

Fișă comparativă a furnizorilor DPP

Se bifează doar funcțiile deja existente și verificabile – nu și anunțurile sau declarațiile de intenție.

Coloana „Transpareo” este completată automat; cele două coloane goale le completați dumneavoastră atunci când verificați alți furnizori. Explicațiile și sursele pentru fiecare criteriu se găsesc la sfârșitul documentului.

Situația la data de: 10.09.2026

Obligatoriu prin lege

Criteriu	Transpareo		
Schimbul de date într-un format deschis și standardizat Datele din pașaport sunt accesibile prin standarde deschise – pot fi citite de orice sistem autorizat, nu doar de software-ul unui singur furnizor. EN 18216	☒	☐	☐
Identificator unic și portabil, independent de furnizor Codul de identificare al produsului aparține produsului, nu platformei – în cazul schimbării furnizorului, cardul își păstrează identitatea. EN 18219	☒	☐	☐
Suport fizic de date, care poate fi citit pe termen lung Codul QR de pe produs redirecționează către Pass în orice browser – fără aplicație, fără cont, de pe orice smartphone. EN 18220	☒	☐	☐
Stocare și arhivare pe durata minimă de valabilitate Fiecare versiune publicată rămâne disponibilă pe durata prevăzută de lege – inclusiv versiunile mai vechi, nu doar cea actuală. EN 18221	☒	☐	☐

Criteriu	Transpareo		
API pentru gestionarea ciclului de viață și căutabilitate O interfață de programare citește, creează și caută în pașapoarte - nu este doar o interfață web pe care să dai clic. EN 18222	☒	☐	☐
Model de date interoperabil Datele din pașaport respectă un model comun, care poate fi citit de alte sisteme fără a fi necesară reformatarea. EN 18223	☒	☐	☐
Model de drepturi de acces în trei niveluri Datele publice, autorizate și administrative sunt clar separate - fiecare vede exact ceea ce are dreptul să vadă. EN 18239	☒	☐	☐
Autenticitatea și integritatea verificabile ale datelor Fiecare versiune este semnată de două ori și poate fi verificată în browser - fără a fi nevoie să aveți încredere în noi, doar pe baza datelor. EN 18246	☒	☐	☐
Conectarea la registrul Comisiei Europene Înregistrarea, însoțită de un document oficial de atestare - imediat ce UE va publica interfața tehnică. Aceasta nu este încă disponibilă, așa că niciun furnizor nu poate îndeplini această cerință în prezent.	☐	☐	☐
Păstrarea datelor de înregistrare peste termenul prevăzut de lege O arhivă imuabilă pe zece ani - nici producătorul, nici Transpareo nu pot modifica o versiune ulterior.	☒	☐	☐
Date despre produse în limbile oficiale ale fiecărei piețe țintă Informațiile obligatorii sunt publicate în limbile oficiale ale fiecărei țări în care se comercializează produsul - în cazul distribuției la nivelul UE, adică în toate cele 24 de limbi oficiale, nu doar pe piața internă.	☒	☐	☐

Util pentru funcționarea unei baze de date DPP

Criteriu	Transpareo		
Limbi dincolo de granițele UE 16 limbi suplimentare, pe lângă cele 24 de limbi oficiale ale UE - 40 în total, pentru piețele țintă din afara Uniunii.	☒	☐	☐
Versiuni și istoricul modificărilor Fiecare modificare generează o versiune nouă, trasabilă, care include data și autorul - pe întreaga durată a ciclului de viață al produsului.	☒	☐	☐
Instalație de producție în serie scalabilă pentru familii de produse Încărcați datele despre produse în format Excel sau CSV și atribuiți-le câmpurilor obligatorii - pentru cantități mari, aveți la dispoziție și o API pentru import în bloc.	☒	☐	☐
Gestionarea drepturilor interne pe bază de roluri Există reguli clare privind persoanele din cadrul companiei care au dreptul să gestioneze sau să partajeze anumite date, inclusiv accesul strict limitat și temporar acordat persoanelor externe.	☒	☐	☐
Păstrarea datelor după expirarea contractului Dacă vă dezabonați, pașapoartele pe care le-ați publicat vor rămâne accesibile în arhiva inalterabilă pe o perioadă de zece ani.	☒	☐	☐
Semnătură cu cheie criptografică proprie „Bring Your Own Key”: Dumneavoastră dețineți cheia privată, iar noi adăugăm doar o contrasemnătură independentă.	☒	☐	☐
Identitatea expozantului, independentă de platformă Identitatea dumneavoastră de expozant, sub forma DID:web, se află pe propriul dumneavoastră domeniu, nu pe al nostru - schimbarea furnizorului se traduce printr-o migrare DNS.	☒	☐	☐
Verificabilitatea de către terți, fără implicarea furnizorului Un motor de randare cu sursă deschisă verifică valorile hash și semnăturile direct în browser - fără a contacta vreun server al nostru.	☒	☐	☐

