Transpareo

DPP provider comparison sheet

Only functions that already exist and can be verified receive a tick - no announcements or declarations of intent. The Transpareo column is pre-filled; complete the two blank columns while you evaluate other providers. Details and sources for every criterion are at the end of the document.

As of 13 September 2026

Legally mandatory

Criterion	Transpareo	_____	_____
Data exchange in an open, standardised format The passport data is retrievable through open standards - readable by any authorised system, not only one provider's software. `EN 18216`	☑	☐	☐
Unique, portable identifier without vendor lock-in The product's identifier belongs to the product, not to the platform - the passport keeps its identity if you change provider. `EN 18219`	☑	☐	☐
Physical data carrier, durably readable The QR code on the product opens the passport in any browser - no app, no account, on any smartphone. `EN 18220`	☑	☐	☐
Storage and archiving over the minimum term Every published version stays retrievable for the legally prescribed period - earlier states too, not just the current one. `EN 18221`	☑	☐	☐
API for lifecycle management and searchability A programming interface reads, creates and searches passports - not just a web interface to click through. `EN 18222`	☑	☐	☐

Criterion	Transpareo		
Interoperable data model The passport data follows a shared model that other systems can read without reformatting. `EN 18223`	☑	☐	☐
Three-tier access rights model Public, authorised and authority-only data are cleanly separated - everyone sees exactly what they are entitled to. `EN 18239`	☑	☐	☐
Verifiable data authenticity and integrity Every version is signed twice and can be checked in the browser - trusting the data itself, not us. `EN 18246`	☑	☐	☐
Connection to the EU Commission register Registration including an official proof - as soon as the EU publishes the technical interface. It does not exist yet, so no provider can meet this today.	☐	☐	☐
Retention of registration data over the statutory period An immutable ten-year archive - neither the manufacturer nor Transpareo can change a version after the fact.	☑	☐	☐
Product data in the official languages of each target market The mandatory content appears in the official languages of every country where the product is sold - so for EU-wide sales, all 24 official languages, not just the home market.	☑	☐	☐

Useful for running a DPP database

Criterion	Transpareo		
Languages beyond the EU 16 further languages beyond the 24 EU official languages - 40 in total, for markets outside the Union.	☑	☐	☐

Criterion	Transpareo		
Versioning and change history Every change creates a new, traceable version with timestamp and author - across the whole product lifecycle.	☑	☐	☐
Scalable bulk creation for product families Upload product data via Excel or CSV and map it to the mandatory fields - plus a bulk API for large volumes.	☑	☐	☐
Role-based internal permissions Who in the company may maintain or release which data is governed - including tightly scoped, time-limited access for outsiders.	☑	☐	☐
Retention beyond the end of the contract If you cancel, your published passports stay reachable in the immutable ten-year archive.	☑	☐	☐
Signing with your own cryptographic key Bring Your Own Key: you hold the private key yourself, we only add an independent counter-signature.	☑	☐	☐
Issuer identity independent of the platform Your issuer identity lives as a DID:web on your own domain, not ours - a change of provider becomes a DNS move.	☑	☐	☐
Verifiability by third parties, entirely without the provider An open-source renderer checks the hash and signatures in the browser - without contacting any server of ours.	☑	☐	☐

Desirable extra features

Criterion	Transpareo		
Switching provider without data loss When you move, you take the full passport set in open formats - signed and self-verifying; at contract end the mandatory passports stay reachable in the immutable ten-year archive, with no data loss.	☑	☐	☐

Criterion	Transpareo		
Connection to existing systems instead of a data island Signed webhooks and a bulk API connect the passport to your systems - no ready-made connector for one specific ERP.	☑	☐	☐
Batch import and export beyond the bare EU obligation Larger volumes of data move in both directions - not just the bare mandatory fields.	☑	☐	☐

Security & data protection

Criterion	Transpareo		
Separate database and key Your data sits in its own database, encrypted with its own key - separated at both the database and the encryption level.	☑	☐	☐
Encryption and backups TLS on all connections, AES encryption of sensitive data, and encrypted backups with key rotation.	☑	☐	☐
Security event log Login attempts, MFA challenges and API key activity are logged and kept for one year.	☑	☐	☐
Multi-factor authentication Authenticator app, passkey or hardware key for every user, with backup codes for loss.	☑	☐	☐
ISO 27001-certified hosting in Germany Servers in Germany with strict physical and organisational security measures.	☑	☐	☐

