die dauerhaft auf dasselbe Produkt verweist und keinen Anbieter voraussetzt. Bindet ein Anbieter die Kennung an seine eigene Infrastruktur, verlieren Sie bei einem Wechsel die Identität Ihrer Pässe – jeder gedruckte Code und jede Registrierung zeigt dann ins Leere. Die Norm ist seit dem 15. Juli 2026 im EU-Amtsblatt zitiert.

Transpareo vergibt die Kennung als GS1 Digital Link mit Ihrer GTIN – einem offenen Industriestandard, der dem Produkt gehört, nicht der Plattform – und prüft jede Kennung gegen die zugelassenen Norm-Schemata. Die Signatur-Identität liegt als DID:web auf Ihrer eigenen Domain, nicht auf unserer. Die Kennung bleibt gültig, auch wenn ein System ausfällt: Eine dauerhafte Fallback-Adresse löst sie weiter auf, und der Pass behält seine Identität über jeden Anbieterwechsel hinweg.

Quelle: EN 18219, Abschnitt 4.6.2(3): «Der eindeutige Identifikator darf nicht zu einer Anbieterbindung führen.»

Physischer Datenträger, dauerhaft lesbar EN 18220

Der Pass muss über einen maschinenlesbaren Datenträger am Produkt erreichbar sein, den jeder ohne Spezialsoftware aufrufen kann – und der über die gesamte Produktlebensdauer lesbar bleibt, auch nach Nutzung und Reparatur. Ein Datenträger, der eine bestimmte App oder ein Konto verlangt, sperrt einen Teil der Öffentlichkeit aus. Die Norm ist seit dem 15. Juli 2026 im EU-Amtsblatt zitiert.

Transpareo erzeugt einen QR-Code nach ISO/IEC 18004, der eine GS1-Digital-Link-Adresse trägt und in jedem Browser direkt zum Pass auflöst – kein Login, kein Download, jedes Smartphone. Modell, Charge und Artikel stecken bereits in der kodierten Adresse, sodass ein Scan direkt auf der richtigen Ebene landet. Weil die Adresse über eine dauerhafte Fallback-Auflösung stabil bleibt, bleibt ein einmal gedruckter Code über die gesamte Produktlebensdauer gültig.

Quelle: EN 18220, Anforderungen an Datenträger (Abschnitt 5): Symbolik, Kodierung, Druckqualität und Beständigkeit; der Datenträger soll auch nach mehreren Nutzungs- und Reparaturzyklen lesbar bleiben.

Speicherung & Archivierung über die Mindestlaufzeit EN 18221

Die Norm verlangt, dass ein Pass samt seiner Versionsgeschichte über die regulatorisch vorgeschriebene Dauer gespeichert und unverändert abrufbar bleibt. Wird nur der jeweils aktuelle Stand gehalten, geht die Nachvollziehbarkeit früherer Angaben verloren – genau das aber muss ein Wirtschaftsakteur

gegenüber Behörden belegen können. Die Aufbewahrungsfrist richtet sich nach dem jeweiligen Sektorrecht, mindestens jedoch zehn Jahre. Die Norm ist seit dem 15. Juli 2026 im EU-Amtsblatt zitiert.

Transpareo schreibt jede Veröffentlichung als eingefrorene, signierte Version in ein unveränderbares Archiv, in dem sie später niemand mehr ändern oder löschen kann – weder Sie noch wir. Ältere Stände bleiben neben dem aktuellen abrufbar, und jede Version trägt Zeitstempel und Signatur. So lässt sich für jeden Zeitpunkt belegen, was der Pass damals ausgewiesen hat.

Quelle: EN 18221: «Der Digitale Produktpass ist autorisierten Nutzern während seiner gesamten Lebensdauer verfügbar zu halten.»

API für Lifecycle-Management & Durchsuchbarkeit EN 18222

Neben der Anzeige im Browser verlangt die Norm eine Programmierschnittstelle, über die Pässe angelegt, gelesen, aktualisiert und über Produktkennungen durchsucht werden können. Ohne solche Schnittstelle bleibt jede Massenverarbeitung Handarbeit, und andere Systeme können den Passbestand nicht automatisiert nutzen. Die Norm ist seit dem 15. Juli 2026 im EU-Amtsblatt zitiert.

