

Arkusz porównawczy dostawców DPP

Zaznacza się wyłącznie istniejące, możliwe do zweryfikowania funkcje – nie uwzględnia się zapowiedzi ani deklaracji intencyjnych. Kolumna „Transpareo” jest wstępnie wypełniona; dwie puste kolumny należy wypełnić podczas sprawdzania innych dostawców. Objasnienia i źródła dotyczące każdego kryterium znajdują się na końcu dokumentu.

Stan na dzień: 10.09.2026

Wymagane przez prawo

Kryterium	Transpareo		
Wymiana danych w otwartym, znormalizowanym formacie Dane dotyczące paszportów są dostępne w oparciu o otwarte standardy – są one czytelne dla każdego uprawnionego systemu, a nie tylko dla oprogramowania jednego dostawcy. EN 18216	☒	☐	☐
Jednoznaczny, przenośny identyfikator niezależny od dostawcy Identyfikator produktu jest powiązany z produktem, a nie z platformą – w przypadku zmiany dostawcy identyfikator pozostaje niezmienny. EN 18219	☒	☐	☐
Nośnik fizyczny, umożliwiający trwały odczyt Kod QR umieszczony na produkcie otwiera profil w każdej przeglądarce – bez aplikacji, bez konta, na każdym smartfonie. EN 18220	☒	☐	☐

Kryterium	Transpareo		
Przechowywanie i archiwizacja przez okres dłuższy niż minimalny Każda opublikowana wersja pozostaje dostępna przez okres przewidziany przepisami prawa – dotyczy to również starszych wersji, a nie tylko aktualnej. EN 18221	☒	☐	☐
API do zarządzania cyklem życia i przeszukiwalnością Interfejs programistyczny odczytuje, tworzy i przeszukuje paszporty – to nie tylko interfejs internetowy, w którym wystarczy klikać. EN 18222	☒	☐	☐
Model danych zapewniający interoperacyjność Dane paszportowe są zgodne ze wspólnym modelem, który umożliwia odczytanie ich przez inne systemy bez konieczności zmiany formatu. EN 18223	☒	☐	☐
Trzystopniowy model uprawnień dostępu Dane publiczne, autoryzowane i urzędowe są wyraźnie rozdzielone – każdy widzi dokładnie to, do czego ma uprawnienia. EN 18239	☒	☐	☐
Weryfikowalna autentyczność i integralność danych Każda wersja jest podwójnie podpisana i można ją zweryfikować w przeglądarce – bez konieczności ufać nam, wyłącznie na podstawie danych. EN 18246	☒	☐	☐
Połączenie z rejestrem Komisji Europejskiej Rejestracja wraz z urzędowym potwierdzeniem – gdy tylko UE opublikuje interfejs techniczny. Na razie nie jest on jeszcze dostępny, więc żaden dostawca nie jest w stanie spełnić tego wymogu.	☐	☐	☐
Przechowywanie danych rejestracyjnych po upływie terminu przewidzianego przepisami Niezmiennie archiwum obejmujące okres dziesięciu lat – ani producent, ani firma Transpareo nie mogą później wprowadzać zmian w żadnej wersji.	☒	☐	☐

Kryterium	Transpareo		
Dane dotyczące produktów w językach urzędowych każdego rynku docelowego Obowiązkowe informacje są zamieszczane w językach urzędowych każdego kraju, w którym produkt jest sprzedawany – w przypadku dystrybucji na terenie całej UE oznacza to wszystkie 24 języki urzędowe, a nie tylko język rynku krajowego.	☒	☐	☐

Przydatne do obsługi bazy danych DPP

Kryterium	Transpareo		
Języki poza UE 16 dodatkowych języków poza 24 językami urzędowymi UE – łącznie 40, przeznaczonych dla rynków docelowych poza Unią.	☒	☐	☐
Wersje i historia zmian Każda zmiana generuje nową, identyfikowalną wersję wraz z datą i autorem – w całym cyklu życia produktu.	☒	☐	☐
Skalowalna instalacja masowa dla rodzin produktów Prześlij dane produktów w formacie Excel lub CSV i przypisz je do pól obowiązkowych – w przypadku dużych ilości dostępny jest dodatkowo interfejs API do obsługi zbiorczej.	☒	☐	☐
Wewnętrzne zarządzanie uprawnieniami oparte na rolach W firmie obowiązują zasady określające, kto może aktualizować lub udostępniać dane – w tym ściśle ograniczone, czasowe uprawnienia dostępu dla osób z zewnątrz.	☒	☐	☐
Przechowywanie po wygaśnięciu umowy Jeśli zrezygnujesz, Twoje opublikowane paszporty pozostaną dostępne w niezmiennym archiwum obejmującym okres dziesięciu lat.	☒	☐	☐