Commercial and organisational questions

Criterion	Transpareo		
Does the provider handle EU registration for you? We handle registration including the official proof as soon as the EU publishes the interface - so it costs you no effort.	☑	☐	☐
A clear rule for support effort and support costs At Transpareo, support is included in the price - no separate support contract, no extra costs.	☑	☐	☐
Transparent pricing structure Four public tariffs for every company size, a free trial, cancel any time - without hidden extra costs per language, product or API call.	☑	☐	☐

Details and sources

Data exchange in an open, standardised format `EN 18216`

The standard requires digital product passports to be accessible over open, standardised protocols - so that authorities, partners and your own systems can read the data without being tied to one provider's software. A proprietary format would be an island: without the provider you could no longer reach your own data. The standard has been cited in the EU Official Journal since 15 July 2026 (Commission Implementing Decision (EU) 2026/1736), carrying the presumption of conformity with the ESPR.

Transpareo delivers all passport data and interfaces over standard HTTPS in structured, machine-readable form - no special software, no proprietary protocols. Every published version is additionally signed, so a recipient can not only read the data but verify that it is unchanged. What you see in the interface is the same record any authorised system retrieves over the open interfaces.

Source: EN 18216, data-exchange-protocol requirement: 'The data exchange protocols specified in this clause shall be used for standardized DPP access.'

Unique, portable identifier without vendor lock-in `EN 18219`

Every passport needs a unique identifier that points to the same product permanently and assumes no particular provider. If a provider ties the identifier to its own infrastructure, you lose the identity of your

passports when you move - every printed code and every registration would then point into the void. The standard has been cited in the EU Official Journal since 15 July 2026.

Transpareo issues the identifier as a GS1 Digital Link carrying your GTIN - an open industry standard that belongs to the product, not the platform - and validates every identifier against the permitted standard schemes. The signing identity lives as a DID:web on your own domain, not ours. The identifier keeps resolving even if a system fails: a permanent fallback address keeps answering, and the passport keeps its identity across any change of provider.

Source: EN 18219, clause 4.6.2(3): 'The unique identifier shall not result in vendor lock-in.'

Physical data carrier, durably readable `EN 18220`

The passport must be reachable through a machine-readable carrier on the product that anyone can open without special software - and that stays readable over the whole product life, including use and repair. A carrier that demands a particular app or account shuts out part of the public. The standard has been cited in the EU Official Journal since 15 July 2026.

Transpareo produces a QR code per ISO/IEC 18004 that carries a GS1 Digital Link address and resolves straight to the passport in any browser - no login, no download, any smartphone. Model, batch and item are already encoded in the address, so a scan lands on the right level directly. Because the address stays stable through a permanent fallback resolution, a code once printed stays valid over the whole product life.

Source: EN 18220, data-carrier requirements (Clause 5): symbology, encoding, print quality and durability; the carrier should remain usable after several use-reuse-repair cycles.

Storage and archiving over the minimum term `EN 18221`

The standard requires a passport and its version history to be stored and kept unchanged and retrievable for the period prescribed by regulation. If only the current state is held, the traceability of earlier entries is lost - yet that is exactly what an economic operator must be able to prove to authorities. The retention period follows the relevant sector law, but at least ten years. The standard has been cited in the EU Official Journal since 15 July 2026.

Transpareo writes every publication as a frozen, signed version into an immutable archive where no one can later change or delete it - neither you nor us. Earlier states stay retrievable alongside the current one, and every version carries a timestamp and signature. For any point in time you can prove what the passport stated back then.

Source: EN 18221: 'The digital product passport shall be available to specifically authorized users ... during the digital product passport lifetime.'

API for lifecycle management and searchability `EN 18222`

Beyond display in the browser, the standard requires a programming interface through which passports can be created, read, updated and searched by product identifier. Without such an interface, every bulk operation stays manual and other systems cannot use the passport inventory automatically. The standard has been cited in the EU Official Journal since 15 July 2026.