Transpareo bedient die vorgeschriebenen Norm-Methoden über eine versionierte, standardisierte Schnittstelle: Pässe lassen sich programmgesteuert anlegen, lesen, aktualisieren und seitenweise über Produktkennungen durchsuchen. Der signierte Pass wird dabei unverändert ausgeliefert – die Schnittstelle gibt exakt die Bytes heraus, deren Signatur ein Prüfer nachrechnen kann.

Quelle: EN 18222: standardisierte Programmierschnittstelle (API) für Lifecycle-Management und Durchsuchbarkeit des DPP, wie von der ESPR gefordert.

Interoperables Datenmodell EN 18223

Damit Pässe zwischen Systemen und über Lieferketten hinweg zusammenpassen, schreibt die Norm ein gemeinsames Datenmodell mit einheitlicher Bedeutung der Felder vor. Ein anbiereigenes Modell zwingt jeden Partner zu einer eigenen Übersetzung – und jede Übersetzung ist eine Fehlerquelle. Die Norm ist seit dem 15. Juli 2026 im EU-Amtsblatt zitiert.

Transpareo baut auf eine horizontale Vokabular-Schicht mit parallelen, anerkannten Fachvokabularen (GSI, EPCIS und weitere) und beschreibt jeden Datenpunkt mit Verweis auf sein Wörterbuch und seinen Datentyp. Ein empfangendes System erfährt dadurch nicht nur, wie ein Feld heisst, sondern auch, was es bedeutet – der Pass bleibt ohne Umformatierung lesbar.

Quelle: EN 18223: gemeinsames semantisches Datenmodell für die Systeminteroperabilität des DPP.

Dreistufiges Zugriffsrechtemodell EN 18239

Ein Produktpass enthält öffentliche Angaben, Daten für autorisierte Wirtschaftsakteure und Daten nur für Behörden; die Norm verlangt, dass diese Ebenen getrennt gehalten und je Datenfeld geregelt wer-

den. Öffentliche Daten müssen ohne Anmeldung erreichbar sein, alles Weitere nur nach Prüfung. EN 18239 befindet sich in der finalen Annahme.

Transpareo führt die Sichtbarkeit als Eigenschaft je Datenfeld: Die öffentliche Ebene wird ohne Authentifizierung ausgeliefert, die höheren Ebenen sind über eine eigene, protokollierte Behördenschnittstelle mit ausschliesslich lesendem Zugriff geschützt, und jeder Zugriff auf geschützte Daten landet im Audit-Log. Das dreistufige Modell der Norm ist damit bereits heute in der Architektur abgebildet, nicht nachträglich aufgesetzt.

Quelle: EN 18239 (Entwurf, in finaler Annahme): «Der Zugriff auf öffentliche Daten muss für EU- und Nicht-EU-Akteure ohne zusätzliche Authentifizierung möglich sein»; kontrollierte Daten erfordern authentifizierten, nachweisbaren Zugriff.

Nachweisbare Datenauthentizität & Integrität EN 18246

Die Norm verlangt, dass Echtheit und Unversehrtheit eines Passes nachweisbar sind und die Prüfung frei und unbegrenzt möglich ist. Vertrauen darf nicht am Fortbestand des Anbieters hängen, sondern muss am Datensatz selbst kleben – sonst wäre jeder Pass nur so glaubwürdig wie die Firma, die ihn gerade hostet. EN 18246 befindet sich in der finalen Annahme.

Transpareo signiert jede veröffentlichte Version mit zwei unabhängigen Schlüsseln (Aussteller und Transpareo) und verkettet die Versionen über ihren Hash, sodass auch die Geschichte nicht unbemerkt umgeschrieben werden kann. Ein quelloffener Renderer prüft beide Signaturen direkt im Browser, ohne einen Server von uns zu kontaktieren – der geforderte signierte, selbstprüfbare Nachweis ist damit bereits umgesetzt.

Quelle: EN 18246 (Entwurf, in finaler Annahme): Authentizität, Verlässlichkeit und Integrität der DPP-Daten müssen nachweisbar sein.

Anbindung an das EU-Kommissionsregister

Jeder registrierungspflichtige Pass muss künftig im zentralen EU-Register eingetragen sein, das eine dauerhafte Registrierungs-ID und einen amtlichen Registrierungsnachweis ausstellt. Die EU hat die technische Schnittstelle dazu noch nicht veröffentlicht – deshalb kann heute kein Anbieter diese Anbindung nachweisen; wo ein Anbieter das behauptet, sollten Sie nachfragen.