Kryterium	Transpareo		
Podpis przy użyciu własnego klucza kryptograficznego Bring Your Own Key: To Państwo przechowują klucz prywatny, a my dodajemy jedynie niezależny podpis potwierdzający.	☒	☐	☐
Tożsamość wystawcy niezależna od platformy Twoja tożsamość wystawcy jako DID:web znajduje się na Twojej własnej domenie, a nie na naszej - zmiana dostawcy oznacza przeniesienie DNS.	☒	☐	☐
Możliwość weryfikacji przez osoby trzecie, całkowicie bez udziału dostawcy Renderer oparty na kodzie otwartym weryfikuje skróty i podpisy w przeglądarce - bez nawiązywania połączenia z naszym serwerem.	☒	☐	☐

Pożądane funkcje dodatkowe

Kryterium	Transpareo		
Zmiana dostawcy bez utraty danych W momencie zmiany dostawcy zabierają Państwo ze sobą kompletną bazę paszportów w otwartych formatach - podpisanych i umożliwiającą samodzielną weryfikację; po wygaśnięciu umowy obowiązkowe paszporty pozostają dostępne w niezmiennym archiwum dziesięcioletnim, bez utraty danych.	☒	☐	☐
Integracja z istniejącymi systemami zamiast izolowanych baz danych Podpisane webhooki i interfejs API do obsługi operacji zbiorczych umożliwiają integrację Pass z Państwa systemami - nie jest to gotowy łącznik przeznaczony dla konkretnego systemu ERP.	☒	☐	☐
Import i eksport zbiorczy wykraczający poza czyste wymogi UE Duże ilości danych można przenosić w obu kierunkach - nie tylko same pola obowiązkowe.	☒	☐	☐

Bezpieczeństwo i ochrona danych

Kryterium	Transpareo		
Oddzielna baza danych i własny klucz Państwa dane są przechowywane w osobnej bazie danych, zaszyfrowane za pomocą własnego klucza - z zachowaniem oddzielności na poziomie bazy danych i szyfrowania.	☒	☐	☐
Szyfrowanie i kopie zapasowe Protokół TLS dla wszystkich połączeń, szyfrowanie danych wrażliwych za pomocą algorytmu AES oraz szyfrowane kopie zapasowe z rotacją kluczy.	☒	☐	☐
Dziennik zdarzeń bezpieczeństwa Próby logowania, wyzwania związane z uwierzytelnianiem wieloskładnikowym (MFA) oraz aktywność związana z kluczami API są rejestrowane i przechowywane przez rok.	☒	☐	☐
Uwierzytelnianie wieloskładnikowe Aplikacja uwierzytelniająca, klucz dostępu lub klucz sprzętowy dla wszystkich użytkowników, wraz z kodami zapasowymi na wypadek utraty.	☒	☐	☐
Hosting z certyfikatem ISO 27001 w Niemczech Serwer w Niemczech, na którym stosowane są rygorystyczne fizyczne i organizacyjne środki bezpieczeństwa.	☒	☐	☐

Kwestie gospodarcze i organizacyjne

Kryterium	Transpareo		
Czy dostawca zajmuje się rejestracją w UE w Twoim imieniu? Zajmiemy się rejestracją wraz z uzyskaniem urzędowego zaświadczenia, gdy tylko UE opublikuje interfejs - nie wiąże się to dla Państwa z żadnym wysiłkiem.	☒	☐	☐

Kryterium	Transpareo		
Jasne zasady dotyczące nakładu pracy i kosztów związanych z obsługą techniczną W firmie Transpareo wsparcie techniczne jest wliczone w cenę – nie ma oddzielnej umowy serwisowej ani dodatkowych kosztów.	☒	☐	☐
Przejrzysta struktura cenowa Cztery publiczne plany taryfowe dostosowane do każdej wielkości firmy, bezpłatny okres próbny, możliwość wypowiedzenia w dowolnym momencie – bez ukrytych dodatkowych kosztów związanych z językiem, produktem czy wywołaniem API.	☒	☐	☐

Objaśnienia i źródła

Wymiana danych w otwartym, znormalizowanym formacie EN 18216

Norma wymaga, aby cyfrowe paszporty produktów były dostępne za pośrednictwem otwartych, znormalizowanych protokołów – tak aby organy administracji, partnerzy oraz Państwa własne systemy mogły odczytywać dane bez konieczności korzystania z oprogramowania konkretnego dostawcy. Format zastrzeżony stanowiłby „wyspę”: bez dostawcy nie miałoby Państwo już dostępu do własnych danych. Norma została opublikowana w Dzienniku Urzędowym UE 15 lipca 2026 r. (decyzja wykonawcza (UE) 2026/1736) i tym samym objęta jest domniemaniem zgodności z rozporządzeniem ESPR.

