

DPP Sağlayıcı Karşılaştırma Tablosu

Yalnızca halihazırda mevcut ve doğrulanabilir işlevlerin yanına işaret konulur - duyurular veya niyet beyanları değil. «Transpareo» sütunu önceden doldurulmuştur; diğer sağlayıcıları incelerken iki boş sütunu siz doldurursunuz. Her bir kriterle ilgili açıklamalar ve kaynaklar belgenin sonunda yer almaktadır.

Son güncelleme tarihi: 10.09.2026

Yasalarca zorunlu kılınmıştır

Kriter	Transpareo		
Açık ve standartlaştırılmış formatta veri alışverişi Pasaport verileri açık standartlar aracılığıyla erişilebilir durumdadır; bu veriler, yalnızca tek bir sağlayıcının yazılımı için değil, yetkili her sistem tarafından okunabilir. EN 18216	☒	☐	☐
Sağlayıcıya bağlı olmayan, benzersiz ve taşınabilir kimlik Ürünün kimlik bilgisi platforma değil, ürüne aittir; sağlayıcı değiştirildiğinde kimlik bilgisi aynı kalır. EN 18219	☒	☐	☐
Fiziksel veri taşıyıcısı, kalıcı olarak okunabilir Ürün üzerindeki QR kodu, herhangi bir tarayıcıda Pass sayfasına yönlendirir - uygulama gerekmez, hesap gerekmez, herhangi bir akıllı telefonla erişilebilir. EN 18220	☒	☐	☐
Asgari süre boyunca saklama ve arşivleme Yayınlanan her sürüm, yasal olarak öngörülen süre boyunca erişilebilir durumda kalır - sadece güncel sürüm değil, daha eski sürümler de. EN 18221	☒	☐	☐
Yaşam Döngüsü Yönetimi ve Aranabilirlik için API Bir programlama arayüzü, pasaportları okur, oluşturur ve tarar - sadece tıklamaya dayalı bir web arayüzü değildir. EN 18222	☒	☐	☐

Kriter	Transpareo		
Birbiriyle uyumlu veri modeli Pasaport verileri, diğer sistemlerin yeniden biçimlendirmeye gerek kalmadan okuyabileceği ortak bir modele uygundur. EN 18223	☒	☐	☐
Üç aşamalı erişim hakkı modeli Kamuya açık, yetkili ve resmi veriler birbirinden net bir şekilde ayrılmıştır; herkes yalnızca yetki alanına giren bilgileri görebilir. EN 18239	☒	☐	☐
Kanıtlanabilir veri gerçekliği ve bütünlüğü Her sürüm iki kez imzalanmıştır ve tarayıcıda doğrulanabilir - bize güvenmenize gerek kalmadan, yalnızca verilere dayanarak. EN 18246	☒	☐	☐
AB Komisyonu Kayıt Sistemi ile entegrasyon Resmi belgeyle birlikte kayıt - AB teknik arayüzü yayınlar yayınlamaz. Henüz mevcut değil; bugün hiçbir sağlayıcı bunu yerine getiremez.	☐	☐	☐
Kayıt verilerinin yasal süreden daha uzun süre saklanması Değiştirilemez on yıllık bir arşiv - ne üretici ne de Transpareo bir sürümü sonradan değiştiremez.	☒	☐	☐
Her hedef pazarın resmi dillerinde ürün bilgileri Zorunlu içerik, ürünün satıldığı her ülkenin resmi dillerinde yayınlanır; dolayısıyla AB çapında dağıtım söz konusu olduğunda, sadece iç pazarda değil, 24 resmi dilin tamamında yayınlanır.	☒	☐	☐

Bir DPP veritabanını işletmek için kullanışlıdır

Kriter	Transpareo		
AB'nin ötesindeki diller 24 AB resmi dilinin yanı sıra 16 dil daha - toplamda 40 dil, Birlik dışındaki hedef pazarlar için.	☒	☐	☐