Transpareo hat die Anbindung so weit vorbereitet, wie das ohne die Schnittstelle möglich ist: Die dafür nötigen Felder (Registrierungs-ID, stabile Backup-Adresse, Versions-Hash) sind im Datenmodell bereits angelegt. Sobald die EU die Schnittstelle veröffentlicht, aktivieren wir die Registrierung, ohne dass Sie Ihre Pässe umbauen müssen. Bis dahin bleibt dieser Haken offen – bei uns wie bei jedem ehrlichen Anbieter.

Quelle: Entwurf der DPP-Register-Durchführungsverordnung (Ares(2026)4424976).

Aufbewahrung der Registrierungsdaten über die gesetzliche Frist

Registrierte Passdaten müssen über die gesetzliche Frist – in der Regel zehn Jahre ab Registrierung – unverändert verfügbar bleiben, selbst bei Insolvenz oder Geschäftsaufgabe des Herstellers. Die Pflicht überdauert also sowohl Ihren Vertrag mit einem Anbieter als auch den Anbieter selbst.

Transpareo hält dafür ein unveränderbares Archiv, in dem eine einmal geschriebene Version niemand nachträglich ändern oder löschen kann – weder der Hersteller noch wir. Das Archiv greift automatisch mit der EU-Registrierung. Und damit es auch dann erreichbar bleibt, wenn es Transpareo eines Tages nicht mehr gäbe, ist sein Fortbestand über eine notarielle Hinterlegung in der Schweiz abgesichert.

Quelle: DPP-Register-Durchführungsverordnung, Art. 10(3) (Aufbewahrung zehn Jahre).

Produktdaten in den Amtssprachen jedes Zielmarkts

Die Pflichtangaben eines Passes müssen in den Amtssprachen jedes Mitgliedstaats vorliegen, in dem das Produkt auf den Markt kommt – nicht nur in der Sprache des Herstellersitzes. Wer nur den Heimatmarkt bedient, erfüllt die Pflicht für alle anderen Zielmärkte nicht.

Transpareo pflegt jeden Pass mehrsprachig und liefert den Pflichtinhalt in allen 24 EU-Amtssprachen aus. Sie erfassen den Inhalt einmal; die Sprachversionen entstehen daraus, ohne dass Sie pro Sprache zusätzlich zahlen oder separate Pässe pflegen. Der Pass ist damit in jedem Zielmarkt regelkonform lesbar.

Quelle: Batterieverordnung (EU) 2023/1542: Daten in den Amtssprachen der Mitgliedstaaten, in denen das Produkt in Verkehr gebracht wird.

Sprachen über die EU hinaus

Über die gesetzliche Pflicht hinaus hilft es, wenn ein Pass auch Sprachen ausserhalb der EU abdeckt – für Exportmärkte, internationale Handelspartner und Verbraucher, die keine Amtssprache der Union sprechen.

Transpareo pflegt insgesamt 40 Sprachversionen, die 24 EU-Amtssprachen eingeschlossen. Sie erfassen den Inhalt einmal und geben ihn in jeder gewünschten Sprache aus, ohne pro Sprache zusätzlich zu zahlen. Auch die Oberfläche, in der Sie Ihre Pässe pflegen (der Applikations-Manager), ist in alle 40 Sprachen übersetzt, und Sie können Informationen in jeder der verfügbaren Sprachen eingeben.

Versionierung & Änderungshistorie

Ein Pass verändert sich über die Lebensdauer des Produkts; ohne lückenlose Versionsgeschichte lässt sich später nicht belegen, welcher Stand wann galt. Die Norm verlangt deshalb, dass alle Änderungen am Pass archiviert werden.

Transpareo friert jede Veröffentlichung als eigene, signierte Version ein und hält fest, wer sie wann und mit welchen geänderten Feldern erzeugt hat. So bleibt jede Angabe rückwirkend prüfbar, und eine spätere Korrektur überschreibt die Geschichte nicht, sondern setzt sie fort.

Quelle: EN 18221: «Alle Änderungen am Digitalen Produktpass sind zu archivieren.»

Skalierbare Massenanlage für Produktfamilien

Wer viele ähnliche Produkte führt, kann nicht jeden Pass einzeln von Hand anlegen; ein tragfähiges System braucht einen Weg, ganze Produktfamilien auf einmal zu erfassen.