Transpareo serves the prescribed standard methods over a versioned, standardised interface: passports can be created, read, updated and searched page by page over product identifiers, programmatically. The signed passport is delivered unchanged - the interface hands out exactly the bytes whose signature a verifier can recompute.

Source: EN 18222: a standardized API for DPP lifecycle management and searchability, as mandated by the ESPR.

Interoperable data model `EN 18223`

So that passports fit together across systems and supply chains, the standard prescribes a shared data model with a common meaning for every field. A provider-specific model forces every partner into its own translation - and every translation is a source of errors. The standard has been cited in the EU Official Journal since 15 July 2026.

Transpareo builds on a horizontal vocabulary layer with parallel, recognised domain vocabularies (GS1, EPCIS and others) and describes each data point with a reference to its dictionary and its data type. A receiving system therefore learns not just what a field is called but what it means - the passport stays readable without reformatting.

Source: EN 18223: a common semantic data model for DPP system interoperability.

Three-tier access rights model `EN 18239`

A product passport holds public entries, data for authorised economic operators and data for authorities only; the standard requires these tiers to be kept apart and governed per data field. Public data must be reachable without any login, everything else only after a check. EN 18239 is in final adoption.

Transpareo carries visibility as a property on each data field: the public tier is served without authentication, the higher tiers are protected through a separate, logged authority interface with read-only access, and every access to protected data lands in the audit log. The standard's three-tier model is already reflected in the architecture, not bolted on afterwards.

Source: EN 18239 (draft, in final adoption): 'Access to public data shall be possible for EU and non-EU actors without additional authentication'; controlled data requires authenticated, non-refutable access.

Verifiable data authenticity and integrity `EN 18246`

The standard requires the authenticity and integrity of a passport to be provable, with verification free and unlimited. Trust must not hang on the provider's survival but must stick to the data record itself - otherwise every passport is only as credible as whichever company currently hosts it. EN 18246 is in final adoption.

Transpareo signs every published version with two independent keys (issuer and Transpareo) and chains the versions by their hash, so even the history cannot be rewritten unnoticed. An open-source renderer checks both signatures right in the browser without contacting any server of ours - the required signed, self-verifying proof is already in place.

Source: EN 18246 (draft, in final adoption): authenticity, reliability and integrity of the DPP data must be demonstrable.

Connection to the EU Commission register

Every passport subject to registration will have to be entered in the central EU register, which issues a permanent registration ID and an official proof of registration. The EU has not yet published the technical interface for this - so no provider can demonstrate this connection today; where one claims otherwise, you should ask.

Transpareo has prepared the connection as far as it can be prepared without the interface: the fields it needs (registration ID, stable backup address, version hash) are already in place in the data model. As soon as the EU publishes the interface, we activate registration without you having to rework your passports. Until then this box stays unticked - with us as with every honest provider.

Source: Draft DPP Register Implementing Regulation (Ares(2026)4424976).

Retention of registration data over the statutory period

Registered passport data must stay available unchanged over the statutory period - usually ten years from registration - even if the manufacturer becomes insolvent or ceases trading. The duty therefore outlives both your contract with a provider and the provider itself.

Transpareo holds an immutable archive for this, in which no one can later change or delete a version once written - neither the manufacturer nor us. The archive takes effect automatically with EU registration. And so that it stays reachable even if Transpareo one day no longer existed, its continuity is secured by a notarial deposit in Switzerland.

Source: DPP Register Implementing Regulation, Art. 10(3) (ten-year retention).

Product data in the official languages of each target market

A passport's mandatory entries must be available in the official languages of every member state where the product is placed on the market - not only in the language of the manufacturer's home country. Serving only the home market leaves the duty unmet for every other target market.

Transpareo maintains each passport in multiple languages and delivers the mandatory content in all 24 EU official languages. You capture the content once; the language versions follow from it, without paying per language or maintaining separate passports. The passport is compliant and readable in every target market.

Source: Battery Regulation (EU) 2023/1542: data in the official languages of the member states where the product is placed on the market.