Transpareo dostarcza wszystkie dane paszportowe i interfejsy za pośrednictwem standardowego protokołu HTTPS w ustrukturyzowanej, nadającej się do odczytu maszynowej formie – bez specjalistycznego oprogramowania, bez zastrzeżonych protokołów. Każda opublikowana wersja jest dodatkowo podpisana, dzięki czemu odbiorca może nie tylko odczytać dane, ale także sprawdzić, czy nie zostały one zmienione. To, co widzisz w interfejsie, to ten sam zestaw danych, który każdy uprawniony system pobiera za pośrednictwem otwartych interfejsów.

Źródło: EN 18216, Wymagania dotyczące protokołów wymiany danych: „W celu zapewnienia znormalizowanego dostępu DPP należy stosować określone protokoły wymiany danych”.

Jednoznaczny, przenośny identyfikator niezależny od dostawcy EN 18219

Każdy paszport produktu musi posiadać unikalny identyfikator, który na stałe odnosi się do tego samego produktu i nie jest powiązany z żadnym dostawcą. Jeśli dostawca powiąże identyfikator ze swoją własną infrastrukturą, w przypadku zmiany dostawcy utracą Państwo tożsamość swoich

paszportów – każdy wydrukowany kod i każda rejestracja straciłyby wówczas znaczenie. Norma ta została opublikowana w Dzienniku Urzędowym Unii Europejskiej 15 lipca 2026 r.

Transpareo przypisuje identyfikator w postaci GS1 Digital Link wraz z Państwa numerem GTIN – jest to otwarty standard branżowy, który należy do produktu, a nie do platformy – i weryfikuje każdy identyfikator pod kątem zgodności z zatwierdzonymi schematami normatywnymi. Tożsamość podpisu znajduje się jako DID:web na Państwa własnej domenie, a nie na naszej. Identyfikator pozostaje ważny nawet w przypadku awarii systemu: stały adres rezerwowany nadal go rozpoznaje, a identyfikator zachowuje swoją tożsamość niezależnie od zmiany dostawcy.

Źródło: EN 18219, punkt 4.6.2(3): „Jednoznaczny identyfikator nie może prowadzić do uzależnienia od konkretnego dostawcy”.

Nośnik fizyczny, umożliwiający trwały odczyt EN 18220

Informacje te muszą być dostępne na nośniku danych w formacie nadającym się do odczytu maszynowego, do którego każdy może uzyskać dostęp bez specjalnego oprogramowania – i który pozostaje czytelny przez cały okres użytkowania produktu, nawet po jego zużyciu i naprawie. Nośnik danych wymagający określonej aplikacji lub konta uniemożliwia dostęp części odbiorców. Norma ta została opublikowana w Dzienniku Urzędowym Unii Europejskiej 15 lipca 2026 r.

Transpareo generuje kod QR zgodny z normą ISO/IEC 18004, zawierający adres GS1 Digital Link, który w każdej przeglądarce przekierowuje bezpośrednio do certyfikatu – bez logowania, bez pobierania, na każdym smartfonie. Model, partia i artykuł są już zawarte w zakodowanym adresie, dzięki czemu zeskanowanie kodu prowadzi bezpośrednio do właściwego poziomu. Ponieważ adres pozostaje stabilny dzięki trwałemu rozwiązaniu awaryjnemu, raz wydrukowany kod zachowuje ważność przez cały okres użytkowania produktu.

Źródło: EN 18220, Wymagania dotyczące nośników danych (rozdział 5): symbolika, kodowanie, jakość druku i trwałość; nośnik danych powinien pozostawać czytelny nawet po wielu cyklach użytkowania i napraw.

Przechowywanie i archiwizacja przez okres dłuższy niż minimalny EN 18221

Norma wymaga, aby specyfikacja wraz z historią jej wersji była przechowywana przez okres określony przepisami i pozostawała dostępna w niezmienionej postaci. Jeśli przechowywana jest jedynie aktualna wersja, traci się możliwość odtworzenia wcześniejszych danych – a właśnie to podmiot gospodarczy musi być w stanie wykazać przed organami administracji. Okres przechowywania zależy od przepisów obowiązujących w danym sektorze, ale wynosi co najmniej dziesięć lat. Norma ta została opublikowana w Dzienniku Urzędowym Unii Europejskiej 15 lipca 2026 r.

Transpareo zapisuje każdą publikację jako zamrożoną, podpisaną wersję w niezmiennym archiwum, w którym nikt nie może jej później zmienić ani usunąć – ani Państwo, ani my. Starsze wersje pozostają

dostępne obok aktualnej, a każda wersja posiada sygnaturę czasową i podpis. Dzięki temu można udowodnić, jakie informacje zawierał paszport w danym momencie.

Źródło: EN 18221: „Cyfrowy paszport produktu musi być dostępny dla uprawnionych użytkowników przez cały okres jego eksploatacji”.