Transpareo lässt Sie Produktdaten per Excel oder CSV hochladen und den Pflichtfeldern zuordnen; für sehr grosse Mengen steht zusätzlich eine Bulk-API bereit, die Pässe programmgesteuert anlegt. Damit skaliert die Anlage von einem Dutzend bis zu Zehntausenden Pässen.

Rollenbasierte interne Rechteverwaltung

Nicht jeder im Unternehmen soll jeden Passinhalt bearbeiten oder freigeben dürfen; die Norm verlangt eine rollenbasierte Rechteverwaltung mit protokollierten Zugriffen.

Transpareo vergibt Rechte je Rolle und Nutzergruppe und protokolliert jede Änderung. Auch Externe wie Werkstätten oder Recycler erhalten nur eng begrenzte, zeitlich befristete Zugänge; Behörden greifen über eine getrennte, ausschliesslich lesende Schnittstelle zu, die jeden Zugriff im Audit-Log markiert.

Quelle: EN 18239 (Entwurf), Zugriffsrechte-Management: regelt, welche Akteure DPP-Daten pflegen und freigeben dürfen.

Aufbewahrung über das Vertragsende hinaus

Die Aufbewahrungspflicht endet nicht mit dem Vertrag: Ein registrierter Pass muss die gesetzliche Frist über bestehen bleiben, auch wenn Sie den Anbieter verlassen. Ein Anbieter, der Pässe mit der Kündigung abschaltet, hinterlässt Ihnen ein Compliance-Problem.

Transpareo trägt das über dasselbe unveränderbare Zehn-Jahres-Archiv wie die Registrierungsdaten - nach einer Kündigung liefert eine dauerhafte Fallback-Adresse die Pässe weiter aus, und die Behördenschnittstelle liest denselben Datensatz aus dem nachvertraglichen Archiv. Bereits gedruckte QR-Codes bleiben gültig.

Quelle: EN 18221: Archivversionen werden auch beim Back-up-Diensteanbieter gespeichert.

Signatur mit eigenem kryptografischen Schlüssel

Wer den privaten Signaturschlüssel hält, kann Pässe im Namen des Ausstellers erzeugen; darum ist es sicherer, wenn der Aussteller diesen Schlüssel selbst behält, statt ihn dem Anbieter anzuvertrauen.

Mit Bring Your Own Key betreibt Ihr Unternehmen einen eigenen Signatur-Endpunkt – Transpareo hält den privaten Schlüssel nie und ergänzt nur eine unabhängige Gegensignatur. So trägt jede Version zwei voneinander unabhängige Signaturen, und Ihre Ausstellersignatur ist eine, die Transpareo selbst nicht erzeugen kann.

Ausstelleridentität unabhängig von der Plattform

Damit ein Prüfer Ihre öffentlichen Schlüssel findet, braucht der Pass eine veröffentlichte Ausstelleridentität. Liegt diese auf der Domain des Anbieters, bindet sie Sie an ihn: Ein Wechsel würde jeden bereits gedruckten Code entwerten.

Transpareo veröffentlicht Ihre Identität als DID:web auf Ihrer eigenen Domain, nicht auf unserer – ein Anbieterwechsel wird damit zu einem DNS-Umzug, und bereits gedruckte Codes samt ihrer Prüfung bleiben gültig. Zusätzlich spiegeln wir jeden öffentlichen Schlüssel zum Zeitpunkt der Veröffentlichung auf eine dauerhafte Adresse, damit jede Version prüfbar bleibt, auch wenn der ursprüngliche Host verschwindet.

Quelle: EN 18219, Abschnitt 4.2.2 (Beständigkeit): Kennungen bleiben über den Lebenszyklus bestehen; Web-Domains sind übertragbar oder umleitbar.

Prüfbarkeit durch Dritte, ganz ohne den Anbieter

Der entscheidende Test für Vertrauen ist, ob ein Dritter den Pass ohne die Infrastruktur des Anbieters prüfen kann. Die Norm verlangt, dass die Prüfung von Gültigkeit und Integrität für den Prüfer kostenlos und ohne Einschränkungen möglich ist.

Transpareo veröffentlicht dafür einen quelloffenen Renderer, der die Bytes einer Version aus beliebiger Quelle lädt, den Hash neu berechnet und beide Signaturen gegen die im Pass genannten öffentlichen Schlüssel prüft – kein Login, kein Anruf bei uns, keine Abhängigkeit von einer laufenden Plattform. Wer misstrauisch ist, kann den Quellcode lesen.