Funcții suplimentare dorite

Criteriu	Transpareo		
Schimbarea furnizorului fără pierderea datelor La schimbare, preluați întregul stoc de pașapoarte în formate deschise – semnate și verificabile automat; la expirarea contractului, pașapoartele obligatorii rămân accesibile în arhiva de zece ani, care nu poate fi modificată, fără pierderi de date.	☒	☐	☐
Integrare cu sistemele existente, în loc de insule de date Webhook-urile semnate și o API de procesare în bloc integrează Pass în sistemele dumneavoastră – nu există un conector predefinit pentru un anumit sistem ERP.	☒	☐	☐
Importul și exportul în bloc, dincolo de cerințele obligatorii ale UE Volumele mari de date pot fi transferate în ambele sensuri – nu doar câmpurile obligatorii.	☒	☐	☐

Securitate și protecția datelor

Criteriu	Transpareo		
Bază de date separată și cheie proprie Datele dumneavoastră sunt stocate într-o bază de date separată, criptate cu o cheie proprie – separat atât la nivelul bazei de date, cât și la nivelul criptării.	☒	☐	☐
Criptare și copii de siguranță TLS pentru toate conexiunile, criptarea datelor sensibile cu AES și copii de rezervă criptate cu rotație a cheilor.	☒	☐	☐
Jurnalul evenimentelor de securitate Încercările de autentificare, solicitările de autentificare multifactorială (MFA) și activitatea legată de cheile API sunt înregistrate și păstrate timp de un an.	☒	☐	☐

Criteriu	Transpareo		
Autentificare multifactorială Aplicație de autentificare, cheie de acces sau cheie hardware pentru toți utilizatorii, cu coduri de rezervă în caz de pierdere.	☒	☐	☐
Servicii de găzduire certificate ISO 27001 în Germania Servere situate în Germania, dotate cu măsuri stricte de securitate fizică și organizațională.	☒	☐	☐

Aspecte economice și organizatorice

Criteriu	Transpareo		
Furnizorul se ocupă de înregistrarea în UE în numele dumneavoastră? Ne ocupăm noi de înregistrare, inclusiv de obținerea certificatului oficial, imediat ce UE va publica interfața – astfel, dumneavoastră nu veți avea niciun efort de depus.	☒	☐	☐
Reglementări clare privind efortul și costurile de asistență La Transpareo, asistența tehnică este inclusă în preț – nu este necesar un contract separat de asistență și nu există costuri suplimentare.	☒	☐	☐
Structură transparentă a prețurilor Patru tarife publice pentru orice dimensiune a companiei, perioadă de probă gratuită, posibilitatea de a rezilia contractul în orice moment – fără costuri suplimentare ascunse pe limbă, produs sau apel API.	☒	☐	☐

Explicații și surse

Schimbul de date într-un format deschis și standardizat **EN 18216**

Standardul prevede ca pașapoartele digitale ale produselor să fie accesibile prin protocoale deschise și standardizate – astfel încât autoritățile, partenerii și propriile dumneavoastră sisteme să poată citi

datele fără a fi dependente de software-ul unui furnizor. Un format proprietar ar fi o „insulă”: fără furnizor, nu ați mai avea acces la propriile date. Standardul este publicat în Jurnalul Oficial al UE începând cu 15 iulie 2026 (Decizia de punere în aplicare (UE) 2026/1736) și beneficiază astfel de prezumția de conformitate cu ESPR.