API do zarządzania cyklem życia i przeszukiwalnością EN 18222

Oprócz wyświetlania w przeglądarce norma wymaga interfejsu programistycznego, za pomocą którego można tworzyć, odczytywać i aktualizować paszporty oraz wyszukiwać je na podstawie identyfikatorów produktów. Bez takiego interfejsu każda operacja przetwarzania zbiorczego pozostaje zadaniem wykonywanym ręcznie, a inne systemy nie mogą automatycznie korzystać z bazy paszportów. Norma została opublikowana w Dzienniku Urzędowym Unii Europejskiej 15 lipca 2026 r.

Transpareo obsługuje wymagane metody normatywne za pośrednictwem wersjonowanego, znormalizowanego interfejsu: Paszporty można tworzyć, odczytywać, aktualizować i przeszukiwać strona po stronie za pomocą identyfikatorów produktów w sposób sterowany programowo. Podpisany paszport jest przy tym dostarczany w niezmienionej postaci – interfejs zwraca dokładnie te bajty, których podpis może zostać zweryfikowany przez kontrolera.

Źródło: EN 18222: znormalizowany interfejs programistyczny (API) służący do zarządzania cyklem życia i zapewnienia możliwości przeszukiwania DPP, zgodnie z wymogami ESPR.

Model danych zapewniający interoperacyjność EN 18223

Aby paszporty były spójne między systemami i w ramach łańcuchów dostaw, norma nakłada obowiązek stosowania wspólnego modelu danych o ujednoliconym znaczeniu pól. Model własny dostawcy zmusza każdego partnera do tworzenia własnego tłumaczenia – a każde tłumaczenie stanowi źródło błędów. Norma została opublikowana w Dzienniku Urzędowym UE 15 lipca 2026 r.

Transpareo opiera się na horyzontalnej warstwie słownikowej z równoległymi, uznanymi słownikami specjalistycznymi (GSI, EPCIS i inne) i opisuje każdy punkt danych poprzez odniesienie do jego słownika oraz typu danych. Dzięki temu system odbierający dowiadyuje się nie tylko, jak nazywa się dane pole, ale także, co ono oznacza – paszport pozostaje czytelny bez konieczności zmiany formatu.

Źródło: EN 18223: wspólny semantyczny model danych na potrzeby interoperacyjności systemów w ramach DPP.

Trzystopniowy model uprawnień dostępu EN 18239

Karta produktu zawiera informacje publiczne, dane przeznaczone dla uprawnionych podmiotów gospodarczych oraz dane przeznaczone wyłącznie dla organów administracji; norma wymaga, aby te poziomy były oddzielone i regulowane osobno dla każdego pola danych. Dane publiczne muszą być

dostępne bez konieczności logowania, a pozostałe dane – wyłącznie po weryfikacji. Norma EN 18239 znajduje się na etapie ostatecznego zatwierdzenia.

Transpareo traktuje widoczność jako cechę każdego pola danych: poziom publiczny jest udostępniany bez uwierzytelniania, wyższe poziomy są chronione za pomocą oddzielnego, protokołowanego interfejsu dla organów administracji publicznej z dostępem wyłącznie do odczytu, a każdy dostęp do chronionych danych jest rejestrowany w dzienniku audytowym. Trzystopniowy model normy jest zatem już dziś odzwierciedlony w architekturze, a nie dodawany później.

Źródło: EN 18239 (projekt, w fazie ostatecznego zatwierdzenia): „Dostęp do danych publicznych musi być możliwy dla podmiotów z UE i spoza UE bez konieczności dodatkowego uwierzytelniania”; dane podlegające kontroli wymagają uwierzytelnionego, weryfikowalnego dostępu.

Weryfikowalna autentyczność i integralność danych EN 18246

Norma wymaga, aby autentyczność i integralność paszportu były możliwe do zweryfikowania, a weryfikacja mogła odbywać się swobodnie i bez ograniczeń. Zaufanie nie może zależeć od dalszego istnienia dostawcy, lecz musi opierać się na samym zestawie danych – w przeciwnym razie każdy paszport byłby wiarygodny tylko na tyle, na ile wiarygodna jest firma, która go aktualnie hostuje. Norma EN 18246 znajduje się na etapie ostatecznego zatwierdzenia.

Transpareo podpisuje każdą opublikowaną wersję dwoma niezależnymi kluczami (wydawcy i Transpareo) oraz łączy wersje za pomocą ich skrótów, dzięki czemu nie można niezauważalnie zmienić historii dokumentu. Renderer typu open source weryfikuje oba podpisy bezpośrednio w przeglądarce, bez konieczności kontaktowania się z naszym serwerem – wymagany podpisany, samoweryfikowalny dowód jest zatem już zaimplementowany.

Źródło: EN 18246 (projekt, w fazie ostatecznego zatwierdzenia): Autentyczność, wiarygodność i integralność danych DPP muszą być możliwe do udowodnienia.