Kriter	Transpareo		
Sürüm Yönetimi ve Değişiklik Geçmişi Her değişiklik, ürünün tüm yaşam döngüsü boyunca, tarih ve yazar bilgilerini içeren yeni ve izlenebilir bir sürüm oluşturur.	☒	☐	☐
Ürün aileleri için ölçeklenebilir seri üretim tesisi Ürün verilerini Excel veya CSV dosyası olarak yükleyin ve zorunlu alanlara atayın - büyük miktarlar için ayrıca bir toplu API de mevcuttur.	☒	☐	☐
Rol tabanlı dahili hak yönetimi Şirkette hangi verilerin kimler tarafından güncellenebileceği veya paylaşılabileceği belirlenmiştir; buna, dışarıdan gelen kişiler için sıkı sınırlamalara tabi ve süreli erişim hakları da dahildir.	☒	☐	☐
Sözleşme süresinin bitiminden sonra saklama Üyeliğinizi iptal etseniz bile, yayınladığınız pasaportlar değiştirilemez on yıllık arşivde erişilebilir durumda kalır.	☒	☐	☐
Kendi kriptografik anahtarıyla imza Kendi Anahtarınızı Getirin: Özel anahtarı siz saklıyorsunuz, biz sadece bağımsız bir karşı imza ekliyoruz.	☒	☐	☐
Platformdan bağımsız katılımcı kimliği Katılımcı kimliğiniz, DID:web olarak kendi alan adınızda yer alır, bizimkinde değil; sağlayıcı değişikliği, DNS taşıma işlemi anlamına gelir.	☒	☐	☐
Üçüncü taraflarca doğrulanabilirlik, sağlayıcıya hiç ihtiyaç duyulmadan Açık kaynaklı bir renderer, tarayıcıda hash değerlerini ve imzaları kontrol eder - bizim sunucularımızla bağlantı kurmadan.	☒	☐	☐

İstenen ek işlevler

Kriter	Transpareo		
Veri kaybı olmadan operatör değiştirme Geçiş sırasında, tüm pasaport veritabanını açık formatlarda yanınızda götürürsünüz - imzalanmış ve kendi kendini kontrol edebilen; sözleşme süresi sonunda, zorunlu pasaportlar veri kaybı olmaksızın değiştirilemez on yıllık arşivde erişilebilir durumda kalır.	☒	☐	☐
Veri adacığı yerine mevcut sistemlere entegrasyon İmzalı webhook'lar ve bir toplu işlem API'si, Pass'ı sistemlerinize entegre eder - belirli bir ERP sistemi için hazır bir bağlayıcı yoktur.	☒	☐	☐
AB'nin zorunlu kıldığı sınırların ötesinde toplu içe aktarma ve dışa aktarma Sadece zorunlu alanlar değil, daha büyük veri kümeleri de her iki yönde aktarılabilir.	☒	☐	☐

Güvenlik ve Gizlilik

Kriter	Transpareo		
Ayrı bir veritabanı ve kendine özgü anahtar Verileriniz, kendi anahtarınızla şifrelenmiş ayrı bir veritabanında saklanmaktadır; bu şifreleme, veritabanı ve şifreleme düzeylerinde ayrı olarak gerçekleştirilmektedir.	☒	☐	☐
Şifreleme ve yedeklemeler Tüm bağlantılar için TLS, hassas veriler için AES şifreleme ve anahtar rotasyonlu şifreli yedeklemeler.	☒	☐	☐
Güvenlik Olay Günlüğü Giriş denemeleri, çok faktörlü kimlik doğrulama (MFA) sorguları ve API anahtarları etkinlikleri kaydedilir ve bir yıl boyunca saklanır.	☒	☐	☐
Çok faktörlü kimlik doğrulama Tüm kullanıcılar için Authenticator uygulaması, şifre anahtarı veya donanım anahtarı; kayıp durumuna karşı yedek kodlar da mevcuttur.	☒	☐	☐

Kriter	Transpareo		
Almanya'da ISO 27001 sertifikalı barındırma hizmeti Almanya'da bulunan ve sıkı fiziksel ve organizasyonel güvenlik önlemlerine sahip sunucular.	☒	☐	☐