Transpareo furnizează toate datele de trecere și interfețele prin HTTPS standard, într-un format structurat și lizibil de către mașini – fără software special, fără protocoale proprietare. Fiecare versiune publicată este, de asemenea, semnată digital, astfel încât destinatarul nu numai că poate citi datele, ci și poate verifica dacă acestea sunt intacte. Ceea ce vedeți în interfață este același set de date pe care orice sistem autorizat îl preia prin intermediul interfețelor deschise.

Sursă: EN 18216, Cerințe privind protocoalele de schimb de date: „Pentru accesul standardizat la DPP trebuie utilizate protocoalele de schimb de date stabilite.”

Identificator unic și portabil, independent de furnizor EN 18219

Fiecare pașaport de produs trebuie să aibă un identificator unic, care să se refere în mod permanent la același produs și care să nu depindă de un anumit furnizor. Dacă un furnizor leagă identificatorul de propria sa infrastructură, în cazul unei schimbări veți pierde identitatea pașapoartelor dumneavoastră – fiecare cod tipărit și fiecare înregistrare ar deveni atunci fără sens. Standardul este publicat în Jurnalul Oficial al UE începând cu 15 iulie 2026.

Transpareo atribuie identificatorul sub forma unui GS1 Digital Link asociat cu GTIN-ul dumneavoastră – un standard industrial deschis care aparține produsului, nu platformei – și verifică fiecare identificator în raport cu schemele standardizate aprobate. Identitatea semnăturii se află sub forma DID:web pe propriul dumneavoastră domeniu, nu pe al nostru. Identificatorul rămâne valabil chiar și în cazul în care un sistem se defectează: o adresă de rezervă permanentă continuă să îl rezolve, iar „pașaportul” își păstrează identitatea indiferent de schimbarea furnizorului.

Sursă: EN 18219, secțiunea 4.6.2(3): „Identificatorul unic nu trebuie să conducă la o legătură cu un anumit furnizor.”

Suport fizic de date, care poate fi citit pe termen lung EN 18220

Certificatul trebuie să fie accesibil prin intermediul unui suport de date lizibil automat, pe care oricine îl poate accesa fără software special – și care rămâne lizibil pe întreaga durată de viață a produsului, chiar și după utilizare și reparații. Un suport de date care necesită o anumită aplicație sau un cont exclude o parte din public. Standardul este menționat în Jurnalul Oficial al UE începând cu 15 iulie 2026.

Transpareo generează un cod QR conform standardului ISO/IEC 18004, care conține o adresă GS1 Digital Link și care, în orice browser, redirecționează direct către pașaport – fără autentificare, fără descărcare, pe orice smartphone. Modelul, lotul și articolul sunt deja incluse în adresa codificată, astfel încât o scanare duce direct la nivelul corect. Deoarece adresa rămâne stabilă datorită unei rezoluții de

rezervă permanente, un cod tipărit o singură dată rămâne valabil pe întreaga durată de viață a produsului.

Sursă: EN 18220, Cerințe privind suporturile de date (secțiunea 5): simboluri, codificare, calitatea tipăririi și durabilitate; suportul de date trebuie să rămână lizibil chiar și după mai multe cicluri de utilizare și reparații.

Stocare și arhivare pe durata minimă de valabilitate EN 18221

Standardul prevede ca un document, împreună cu istoricul versiunilor sale, să fie stocat pe durata prevăzută de reglementări și să rămână accesibil fără modificări. Dacă se păstrează doar versiunea actuală, se pierde trasabilitatea datelor anterioare – tocmai aceasta fiind însă ceea ce un operator economic trebuie să poată demonstra în fața autorităților. Perioada de păstrare se stabilește în conformitate cu legislația specifică sectorului, fiind însă de cel puțin zece ani. Standardul este menționat în Jurnalul Oficial al UE începând cu 15 iulie 2026.

Transpareo înregistrează fiecare publicare sub forma unei versiuni „înghețate” și semnate într-o arhivă nemodificabilă, în care nimeni nu o mai poate modifica sau șterge ulterior – nici dumneavoastră, nici noi. Versiunile mai vechi rămân disponibile alături de cea actuală, iar fiecare versiune poartă un timbru temporal și o semnătură. Astfel, se poate dovedi pentru orice moment ce informații conținea pașaportul la momentul respectiv.

Sursă: EN 18221: „Pașaportul digital al produsului trebuie să fie pus la dispoziția utilizatorilor autorizați pe toată durata de viață a acestuia.”