Połączenie z rejestrem Komisji Europejskiej

Każdy paszport podlegający obowiązkowi rejestracji musi być w przyszłości wpisany do centralnego rejestru UE, który wydaje stały identyfikator rejestracyjny oraz urzędowe zaświadczenie o rejestracji. UE nie opublikowała jeszcze interfejsu technicznego do tego celu – dlatego obecnie żaden dostawca nie może wykazać się tym połączeniem; jeśli jakiś dostawca tak twierdzi, należy to zweryfikować.

Firma Transpareo przygotowała integrację w takim zakresie, w jakim jest to możliwe bez dostępu do interfejsu: niezbędne pola (identyfikator rejestracyjny, stały adres zapasowy, skrót wersji) zostały już utworzone w modelu danych. Gdy tylko UE opublikuje interfejs, aktywujemy rejestrację bez konieczności modyfikacji Państwa paszportów. Do tego czasu ta kwestia pozostaje otwarta – zarówno u nas, jak i u każdego uczciwego dostawcy.

Źródło: Projekt rozporządzenia wykonawczego w sprawie rejestru DPP (Ares(2026)4424976).

Przechowywanie danych rejestracyjnych po upływie terminu przewidzianego przepisami

Zarejestrowane dane dotyczące pasów muszą pozostawać dostępne w niezmienionej postaci przez okres przewidziany przepisami – zazwyczaj dziesięć lat od rejestracji – nawet w przypadku upadłości lub zaprzestania działalności przez producenta. Obowiązek ten trwa zatem dłużej niż umowa zawarta z dostawcą, a także dłużej niż sam dostawca.

W tym celu Transpareo prowadzi niezmienialne archiwum, w którym nikt nie może później zmienić ani usunąć raz zapisanej wersji – ani producent, ani my. Archiwum zostaje uruchomione automatycznie wraz z rejestracją w UE. Aby zapewnić dostęp do niego nawet w przypadku, gdyby firma Transpareo przestała kiedyś istnieć, jego trwałość jest zabezpieczona poprzez notarialne zdeponowanie w Szwajcarii.

Źródło: Rozporządzenie wykonawcze w sprawie rejestru DPP, art. 10 ust. 3 (okres przechowywania: dziesięć lat).

Dane dotyczące produktów w językach urzędowych każdego rynku docelowego

Obowiązkowe informacje zawarte w paszporcie muszą być dostępne w językach urzędowych każdego państwa członkowskiego, w którym produkt jest wprowadzany na rynek – a nie tylko w języku kraju, w którym znajduje się siedziba producenta. Kto obsługuje wyłącznie rynek krajowy, nie spełnia tego wymogu w odniesieniu do wszystkich pozostałych rynków docelowych.

Transpareo prowadzi każdy paszport w wersji wielojęzycznej i dostarcza obowiązkową treść we wszystkich 24 językach urzędowych UE. Wystarczy wprowadzić treść tylko raz; wersje językowe powstają na tej podstawie, bez konieczności ponoszenia dodatkowych opłat za każdy język ani prowadzenia oddzielnych paszportów. Dzięki temu paszport jest czytelny i zgodny z przepisami na każdym rynku docelowym.

Źródło: Rozporządzenie w sprawie baterii (UE) 2023/1542: dane w językach urzędowych państw członkowskich, w których produkt jest wprowadzany do obrotu.

Języki poza UE

Poza wymogami prawnymi warto, aby paszport obejmował również języki spoza UE – z myślą o rynkach eksportowych, międzynarodowych partnerach handlowych oraz konsumentach, którzy nie posługują się żadnym z języków urzędowych Unii.

Transpareo obsługuje łącznie 40 wersji językowych, w tym 24 języki urzędowe UE. Wystarczy wprowadzić treść tylko raz, a następnie wygenerować ją w dowolnym języku bez konieczności ponoszenia dodatkowych opłat za każdy język. Również interfejs, w którym zarządzasz swoimi paszportami (menedżer aplikacji), jest przetłumaczony na wszystkie 40 języków i możesz wprowadzać informacje w każdym z dostępnych języków.

Wersje i historia zmian

Karta zmienia się w trakcie cyklu życia produktu; bez kompletnej historii wersji nie da się później udowodnić, jaki stan obowiązywał w danym momencie. Norma wymaga zatem, aby wszystkie zmiany wprowadzone w karcie były archiwizowane.

Transpareo zamraża każdą publikację jako odrębną, podpisaną wersję i rejestruje, kto ją utworzył, kiedy oraz z jakimi zmienionymi polami. Dzięki temu każda informacja pozostaje weryfikowalna z mocą wsteczną, a późniejsza korekta nie nadpisuje historii, lecz ją kontynuuje.

Źródło: EN 18221: „Wszelkie zmiany wprowadzone w cyfrowym paszporcie produktu należy archiwizować”.

Skalowalna instalacja masowa dla rodzin produktów

Kto ma w ofercie wiele podobnych produktów, nie może ręcznie tworzyć każdego wpisu z osobna; sprawny system wymaga możliwości wprowadzania całych rodzin produktów jednocześnie.