Quelle: EN 18246 (Entwurf): «Die Prüfung von Gültigkeit und Integrität der DPP-Daten muss für den Prüfer kostenlos und ohne Einschränkungen möglich sein.»

Anbieterwechsel ohne Datenverlust

Ein Anbieter, der den Wechsel erschwert, hält Sie über Ihre eigenen Daten fest – und was am Vertragsende mit den Daten geschieht, entscheidet, ob Sie frei wechseln können. Die Norm verlangt deshalb, dass die Daten über ein offenes, interoperables Netz ohne Anbieterbindung übertragbar sind.

Transpareo legt die regulatorischen Passartefakte von vornherein in einem offenen, öffentlich spiegelbaren Bereich ab: Ein einfacher Sync erzeugt eine vollständige, signierte Kopie, die sich gegen die veröffentlichten Schlüssel selbst prüft, ohne Zutun von uns. Das vollständige Ereignisarchiv geben wir über eine signierte, zeitlich begrenzte Download-Adresse an Sie oder Ihren neuen Anbieter, den vorgelager-

ten Produktkatalog zusätzlich als JSON-LD und CSV. Am Vertragsende bleiben die registrierten Pflichtpässe über das unveränderbare Zehn-Jahres-Archiv weiter erreichbar: Öffentliche Spiegelung und Archiv bleiben synchron und übergeben denselben Datenbestand, bereits gedruckte QR-Codes lösen über die dauerhafte Fallback-Adresse weiter auf, und der Registerverweis zeigt auf die neue Adresse. So endet der Vertrag ohne Datenverlust und ohne Bruch der gesetzlichen Aufbewahrung.

Quelle: EN 18216: Daten müssen «über ein offenes, interoperables Netz ohne Anbieterbindung übertragbar» sein.

Anbindung an bestehende Systeme statt Dateninsel

Ein Pass, der nur in der Oberfläche des Anbieters lebt, wird zur Dateninsel neben Ihren übrigen Systemen – jede Änderung muss dann doppelt gepflegt werden.

Transpareo meldet Ereignisse über signierte Webhooks und lässt Daten über eine Bulk-API ein- und auslesen, sodass Sie den Pass an Ihre eigene Systemlandschaft anbinden können. Einen vorgefertigten Konnektor für ein bestimmtes ERP-System liefern wir bewusst nicht – die offenen, signierten Schnittstellen passen zu jedem System, statt eines zu bevorzugen.

Batch-Import & -Export über die reine EU-Pflicht hinaus

Wer die erfassten Daten auch ausserhalb des Passes nutzen will, braucht Import und Export für mehr als nur die gesetzlichen Pflichtfelder.

Transpareo nimmt grössere Datenmengen über Excel, CSV und die Bulk-API entgegen und gibt sie im selben Umfang wieder aus. So dient das System nicht nur der Erfüllung der EU-Pflicht, sondern auch Ihrer eigenen Datenhaltung.

Separate Datenbank und eigener Schlüssel

In einer geteilten Datenbank hängen Ihre Daten mit denen anderer Kunden zusammen; eine saubere, nachweisbare Trennung ist dann kaum möglich – und das Recht auf Löschung nach DSGVO Art. 17 lässt sich schwer belegen.

Bei Transpareo liegt jeder Kunde in einer eigenen Datenbank, verschlüsselt mit einem eigenen Schlüssel – die Trennung besteht auf Datenbank- und auf Verschlüsselungsebene. Das erfüllt das Recht auf Löschung durch verifizierbare Löschung; das Hosting liegt in Deutschland, und der Auftragsverarbeitungsvertrag (AVV) ist inklusive.

Quelle: DSGVO Art. 17 (Recht auf Löschung), erfüllt durch getrennte Datenbank, eigenen Schlüssel und verifizierbare Löschung.

Verschlüsselung und Backups

Ein Anbieter muss Daten bei der Übertragung und im Ruhezustand schützen und gegen Ausfall sichern; die DSGVO verlangt dafür dem Stand der Technik entsprechende Massnahmen.

Transpareo verschlüsselt alle Verbindungen mit TLS und sensible Anwendungsdaten mit AES. Die Backups sind GPG-verschlüsselt, werden mit regelmässiger Schlüsselrotation erneuert, alle vier Stunden erstellt und zwölf Monate lang auf einem separaten Server aufbewahrt.