API pentru gestionarea ciclului de viață și căutabilitate EN 18222

Pe lângă afișarea în browser, standardul impune existența unei interfețe de programare prin care pașapoartele să poată fi create, citite, actualizate și căutate pe baza codurilor de identificare ale produselor. Fără o astfel de interfață, orice procesare în masă rămâne o operațiune manuală, iar alte sisteme nu pot utiliza automat baza de date a pașapoartelor. Standardul este publicat în Jurnalul Oficial al UE începând cu 15 iulie 2026.

Transpareo pune în aplicare metodele prevăzute de standard printr-o interfață standardizată și cu versiuni: Pașapoartele pot fi create, citite, actualizate și căutate pagină cu pagină pe baza codurilor de identificare ale produsului, prin intermediul unui program. Pașaportul semnat este livrat neschimbat – interfața furnizează exact acei octeți a căror semnătură poate fi verificată de un controlor.

Sursă: EN 18222: interfață de programare standardizată (API) pentru gestionarea ciclului de viață și asigurarea posibilității de căutare a DPP, conform cerințelor ESPR.

Model de date interoperabil EN 18223

Pentru ca pașapoartele să fie compatibile între sisteme și de-a lungul lanțurilor de aprovizionare, standardul impune un model comun de date cu semnificații uniforme ale câmpurilor. Un model propriu al unui furnizor obligă fiecare partener să realizeze propria traducere – iar fiecare traducere reprezintă o sursă de erori. Standardul este menționat în Jurnalul Oficial al UE începând cu 15 iulie 2026.

Transpareo se bazează pe un strat de vocabular orizontal cu vocabulare tehnice paralele și recunoscute (GSI, EPCIS și altele) și descrie fiecare punct de date cu referire la dicționarul său și la tipul său de date. Astfel, un sistem receptor află nu doar cum se numește un câmp, ci și ce înseamnă acesta – pașaportul rămâne lizibil fără a fi necesară reformatarea.

Sursă: EN 18223: model semantic comun de date pentru interoperabilitatea sistemelor din cadrul DPP.

Model de drepturi de acces în trei niveluri EN 18239

Un pașaport al produsului conține informații publice, date destinate operatorilor economici autorizați și date destinate exclusiv autorităților; standardul impune ca aceste niveluri să fie menținute separate și reglementate pentru fiecare câmp de date în parte. Datele publice trebuie să fie accesibile fără autentificare, iar restul datelor numai după verificare. Standardul EN 18239 se află în faza finală de adoptare.

Transpareo gestionează vizibilitatea ca o caracteristică specifică fiecărui câmp de date: nivelul public este disponibil fără autentificare, nivelurile superioare sunt protejate printr-o interfață proprie, înregistrată, destinată autorităților, cu acces exclusiv în citire, iar fiecare acces la datele protejate este consemnat în jurnalul de audit. Modelul pe trei niveluri al standardului este astfel deja integrat în arhitectură, nefiind implementat ulterior.

Sursă: EN 18239 (proiect, în faza de adoptare finală): „Accesul la datele publice trebuie să fie posibil pentru actorii din UE și din afara UE fără autentificare suplimentară”; datele controlate necesită un acces autentificat și verificabil.

Autenticitatea și integritatea verificabile ale datelor EN 18246

Standardul impune ca autenticitatea și integritatea unui pașaport să poată fi demonstrate, iar verificarea să fie posibilă în mod liber și nelimitat. Încrederea nu trebuie să depindă de continuitatea furnizorului, ci trebuie să se bazeze pe setul de date în sine – altfel, fiecare pașaport ar fi la fel de credibil ca firma care îl găzduiește în acel moment. EN 18246 se află în faza finală de adoptare.

Transpareo semnează fiecare versiune publicată cu două chei independente (emitentul și Transpareo) și leagă versiunile între ele prin hash-ul lor, astfel încât nici istoricul să nu poată fi modificat fără a fi observat. Un renderer open-source verifică ambele semnături direct în browser, fără a contacta un server al nostru – astfel, dovada semnată și auto-verificabilă solicitată este deja implementată.

Sursă: EN 18246 (proiect, în faza de adoptare finală): Autenticitatea, fiabilitatea și integritatea datelor DPP trebuie să poată fi demonstrate.