Transpareo umożliwia przesyłanie danych produktów w formacie Excel lub CSV oraz przypisywanie ich do pól obowiązkowych; w przypadku bardzo dużych ilości dostępny jest dodatkowo interfejs API do obsługi zbiorczej, który tworzy karty programowo. Dzięki temu system może obsługiwać od kilkunastu do dziesiątek tysięcy kart.

Wewnętrzne zarządzanie uprawnieniami oparte na rolach

Nie każdy pracownik firmy powinien mieć uprawnienia do edytowania lub zatwierdzania treści paszportów; norma wymaga zarządzania uprawnieniami opartego na rolach, z rejestrowaniem dostępu.

Transpareo przyznaje uprawnienia w zależności od roli i grupy użytkowników oraz rejestruje każdą zmianę. Również podmioty zewnętrzne, takie jak warsztaty czy firmy zajmujące się recyklingiem, otrzymują jedynie ściśle ograniczony, czasowo ograniczony dostęp; organy administracji mają dostęp za pośrednictwem oddzielnego interfejsu, przeznaczonego wyłącznie do odczytu, który rejestruje każde wejście w dzienniku audytowym.

Źródło: EN 18239 (projekt), Zarządzanie uprawnieniami dostępu: określa, które podmioty mogą aktualizować i udostępniać dane DPP.

Przechowywanie po wygaśnięciu umowy

Obowiązek przechowywania danych nie wygasa wraz z wygaśnięciem umowy: zarejestrowany certyfikat musi pozostać aktywny przez okres przewidziany przepisami, nawet jeśli zrezygnujesz z usług dostawcy. Dostawca, który dezaktywuje certyfikaty wraz z wypowiedzeniem umowy, stwarza Ci problem związany z przestrzeganiem przepisów.

Transpareo zapewnia to dzięki temu samemu, niezmiennalnemu, dziesięcioletniemu archiwum, co dane rejestracyjne – po wypowiedzeniu umowy stały adres awaryjny nadal dostarcza paszporty, a interfejs urzędowy odczytuje ten sam zestaw danych z archiwum po wygaśnięciu umowy. Już wydrukowane kody QR pozostają ważne.

Źródło: EN 18221: Wersje archiwalne są również przechowywane u dostawcy usług tworzenia kopii zapasowych.

Podpis przy użyciu własnego klucza kryptograficznego

Każdy, kto posiada prywatny klucz podpisu, może generować paszporty w imieniu wystawcy; dlatego bezpieczniej jest, gdy wystawca sam przechowuje ten klucz, zamiast powierzać go dostawcy.

Dzięki funkcji „Bring Your Own Key” Państwa firma obsługuje własny punkt końcowy podpisu – Transpareo nigdy nie przechowuje klucza prywatnego, a jedynie dodaje niezależny podpis kontrpartyjny. W ten sposób każda wersja zawiera dwa niezależne od siebie podpisy, a podpis wystawcy jest takim, którego sama firma Transpareo nie jest w stanie wygenerować.

Tożsamość wystawcy niezależna od platformy

Aby weryfikator mógł znaleźć Państwa klucze publiczne, certyfikat musi zawierać opublikowaną tożsamość wystawcy. Jeśli znajduje się ona w domenie dostawcy, wiąże Państwa z nim: zmiana dostawcy spowodowałaby unieważnienie wszystkich już wydrukowanych kodów.

Transpareo publikuje Państwa tożsamość jako DID: w sieci na Państwa własnej domenie, a nie na naszej – zmiana dostawcy sprowadza się zatem do przeniesienia DNS, a już wydrukowane kody wraz z ich weryfikacją pozostają ważne. Dodatkowo w momencie publikacji odzwierciedlamy każdy klucz publiczny pod stałym adresem, dzięki czemu każda wersja pozostaje weryfikowalna, nawet jeśli pierwotny serwer zniknie.

Źródło: EN 18219, sekcja 4.2.2 (Trwałość): identyfikatory zachowują swoją ważność przez cały cykl życia; domeny internetowe można przenosić lub przekierowywać.

Możliwość weryfikacji przez osoby trzecie, całkowicie bez udziału dostawcy

Decydującym kryterium zaufania jest to, czy strona trzecia może zweryfikować certyfikat bez korzystania z infrastruktury dostawcy. Norma wymaga, aby weryfikacja ważności i integralności była dla weryfikatora bezpłatna i możliwa bez żadnych ograniczeń.

W tym celu firma Transpareo udostępnia renderer na licencji open source, który pobiera bajty danej wersji z dowolnego źródła, ponownie oblicza skrót i weryfikuje oba podpisy przy użyciu kluczy publicznych podanych w paszporcie – bez logowania, bez konieczności kontaktowania się z nami, bez zależności od działającej platformy. Każdy, kto ma wątpliwości, może zapoznać się z kodem źródłowym.