Ekonomik ve organizasyonel konular

Kriter	Transpareo		
Sağlayıcı, sizin adınıza AB kaydını üstleniyor mu? AB bu arayüzü yayınlar yayınlamaz, resmi belge dahil olmak üzere kayıt işlemlerini biz üstleniriz - böylece sizin için herhangi bir zahmet olmaz.	☒	☐	☐
Destek çalışmaları ve destek maliyetlerine ilişkin net düzenleme Transpareo'da destek hizmetine fiyat dahildir - ayrı bir destek sözleşmesi yoktur, ek masraf da yoktur.	☒	☐	☐
Şeffaf fiyat yapısı Her ölçekteki işletme için dört farklı genel tarifi, ücretsiz deneme süresi, istediğiniz zaman iptal edilebilir - dil, ürün veya API çağırısı başına gizli ek maliyetler yoktur.	☒	☐	☐

Açıklamalar ve kaynaklar

Açık ve standartlaştırılmış formatta veri alışverişi EN 18216

Standart, dijital ürün pasaportlarının açık ve standartlaştırılmış protokoller aracılığıyla erişilebilir olmasını gerektirir; böylece resmi kurumlar, iş ortakları ve kendi sistemleriniz, herhangi bir sağlayıcının yazılımına bağlı kalmadan verileri okuyabilir. Tescilli bir format ise bir “ada” gibi olur: Sağlayıcı olmadan kendi verilerinize erişemezsiniz. Standart, 15 Temmuz 2026 tarihinden itibaren AB Resmi Gazetesi'nde yayınlanmıştır (Uygulama Kararı (AB) 2026/1736) ve bu sayede ESPR ile uyumluluk varsayımı taşımaktadır.

Transpareo, tüm geçiş verilerini ve arayüzleri standart HTTPS üzerinden yapılandırılmış, makine tarafından okunabilir biçimde sunar - özel yazılım veya tescilli protokoller gerektirmez. Yayınlanan her sürüm ayrıca imzalanır; böylece alıcı, verileri sadece okumakla kalmaz, aynı zamanda verilerin değiştirilmediğini de doğrulayabilir. Arayüzde gördüğünüz, yetkili her sistemin açık arayüzler üzerinden aldığı veri setinin aynısıdır.

Kaynak: EN 18216, Veri alışverişi protokollerine ilişkin gereklilikler: «Standartlaştırılmış DPP erişimi için, belirlenen veri alışverişi protokolleri kullanılmalıdır.»

Sağlayıcıya bağlı olmayan, benzersiz ve taşınabilir kimlik EN 18219

Her ürün pasaportu, kalıcı olarak aynı ürüne atıfta bulunan ve herhangi bir tedarikçiye bağlı olmayan benzersiz bir kimlik numarasına sahip olmalıdır. Bir tedarikçi bu kimlik numarasını kendi altyapısına bağlarsa, tedarikçi değiştiğinde pasaportlarınızın kimliği kaybolur; bu durumda basılı her kod ve her kayıt anlamsız hale gelir. Standart, 15 Temmuz 2026 tarihinden itibaren AB Resmi Gazetesi'nde yayınlanmıştır.

Transpareo, kimliği GTIN'inizle birlikte bir GS1 Digital Link olarak atar – bu, platforma değil ürüne ait olan açık bir endüstri standardıdır – ve her kimliği onaylanmış standart şemalarına göre doğrular. İmza kimliği, bizim alan adımızda değil, kendi alan adınızda DID:web olarak bulunur. Bir sistem arızalansa bile kimlik geçerliliğini korur: Kalıcı bir yedek adres kimliği çözümlmeye devam eder ve kimlik, sağlayıcı değişikliği durumunda bile kimliğini korur.

Kaynak: EN 18219, Bölüm 4.6.2(3): «Benzersiz tanımlayıcı, belirli bir tedarikçiye bağlılığa yol açmamalıdır.»