Languages beyond the EU

Beyond the legal duty, it helps if a passport also covers languages outside the EU - for export markets, international trade partners and consumers who speak no official language of the Union.

Transpareo maintains 40 language versions in total, the 24 EU official languages included. You capture the content once and deliver it in any language you need, without paying extra per language. The interface where you maintain your passports (the application manager) is translated into all 40 languages too, and you can enter information in any of the available languages.

Versioning and change history

A passport changes over the life of the product; without an unbroken version history you cannot later prove which state applied when. The standard therefore requires all changes to the passport to be archived.

Transpareo freezes every publication as its own signed version and records who created it, when, and which fields changed. Every entry stays verifiable in retrospect, and a later correction does not overwrite the history but continues it.

Source: EN 18221: 'All changes to the digital product passport shall be archived.'

Scalable bulk creation for product families

Anyone with many similar products cannot create each passport by hand; a workable system needs a way to capture whole product families at once.

Transpareo lets you upload product data via Excel or CSV and map it to the mandatory fields; for very large volumes a bulk API additionally creates passports programmatically. Creation therefore scales from a dozen to tens of thousands of passports.

Role-based internal permissions

Not everyone in the company should be able to edit or release every passport entry; the standard requires role-based permissions with logged access.

Transpareo assigns rights per role and user group and logs every change. Outsiders such as workshops or recyclers receive only tightly scoped, time-limited access; authorities read through a separate, read-only interface that marks every access in the audit log.

Source: EN 18239 (draft), access-right management: governs which actors may maintain and release DPP data.

Retention beyond the end of the contract

The retention duty does not end with the contract: a registered passport must persist over the statutory period even after you leave the provider. A provider that switches passports off on cancellation leaves you with a compliance problem.

Transpareo carries this through the same immutable ten-year archive as the registration data - after a cancellation a permanent fallback address keeps serving the passports, and the authority interface reads the same record from the post-contract archive. QR codes already printed stay valid.

Source: EN 18221: archived versions are stored by the back-up service provider as well.

Signing with your own cryptographic key

Whoever holds the private signing key can create passports in the issuer's name; that is why it is safer for the issuer to keep that key itself instead of entrusting it to the provider.

With Bring Your Own Key your company runs its own signing endpoint - Transpareo never holds the private key and only adds an independent counter-signature. Every version therefore carries two mutually independent signatures, and your issuer signature is one Transpareo itself cannot produce.

Issuer identity independent of the platform

So that a verifier can find your public keys, the passport needs a published issuer identity. If it lives on the provider's domain, it ties you to that provider: a move would void every code already printed.

Transpareo publishes your identity as a DID:web on your own domain, not ours - a change of provider therefore becomes a DNS move, and codes already printed, along with their verification, stay valid. On top of that we mirror every public key at the moment of publication to a permanent address, so every version stays verifiable even if the original host disappears.

Source: EN 18219, clause 4.2.2 (permanence): identifiers persist across the life cycle; web domains can be transferred or redirected.

Verifiability by third parties, entirely without the provider

The decisive test of trust is whether a third party can check the passport without the provider's infrastructure. The standard requires checking validity and integrity to be free of charge and without limitations for the verifier.

Transpareo publishes an open-source renderer for this, which loads a version's bytes from any source, recomputes the hash and checks both signatures against the public keys named in the passport - no login, no call to us, no dependence on a running platform. Anyone who is suspicious can read the source code.

Source: EN 18246 (draft): 'Checking the validity and the integrity of the data managed by the DPP shall be free of charge and without limitations for the verifier.'

Switching provider without data loss

A provider that makes moving hard holds you captive over your own data - and what happens to your data at the end of the contract decides whether you can move freely. The standard therefore requires data to be transferable through an open, interoperable network without vendor lock-in.

Transpareo places the regulatory passport artefacts from the outset in an open, publicly mirror-friendly area: a simple sync produces a complete, signed copy that verifies itself against the published keys, with nothing needed from us. The full event archive we hand to you or your new provider over a signed, time-limited download address, and the upstream product catalogue additionally as JSON-LD and CSV. At contract end the registered mandatory passports stay reachable through the immutable ten-year archive: the public mirror and the archive stay in sync and hand over the same data set, QR codes already printed keep resolving via the permanent fallback address, and the register reference points to the new address. So the contract ends without data loss and without breaking the statutory retention.