Quelle: DSGVO Art. 32 (Sicherheit der Verarbeitung): TLS, AES und verschlüsselte Backups mit Rotation.

Sicherheits-Ereignisprotokoll

Sicherheitsrelevante Ereignisse müssen nachvollziehbar bleiben – wer sich wann angemeldet hat und wie Schlüssel genutzt wurden. Die NIS-2-Richtlinie verlangt entsprechende Audit-Logs.

Transpareo führt ein Sicherheits-Ereignisprotokoll über Login-Versuche, MFA-Challenges und API-Schlüssel-Aktivität und bewahrt es ein Jahr lang auf. Damit sind die NIS-2-Anforderungen an Audit-Logs erfüllt.

Quelle: NIS-2-Richtlinie (Anforderungen an Audit-Logs): protokollierte Sicherheitsereignisse, ein Jahr Aufbewahrung.

Mehrfaktor-Authentifizierung

Ein einzelnes Passwort schützt einen Zugang nur schwach; die NIS-2-Richtlinie verlangt Zugangskontrolle mit Mehrfaktor-Authentifizierung.

Transpareo bietet Mehrfaktor-Authentifizierung für alle Nutzer des Applikations-Managers – per Authenticator-App, Passkey oder Hardware-Schlüssel – samt Backup-Codes für den Verlustfall. Die MFA-Pflicht lässt sich für Ihr Konto erzwingen.

Quelle: NIS-2-Richtlinie (Zugangskontrolle und Multi-Faktor-Authentifizierung).

ISO 27001-zertifiziertes Hosting in Deutschland

Wo die Server stehen und wie das Rechenzentrum abgesichert ist, entscheidet über die physische Sicherheit Ihrer Daten – und darüber, welchem Recht sie unterliegen.

Transpareo hostet auf ISO-27001-zertifizierten Servern in Deutschland, mit strengen physischen und organisatorischen Sicherheitsmassnahmen. Der Standort Deutschland hält Ihre Daten zudem vollständig unter europäischem Recht.

Quelle: ISO/IEC 27001 (Informationssicherheits-Management), zertifiziertes Rechenzentrum in Deutschland.

Übernimmt der Anbieter die EU-Registrierung für Sie?

Die Eintragung ins EU-Register samt Einholung des amtlichen Nachweises ist wiederkehrender Aufwand, den ein Anbieter für Sie übernehmen kann. Die Register-Verordnung sieht das ausdrücklich vor: Ein Dienstleister darf die Registrierung im Auftrag übernehmen, die rechtliche Verantwortung bleibt beim Wirtschaftsakteur.

Transpareo registriert Ihre Pässe in Ihrem Auftrag, sobald die EU die technische Schnittstelle veröffentlicht – Sie bleiben rechtlich verantwortlicher Wirtschaftsakteur, tragen aber den operativen Aufwand nicht. Bis die Schnittstelle vorliegt, kann diesen Dienst niemand erbringen; wir haben die dafür nötigen Daten bereits vorbereitet.

Quelle: DPP-Register-Durchführungsverordnung (Entwurf), Art. 19: Die Registrierung kann ein Dienstleister im Auftrag übernehmen; die Verantwortung bleibt beim Wirtschaftsakteur.

Klare Regelung für Supportaufwand und Supportkosten

Manche Anbieter trennen die Nutzung vom Support und stellen Hilfe gesondert in Rechnung; unter dem Strich wird die Zusammenarbeit dadurch schwer kalkulierbar.

Bei Transpareo ist der Support Teil des Tarifs – kein separater Supportvertrag, keine nach Aufwand abgerechneten Zusatzstunden. Was Sie an Betreuung brauchen, ist im ausgewiesenen Preis bereits enthalten.

Transparente Preisstruktur

Eine Preisstruktur, die erst im Verkaufsgespräch sichtbar wird oder pro Sprache, Produkt und Schnittstellenaufbau nachberechnet, macht die tatsächlichen Kosten unvorhersehbar.

Transpareo veröffentlicht vier Tarife für jede Unternehmensgrösse offen auf der Website, mit kostenloser Testphase und jederzeitiger Kündigung. Es gibt keine versteckten Zusatzkosten pro Sprache, Produkt oder Schnittstellenaufbau – der ausgewiesene Preis ist der Preis.