Conectarea la registrul Comisiei Europene

În viitor, fiecare pașaport care trebuie înregistrat va trebui să fie înscris în registrul central al UE, care eliberează un cod de înregistrare permanent și un certificat oficial de înregistrare. UE nu a publicat încă interfața tehnică necesară în acest sens – de aceea, în prezent, niciun furnizor nu poate dovedi această conectare; dacă un furnizor susține acest lucru, ar trebui să solicitați clarificări.

Transpareo a pregătit conexiunea în măsura în care este posibil fără această interfață: câmpurile necesare (ID-ul de înregistrare, adresa de rezervă stabilă, hash-ul versiunii) sunt deja create în modelul de date. Imediat ce UE va publica interfața, vom activa înregistrarea, fără ca dumneavoastră să fie nevoie să vă modificați pașapoartele. Până atunci, această opțiune rămâne neactivată – atât la noi, cât și la orice furnizor onest.

Sursă: Proiectul de regulament de punere în aplicare a Registrului DPP (Ares(2026)4424976).

Păstrarea datelor de înregistrare peste termenul prevăzut de lege

Datele de pas înregistrate trebuie să rămână disponibile fără modificări pe durata termenului legal – de regulă zece ani de la înregistrare –, chiar și în cazul insolvenței sau al încetării activității producătorului. Prin urmare, această obligație depășește atât durata contractului dumneavoastră cu un furnizor, cât și existența furnizorului însuși.

Transpareo păstrează în acest scop o arhivă nemodificabilă, în care o versiune odată înregistrată nu poate fi modificată sau ștersă ulterior de nimeni – nici de producător, nici de noi. Arhiva intră automat în vigoare odată cu înregistrarea la nivelul UE. Iar pentru a se asigura că aceasta rămâne accesibilă chiar și în cazul în care Transpareo nu ar mai exista într-o bună zi, continuitatea sa este garantată printr-un depozit notarial în Elveția.

Sursă: Regulamentul de punere în aplicare al Registrului DPP, art. 10 alin. (3) (perioadă de păstrare de zece ani).

Date despre produse în limbile oficiale ale fiecărei piețe țintă

Informațiile obligatorii dintr-un pașaport trebuie să fie disponibile în limbile oficiale ale fiecărui stat membru în care produsul este introdus pe piață – nu doar în limba în care își are sediul producătorul. Cine se adresează doar pieței interne nu îndeplinește această obligație pentru toate celelalte piețe țintă.

Transpareo gestionează fiecare pașaport în mai multe limbi și furnizează conținutul obligatoriu în toate cele 24 de limbi oficiale ale UE. Introduceți conținutul o singură dată; versiunile lingvistice sunt generate automat, fără a fi necesar să plătiți suplimentar pentru fiecare limbă sau să gestionați pașapoarte separate. Astfel, pașaportul este lizibil și conform cu reglementările pe fiecare piață țintă.

Sursă: Regulamentul (UE) 2023/1542 privind bateriile: date în limbile oficiale ale statelor membre în care produsul este introdus pe piață.

Limbi dincolo de granițele UE

Dincolo de obligația legală, este util ca un pașaport să includă și limbi din afara UE – pentru piețele de export, partenerii comerciali internaționali și consumatorii care nu vorbesc nicio limbă oficială a Uniunii.

Transpareo gestionează în total 40 de versiuni lingvistice, inclusiv cele 24 de limbi oficiale ale UE. Introduceți conținutul o singură dată și îl afișați în orice limbă doriți, fără a plăti suplimentar pentru fiecare limbă. De asemenea, interfața în care gestionați pașapoartele (Managerul de aplicații) este tradusă în toate cele 40 de limbi, iar dvs. puteți introduce informații în oricare dintre limbile disponibile.

Versiuni și istoricul modificărilor

Un pașaport suferă modificări pe parcursul ciclului de viață al produsului; fără un istoric complet al versiunilor, nu se poate dovedi ulterior care a fost starea valabilă la un moment dat. Prin urmare, standardul impune ca toate modificările aduse pașaportului să fie arhivate.

Transpareo salvează fiecare publicare ca o versiune separată și semnată și înregistrează cine a generat-o, când și cu ce câmpuri modificate. Astfel, fiecare informație poate fi verificată retroactiv, iar o corectură ulterioară nu suprascrie istoricul, ci îl continuă.