Źródło: EN 18246 (projekt): „Sprawdzanie ważności i integralności danych DPP musi być możliwe dla kontrolera bezpłatnie i bez żadnych ograniczeń”.

Zmiana dostawcy bez utraty danych

Dostawca, który utrudnia zmianę operatora, zatrzymuje użytkownika za pomocą jego własnych danych – a to, co stanie się z tymi danymi po wygaśnięciu umowy, decyduje o tym, czy użytkownik będzie mógł swobodnie zmienić operatora. Norma wymaga zatem, aby dane mogły być przenoszone za pośrednictwem otwartej, interoperacyjnej sieci bez wiązania z konkretnym dostawcą.

Transpareo od samego początku przechowuje dokumenty regulacyjne w otwartej przestrzeni, którą można publicznie zarchiwizować: prosta synchronizacja tworzy kompletną, podpisaną kopię, która samodzielnie weryfikuje się względem opublikowanych kluczy, bez naszego udziału. Pełne archiwum zdarzeń przekazujemy Państwu lub Państwa nowemu dostawcy za pośrednictwem podpisanego, ograniczonego czasowo adresu pobierania, a poprzedni katalog produktów dodatkowo w formatach JSON-LD i CSV. Po wygaśnięciu umowy zarejestrowane dane obowiązkowe pozostają dostępne za pośrednictwem niezmiennego, dziesięcioletniego archiwum: Publiczna kopia lustrzana i archiwum pozostają zsynchronizowane i przekazują ten sam zbiór danych, już wydrukowane kody QR nadal działają poprzez stały adres awaryjny, a odnośnik w rejestrze wskazuje na nowy adres. W ten sposób umowa wygasa bez utraty danych i bez naruszenia ustawowego obowiązku przechowywania.

Źródło: EN 18216: Dane muszą być „przesyłane za pośrednictwem otwartej, interoperacyjnej sieci, bez uzależnienia od konkretnego dostawcy”.

Integracja z istniejącymi systemami zamiast izolowanych baz danych

Karta, która funkcjonuje wyłącznie w interfejsie dostawcy, staje się „wyspą danych” w stosunku do pozostałych systemów – każda zmiana musi być wówczas wprowadzana dwukrotnie.

Transpareo zgłasza zdarzenia za pomocą podpisanych webhooków i umożliwia importowanie oraz eksportowanie danych poprzez interfejs API do obsługi danych zbiorczych, dzięki czemu można zintegrować Pass z własną infrastrukturą systemową. Celowo nie dostarczamy gotowego łącznika dla konkretnego systemu ERP – otwarte, podpisane interfejsy pasują do każdego systemu, zamiast faworyzować jeden z nich.

Import i eksport zbiorczy wykraczający poza czyste wymogi UE

Kto chce wykorzystywać zebrane dane również poza systemem Pass, potrzebuje funkcji importu i eksportu wykraczających poza obowiązkowe pola wymagane przepisami.

Transpareo przyjmuje większe ilości danych z plików Excel, CSV oraz za pośrednictwem interfejsu API Bulk i udostępnia je w takim samym zakresie. Dzięki temu system służy nie tylko spełnieniu wymogów UE, ale także własnej organizacji danych.

Oddzielna baza danych i własny klucz

W wspólnej bazie danych Państwa dane są powiązane z danymi innych klientów; w takiej sytuacji czyste, możliwe do udokumentowania rozdzielanie danych jest praktycznie niemożliwe – a prawo do usunięcia danych zgodnie z art. 17 RODO trudno jest wykazać.

W Transpareo każdy klient znajduje się w osobnej bazie danych, zaszyfrowanej własnym kluczem – rozdzielanie odbywa się zarówno na poziomie bazy danych, jak i szyfrowania. Spełnia to wymogi prawa do usunięcia danych poprzez weryfikowalne usunięcie; hosting znajduje się w Niemczech, a umowa o przetwarzaniu danych (AVV) jest zawarta w pakiecie.

Źródło: art. 17 RODO (prawo do usunięcia danych), spełnione dzięki oddzielnej bazie danych, unikalnemu kluczowi i możliwości weryfikacji usunięcia.

Szyfrowanie i kopie zapasowe

Dostawca musi chronić dane zarówno podczas przesyłania, jak i w stanie spoczynku, a także zabezpieczać je przed awarią; RODO wymaga w tym zakresie zastosowania środków zgodnych z aktualnym stanem techniki.

Transpareo szyfruje wszystkie połączenia za pomocą protokołu TLS, a wrażliwe dane aplikacji – za pomocą algorytmu AES. Kopie zapasowe są szyfrowane za pomocą GPG, odnawiane przy regularnej rotacji kluczy, tworzone co cztery godziny i przechowywane przez dwanaście miesięcy na oddzielnym serwerze.