Fiziksel veri taşıyıcısı, kalıcı olarak okunabilir EN 18220

Pasaport, ürün üzerinde herkesin özel bir yazılım olmadan erişebileceği, makine tarafından okunabilir bir veri taşıyıcısı aracılığıyla erişilebilir olmalı ve ürünün tüm kullanım ömrü boyunca, kullanım ve onarımdan sonra bile okunabilir kalmalıdır. Belirli bir uygulama veya hesap gerektiren bir veri taşıyıcısı, halkın bir kısmını dışarıda bırakır. Standart, 15 Temmuz 2026 tarihinden itibaren AB Resmi Gazetesi'nde yayınlanmıştır.

Transpareo, ISO/IEC 18004 standardına uygun, bir GS1 Digital Link adresi içeren ve her tarayıcıda doğrudan Pasaporta yönlendiren bir QR kodu oluşturur; oturum açmaya gerek yok, indirme gerek yok, her akıllı telefonda çalışır. Model, parti numarası ve ürün kodu kodlanmış adrese zaten dahil olduğundan, tarama işlemi doğrudan doğru sayfaya yönlendirilir. Adres, kalıcı bir yedek çözüm sayesinde sabit kaldığından, bir kez yazdırılan kod ürünün tüm kullanım ömrü boyunca geçerliliğini korur.

Kaynak: EN 18220, Veri Taşıyıcılarına İlişkin Gereklilikler (Bölüm 5): Semboller, Kodlama, Baskı Kalitesi ve Dayanıklılık; veri taşıyıcısı, birçok kullanım ve onarım döngüsünden sonra bile okunabilir durumda kalmalıdır.

Asgari süre boyunca saklama ve arşivleme EN 18221

Standart, bir standardın sürüm geçmişiyle birlikte, mevzuatta öngörülen süre boyunca saklanması ve değiştirilmeden erişilebilir kalmasını gerektirir. Yalnızca güncel durum tutulursa, önceki bilgilerin izlenebilirliği kaybolur; oysa bir ekonomik aktörün resmi makamlara kanıtlayabilmesi gereken tam da budur. Saklama süresi ilgili sektör mevzuatına göre belirlenir, ancak en az on yıldır. Standart, 15 Temmuz 2026 tarihinden itibaren AB Resmi Gazetesi'nde yayınlanmıştır.

Transpareo, her yayını, daha sonra ne siz ne de biz dahil hiç kimse tarafından değiştirilemeyecek veya silinemeyecek şekilde, değiştirilemez bir arşive dondurulmuş ve imzalanmış bir sürüm olarak kaydeder. Eski sürümler güncel sürümün yanında erişilebilir durumda kalır ve her sürüm zaman damgası ve imzayı taşır. Böylelikle, herhangi bir zamanda pasaportun o anda neyi gösterdiği kanıtlanabilir.

Kaynak: EN 18221: «Dijital Ürün Pasaportu, tüm kullanım ömrü boyunca yetkili kullanıcıların erişimine açık tutulmalıdır.»

Yaşam Döngüsü Yönetimi ve Aranabilirlik için API EN 18222

Tarayıcıda görüntülenmenin yanı sıra, standart, pasaportların oluşturulabileceği, okunabileceği, güncellenebileceği ve ürün kimlik numaralarıyla aranabileceği bir programlama arayüzü gerektirmektedir. Böyle bir arayüz olmadan, her türlü toplu işlem manuel olarak yapılmak zorunda kalır ve diğer sistemler pasaport veritabanını otomatik olarak kullanamaz. Standart, 15 Temmuz 2026 tarihinden itibaren AB Resmi Gazetesi'nde yayınlanmıştır.

Transpareo, sürüm kontrollü ve standartlaştırılmış bir arayüz aracılığıyla zorunlu standart yöntemlerini desteklemektedir: Pasaportlar, yazılım kontrollü olarak oluşturulabilir, okunabilir, güncellenebilir ve ürün kimlik numaraları aracılığıyla sayfa sayfa aranabilir. İmzalanmış pasaport bu süreçte değiştirilmeden teslim edilir; arayüz, bir denetçinin imzasını doğrulayabileceği baytları tam olarak verir.