Sursă: EN 18221: „Toate modificările aduse pașaportului digital al produsului trebuie arhivate.”

Instalație de producție în serie scalabilă pentru familii de produse

Cine are în stoc multe produse similare nu poate crea manual fiecare fișă de produs în parte; un sistem viabil are nevoie de o modalitate de a înregistra întregi familii de produse dintr-o singură dată.

Transpareo vă permite să încărcați datele produselor prin Excel sau CSV și să le atribuiți câmpurilor obligatorii; pentru cantități foarte mari, este disponibilă și o API de import în bloc, care creează fișele de produs automat. Astfel, sistemul se poate adapta de la o duzină până la zeci de mii de fișe de produs.

Gestionarea drepturilor interne pe bază de roluri

Nu toți angajații companiei trebuie să aibă dreptul de a edita sau aproba conținutul fiecărui permis; standardul impune o gestionare a drepturilor bazată pe roluri, cu accesuri înregistrate.

Transpareo acordă drepturi în funcție de rol și de grupul de utilizatori și înregistrează fiecare modificare. Chiar și părțile externe, precum atelierele sau firmele de reciclare, primesc doar accesuri strict limitate și temporare; autoritățile accesează sistemul printr-o interfață separată, exclusiv de citire, care înregistrează fiecare acces în jurnalul de audit.

Sursă: EN 18239 (proiect), Gestionarea drepturilor de acces: stabilește care sunt actorii autorizați să gestioneze și să partajeze datele DPP.

Păstrarea datelor după expirarea contractului

Obligația de păstrare nu încetează odată cu încetarea contractului: un pașaport înregistrat trebuie să rămână valabil peste termenul legal, chiar dacă renunțați la furnizor. Un furnizor care dezactivează pașapoartele odată cu rezilierea contractului vă lasă cu o problemă de conformitate.

Transpareo gestionează acest aspect prin aceeași arhivă imuabilă de zece ani ca și datele de înregistrare – după reziliere, o adresă de rezervă permanentă continuă să furnizeze pașapoartele, iar interfața cu autoritățile citește același set de date din arhiva post-contractuală. Codurile QR deja tipărite rămân valabile.

Sursă: EN 18221: Versiunile arhivate sunt stocate și la furnizorul de servicii de backup.

Semnătură cu cheie criptografică proprie

Cel care deține cheia privată de semnătură poate genera pașapoarte în numele emitentului; de aceea, este mai sigur ca emitentul să păstreze el însuși această cheie, în loc să o încredințeze furnizorului.

Cu „Bring Your Own Key”, compania dumneavoastră gestionează propriul punct terminal de semnătură – Transpareo nu deține niciodată cheia privată și adaugă doar o contra-semnătură independentă. Astfel, fiecare versiune poartă două semnături independente una de cealaltă, iar semnătura emitentului este una pe care Transpareo nu o poate genera singură.

Identitatea expozantului, independentă de platformă

Pentru ca un verificator să vă poată găsi cheile publice, pașaportul trebuie să conțină o identitate a emitentului publicată. Dacă aceasta se află pe domeniul furnizorului, vă leagă de acesta: o schimbare ar invalida orice cod deja tipărit.

Transpareo vă publică identitatea sub formă de DID: pe web, pe propriul dumneavoastră domeniu, nu pe al nostru – astfel, schimbarea furnizorului se reduce la o mutare DNS, iar codurile deja tipărite, împreună cu verificarea lor, rămân valabile. În plus, oglindim fiecare cheie publică la momentul publicării pe o adresă permanentă, astfel încât fiecare versiune să rămână verificabilă, chiar și în cazul în care gazda inițială dispare.

Sursă: EN 18219, secțiunea 4.2.2 (Persistență): Identificatorii rămân valabili pe toată durata ciclului de viață; domeniile web pot fi transferate sau redirecționate.

Verificabilitatea de către terți, fără implicarea furnizorului

Testul decisiv pentru încredere este dacă o terță parte poate verifica pașaportul fără a apela la infrastructura furnizorului. Standardul impune ca verificarea valabilității și integrității să fie posibilă pentru verificator fără costuri și fără restricții.