Źródło: RODO, art. 32 (Bezpieczeństwo przetwarzania): TLS, AES oraz zaszyfrowane kopie zapasowe z rotacją.

Dziennik zdarzeń bezpieczeństwa

Zdarzenia związane z bezpieczeństwem muszą pozostawać możliwe do prześledzenia – kto i kiedy się zalogował oraz w jaki sposób wykorzystywano klucze. Dyrektywa NIS 2 wymaga prowadzenia odpowiednich dzienników audytowych.

Transpareo prowadzi dziennik zdarzeń bezpieczeństwa obejmujący próby logowania, wyzwania uwierzytelniania wieloskładnikowego (MFA) oraz aktywność kluczy API i przechowuje go przez okres jednego roku. W ten sposób spełnione są wymagania dyrektywy NIS-2 dotyczące dzienników audytowych.

Źródło: Dyrektywa NIS-2 (wymagania dotyczące dzienników audytowych): zarejestrowane zdarzenia związane z bezpieczeństwem, okres przechowywania wynoszący jeden rok.

Uwierzytelnianie wieloskładnikowe

Pojedyncze hasło zapewnia jedynie słabą ochronę dostępu; dyrektywa NIS-2 wymaga kontroli dostępu z uwierzytelnianiem wieloskładnikowym.

Transpareo oferuje uwierzytelnianie wieloskładnikowe dla wszystkich użytkowników menedżera aplikacji – za pomocą aplikacji Authenticator, klucza dostępu lub klucza sprzętowego – wraz z kodami zapasowymi na wypadek utraty. Można wymusić stosowanie uwierzytelniania wieloskładnikowego (MFA) dla Państwa konta.

Źródło: Dyrektywa NIS-2 (kontrola dostępu i uwierzytelnianie wieloskładnikowe).

Hosting z certyfikatem ISO 27001 w Niemczech

To, gdzie znajdują się serwery i w jaki sposób zabezpieczone jest centrum danych, decyduje o fizycznym bezpieczeństwie Państwa danych – a także o tym, jakim przepisom podlegają.

Transpareo korzysta z serwerów posiadających certyfikat ISO 27001, zlokalizowanych w Niemczech, gdzie stosowane są rygorystyczne środki bezpieczeństwa fizycznego i organizacyjnego. Ponadto lokalizacja w Niemczech gwarantuje, że Państwa dane podlegają w pełni prawu europejskiemu.

Źródło: ISO/IEC 27001 (zarządzanie bezpieczeństwem informacji), certyfikowane centrum danych w Niemczech.

Czy dostawca zajmuje się rejestracją w UE w Twoim imieniu?

Wpis do rejestru UE wraz z uzyskaniem oficjalnego zaświadczenia stanowi powtarzające się obciążenie, które dostawca może przejąć za Państwa. Rozporządzenie w sprawie rejestru wyraźnie to przewiduje: usługodawca może dokonać rejestracji w Państwa imieniu, przy czym odpowiedzialność prawna spoczywa na podmiocie gospodarczym.

Transpareo zarejestruje Państwa certyfikaty w Państwa imieniu, gdy tylko UE opublikuje interfejs techniczny – pozostają Państwo podmiotem gospodarczym ponoszącym odpowiedzialność prawną, ale nie ponoszą Państwo kosztów operacyjnych. Dopóki interfejs nie zostanie udostępniony, nikt nie może świadczyć tej usługi; my już przygotowaliśmy niezbędne do tego dane.

Źródło: Rozporządzenie wykonawcze w sprawie rejestru DPP (projekt), art. 19: Rejestracji może dokonać usługodawca na zlecenie; odpowiedzialność spoczywa na podmiocie gospodarczym.

Jasne zasady dotyczące nakładu pracy i kosztów związanych z obsługą techniczną

Niektórzy dostawcy oddzielają korzystanie z usługi od wsparcia technicznego i rozliczają pomoc osobno; w rezultacie trudno jest oszacować koszty współpracy.

W Transpareo wsparcie techniczne jest częścią pakietu – nie ma oddzielnej umowy serwisowej ani dodatkowych godzin rozliczanych według nakładu pracy. Wszystko, czego potrzebujesz w zakresie wsparcia, jest już zawarte w podanej cenie.

Przejrzysta struktura cenowa

Struktura cenowa, która ujawnia się dopiero podczas rozmowy sprzedażowej lub jest naliczana osobno dla każdego języka, produktu i wywołania interfejsu, sprawia, że rzeczywiste koszty są nieprzewidywalne.

Transpareo publikuje na swojej stronie internetowej cztery taryfy dostosowane do każdej wielkości przedsiębiorstwa, oferując bezpłatny okres próbny i możliwość wypowiedzenia umowy w dowolnym momencie. Nie ma żadnych ukrytych kosztów dodatkowych związanych z językiem, produktem czy wywołaniem interfejsu – podana cena jest ceną ostateczną.