Source: EN 18216: data must be 'transferable through an open, interoperable network without vendor lock-in.'

Connection to existing systems instead of a data island

A passport that lives only in the provider's interface becomes a data island alongside your other systems - every change then has to be maintained twice.

Transpareo reports events over signed webhooks and lets data be read in and out over a bulk API, so you can connect the passport to your own system landscape. We deliberately do not ship a ready-made connector for one specific ERP system - the open, signed interfaces suit any system rather than favouring one.

Batch import and export beyond the bare EU obligation

Anyone who wants to use the captured data outside the passport needs import and export for more than the legal mandatory fields.

Transpareo takes in larger volumes of data via Excel, CSV and the bulk API and gives them back out at the same scope. The system therefore serves not only EU compliance but your own data management too.

Separate database and key

In a shared database your data is entangled with those of other customers; clean, demonstrable separation is then hard to achieve - and the right to erasure under GDPR Art. 17 becomes hard to prove.

At Transpareo each customer sits in its own database, encrypted with its own key - separation exists at both the database and the encryption level. This satisfies the right to erasure through verifiable deletion; hosting is in Germany and the data processing agreement (DPA) is included.

Source: GDPR Art. 17 (right to erasure), met through a separate database, own key and verifiable deletion.

Encryption and backups

A provider must protect data in transit and at rest and guard against loss; the GDPR requires state-of-the-art measures for this.

Transpareo encrypts all connections with TLS and sensitive application data with AES. Backups are GPG-encrypted, renewed with regular key rotation, taken every four hours and kept for twelve months on a separate server.

Source: GDPR Art. 32 (security of processing): TLS, AES and encrypted backups with rotation.

Security event log

Security-relevant events must stay traceable - who logged in when, and how keys were used. The NIS 2 Directive requires audit logs for this.

Transpareo keeps a security event log of login attempts, MFA challenges and API key activity, retained for one year. This meets the NIS 2 requirements for audit logs.

Source: NIS 2 Directive (audit-log requirements): logged security events, one-year retention.

Multi-factor authentication

A single password protects an account only weakly; the NIS 2 Directive requires access control with multi-factor authentication.

Transpareo offers multi-factor authentication for every user of the application manager - via authenticator app, passkey or hardware key - plus backup codes for loss. MFA can be enforced for your account.

Source: NIS 2 Directive (access control and multi-factor authentication).

ISO 27001-certified hosting in Germany

Where the servers sit and how the data centre is secured decides the physical security of your data - and which law it falls under.

Transpareo hosts on ISO 27001-certified servers in Germany, with strict physical and organisational security measures. The German location additionally keeps your data fully under European law.

Source: ISO/IEC 27001 (information security management), certified data centre in Germany.

Does the provider handle EU registration for you?

Entry in the EU register including obtaining the official proof is recurring effort that a provider can take on for you. The Register Regulation provides for this explicitly: a service provider may handle registration on the operator's behalf, while legal responsibility stays with the economic operator.

Transpareo registers your passports on your behalf as soon as the EU publishes the technical interface - you remain the legally responsible economic operator but carry none of the operational effort. Until the interface exists no one can provide this service; we have already prepared the data it needs.

Source: Draft DPP Register Implementing Regulation, Art. 19: registration may be handled by a service provider on the operator's behalf; responsibility stays with the economic operator.

A clear rule for support effort and support costs

Some providers separate usage from support and bill help separately; the collaboration becomes hard to budget as a result.

At Transpareo support is part of the tariff - no separate support contract, no extra hours billed by effort. Whatever support you need is already included in the stated price.

Transparent pricing structure

A pricing structure that only becomes visible in the sales conversation, or bills extra per language, product and API call, makes the true cost unpredictable.

Transpareo publishes four tariffs for every company size openly on the website, with a free trial and cancellation at any time. There are no hidden extra costs per language, product or interface call - the stated price is the price.