În acest scop, Transpareo publică un renderer cu sursă deschisă, care încarcă octeții unei versiuni din orice sursă, recalculează hash-ul și verifică ambele semnături în raport cu cheile publice menționate în pașaport – fără autentificare, fără a ne contacta, fără a depinde de o platformă activă. Cei care sunt sceptici pot citi codul sursă.

Sursă: EN 18246 (proiect): „Verificarea validității și integrității datelor DPP trebuie să poată fi efectuată de către verificator fără costuri și fără restricții.”

Schimbarea furnizorului fără pierderea datelor

Un furnizor care îngreunează schimbarea vă reține prin intermediul propriilor date – iar ceea ce se întâmplă cu datele la expirarea contractului determină dacă puteți schimba furnizorul în mod liber. Prin urmare, standardul impune ca datele să poată fi transferate printr-o rețea deschisă și interoperabilă, fără a fi legate de un anumit furnizor.

Transpareo stochează de la bun început artefactele de conformitate cu reglementările într-un spațiu deschis, care poate fi oglindit public: o simplă sincronizare generează o copie completă și semnată, care se verifică automat în raport cu cheile publicate, fără intervenția noastră. Vă punem la dispoziție arhiva completă a evenimentelor, prin intermediul unei adrese de descărcare semnate și cu durată limitată, fie dumneavoastră, fie noului dumneavoastră furnizor, iar catalogul de produse anterior este furnizat suplimentar în format JSON-LD și CSV. La expirarea contractului, datele obligatorii înregistrate rămân accesibile în continuare prin intermediul arhivei inalterabile pe zece ani: Oglinda publică și arhiva rămân sincronizate și transmit același set de date, codurile QR deja tipărite continuă să se deschidă prin adresa de rezervă permanentă, iar referința din registru indică noua adresă. Astfel, contractul se încheie fără pierderi de date și fără încălcarea obligațiilor legale de păstrare a datelor.

Sursă: EN 18216: Datele trebuie să poată fi „transmise printr-o rețea deschisă și interoperabilă, fără a fi legate de un anumit furnizor”.

Integrare cu sistemele existente, în loc de insule de date

Un Pass care există doar în interfața furnizorului devine o „insulă de date” separată de restul sistemelor dumneavoastră – fiecare modificare trebuie atunci actualizată de două ori.

Transpareo raportează evenimente prin intermediul unor webhook-uri semnate și permite importul și exportul datelor printr-o API de tip bulk, astfel încât să puteți integra Pass-ul în propria dvs. infrastructură de sisteme. Am ales în mod deliberat să nu furnizăm un conector preconfigurat pentru un

anumit sistem ERP – interfețele deschise și semnate se potrivesc cu orice sistem, în loc să favorizeze unul anume.

Importul și exportul în bloc, dincolo de cerințele obligatorii ale UE

Cei care doresc să utilizeze datele înregistrate și în afara sistemului Pass au nevoie de funcții de import și export care să depășească câmpurile obligatorii prevăzute de lege.

Transpareo preia volume mari de date din Excel, CSV și API-ul Bulk și le redă în același volum. Astfel, sistemul nu servește doar la îndeplinirea obligațiilor impuse de UE, ci și la gestionarea propriilor date.

Bază de date separată și cheie proprie

Într-o bază de date partajată, datele dumneavoastră sunt corelate cu cele ale altor clienți; o separare clară și verificabilă este atunci aproape imposibilă – iar dreptul la ștergere prevăzut la articolul 17 din RGPD este greu de demonstrat.

La Transpareo, fiecare client este stocat într-o bază de date separată, criptată cu o cheie proprie – separarea se realizează atât la nivelul bazei de date, cât și la nivelul criptării. Acest lucru îndeplinește dreptul la ștergere prin ștergere verificabilă; găzduirea se află în Germania, iar contractul de prelucrare a datelor (CPD) este inclus.

Sursă: Articolul 17 din RGPD (dreptul la ștergere), respectat prin utilizarea unei baze de date separate, a unei chei proprii și a unei proceduri de ștergere verificabile.

Criptare și copii de siguranță

Un furnizor trebuie să protejeze datele atât în timpul transmiterii, cât și în starea de repaus, și să le asigure împotriva pierderii; RGPD impune în acest sens măsuri conforme cu stadiul actual al tehnologiei.

Transpareo criptează toate conexiunile cu TLS și datele sensibile ale aplicațiilor cu AES. Copiile de rezervă sunt criptate cu GPG, sunt reînnoite prin rotația periodică a cheilor, sunt create la fiecare patru ore și păstrate timp de douăsprezece luni pe un server separat.

Sursă: Articolul 32 din RGPD (Securitatea prelucrării): TLS, AES și copii de rezervă criptate cu rotație.

Jurnalul evenimentelor de securitate

Evenimentele relevante pentru securitate trebuie să rămână trasabile – cine s-a autentificat, când și cum au fost utilizate cheile. Directiva NIS-2 impune existența unor jurnale de audit corespunzătoare.

Transpareo ține un jurnal de evenimente de securitate privind încercările de autentificare, provocările MFA și activitatea cheilor API și îl păstrează timp de un an. Astfel, sunt îndeplinite cerințele NIS-2 privind jurnalele de audit.

Sursă: Directiva NIS-2 (cerințe privind jurnalele de audit): evenimente de securitate înregistrate, păstrare timp de un an.

Autentificare multifactorială

O singură parolă oferă un nivel redus de protecție a accesului; Directiva NIS-2 impune controlul accesului prin autentificare multifactorială.

Transpareo oferă autentificare multifactorială pentru toți utilizatorii Application Manager – prin aplicația Authenticator, Passkey sau cheie hardware – inclusiv coduri de rezervă în caz de pierdere. Obligația de autentificare multifactorială poate fi aplicată contului dumneavoastră.

Sursă: Directiva NIS-2 (controlul accesului și autentificarea multifactorială).

Servicii de găzduire certificate ISO 27001 în Germania

Locația serverelor și modul în care este securizat centrul de date determină securitatea fizică a datelor dumneavoastră – precum și legislația care se aplică acestora.

Transpareo găzduiește datele pe servere certificate ISO 27001 în Germania, cu măsuri stricte de securitate fizică și organizațională. De asemenea, faptul că se află în Germania înseamnă că datele dumneavoastră sunt supuse în totalitate legislației europene.

Sursă: ISO/IEC 27001 (Managementul securității informațiilor), centru de date certificat în Germania.

Furnizorul se ocupă de înregistrarea în UE în numele dumneavoastră?

Înscrierea în registrul UE, inclusiv obținerea certificatului oficial, reprezintă o sarcină recurentă pe care un furnizor de servicii o poate prelua în numele dumneavoastră. Regulamentul privind registrul prevede în mod expres acest lucru: un furnizor de servicii poate efectua înregistrarea în numele dumneavoastră, însă responsabilitatea juridică revine în continuare operatorului economic.

Transpareo vă înregistrează certificatele în numele dumneavoastră, imediat ce UE va publica interfața tehnică – dumneavoastră rămâneți operatorul economic responsabil din punct de vedere juridic, dar nu suportați efortul operațional. Până la disponibilitatea interfeței, nimeni nu poate presta acest serviciu; noi am pregătit deja datele necesare în acest sens.

Sursă: Regulamentul de punere în aplicare al Registrului DPP (proiect), art. 19: Înregistrarea poate fi efectuată de un prestator de servicii în numele operatorului economic; responsabilitatea revine în continuare operatorului economic.

Reglementări clare privind efortul și costurile de asistență

Unii furnizori separă utilizarea de asistență și facturează separat serviciile de asistență; în final, acest lucru face ca colaborarea să fie greu de estimat din punct de vedere financiar.

La Transpareo, asistența tehnică este inclusă în tarif – fără contract separat de asistență, fără ore suplimentare facturate în funcție de efortul depus. Tot ce aveți nevoie în materie de asistență este deja inclus în prețul afișat.

Structură transparentă a prețurilor

O structură de prețuri care devine vizibilă abia în cadrul discuției de vânzare sau care se calculează ulterior în funcție de limbă, produs și apel de interfață face ca costurile reale să fie imprevizibile.

Transpareo publică în mod transparent pe site-ul său patru tarife pentru fiecare dimensiune a companiei, cu o perioadă de testare gratuită și posibilitatea de reziliere în orice moment. Nu există costuri suplimentare ascunse pe limbă, produs sau apel de interfață – prețul afișat este prețul final.