Kaynak: EN 18222: ESPR'nin gerektirdiği şekilde, DPP'nin yaşam döngüsü yönetimi ve aranabilirliği için standartlaştırılmış programlama arayüzü (API).

Birbiriyle uyumlu veri modeli EN 18223

Pasaportların sistemler arasında ve tedarik zincirleri boyunca birbiriyle uyumlu olması için, standart, alanların anlamlarının tek tip olduğu ortak bir veri modeli öngörmektedir. Bir tedarikçiye özgü model, her bir ortağı kendi çevirisini yapmaya zorlar – ve her çeviri bir hata kaynağıdır. Standart, 15 Temmuz 2026 tarihinden itibaren AB Resmi Gazetesi'nde yayınlanmıştır.

Transpareo, paralel ve kabul görmüş teknik sözlükleri (GS1, EPCIS ve diğerleri) içeren yatay bir sözlük katmanına dayanır ve her veri noktasını sözlüğüne ve veri türüne atıfta bulunarak tanımlar. Böylelikle alıcı sistem, bir alanın sadece adını değil, aynı zamanda ne anlama geldiğini de öğrenir; pasaport, yeniden biçimlendirilmeye gerek kalmadan okunabilir kalır.

Kaynak: EN 18223: DPP'nin sistemler arası çalışabilirliği için ortak anlamsal veri modeli.

Üç aşamalı erişim hakkı modeli EN 18239

Bir ürün pasaportu, kamuya açık bilgileri, yetkili ekonomik aktörlere yönelik verileri ve yalnızca resmi makamlara yönelik verileri içerir; standart, bu seviyelerin ayrı tutulmasını ve her bir veri alanı için ayrı ayrı düzenlenmesini gerektirir. Kamuya açık verilere oturum açmaya gerek olmadan erişilebilmelidir; diğer

tüm verilere ise yalnızca doğrulama işleminden sonra erişilebilir. EN 18239 standardı nihai onay aşamasındadır.

Transpareo, görünürlüğü her veri alanı için ayrı bir özellik olarak ele alır: Kamuya açık seviye kimlik doğrulaması gerektirmeden sunulur; daha üst seviyeler ise yalnızca okuma erişimine sahip, protokolü kaydedilen özel bir resmi kurum arayüzü aracılığıyla korunur ve korunan verilere yapılan her erişim denetim günlüğüne kaydedilir. Standarttaki bu üç aşamalı model, böylece mimariye şimdiden entegre edilmiştir; sonradan eklenmiş değildir.

Kaynak: EN 18239 (Taslak, nihai onay aşamasında): «Kamu verilerine erişim, AB üyesi ve AB üyesi olmayan taraflar için ek kimlik doğrulama gerektirmeden mümkün olmalıdır»; denetime tabi veriler ise kimlik doğrulaması yapılmış ve izlenebilir erişim gerektirir.

Kanıtlanabilir veri gerçekliği ve bütünlüğü EN 18246

Standart, bir pasaportun gerçekliğinin ve bütünlüğünün kanıtlanabilir olmasını ve doğrulamanın serbest ve sınırsız bir şekilde yapılabilmesini gerektirir. Güven, hizmet sağlayıcının varlığına bağlı olmamalı, veri setinin kendisine bağlı olmalıdır – aksi takdirde her pasaport, onu barındıran şirket kadar güvenilir olurdu. EN 18246 standardı son onay aşamasındadır.

Transpareo, yayınlanan her sürümü iki bağımsız anahtarla (düzenleyen ve Transpareo) imzalar ve sürümleri hash değerleri üzerinden birbirine bağlar; böylece geçmiş de fark edilmeden değiştirilemez. Açık kaynaklı bir görüntüleyici, bizim sunucularımızla iletişime geçmeden her iki imzayı da doğrudan tarayıcıda doğrular; böylece istenen imzalı, kendi kendini doğrulayabilen kanıt zaten uygulanmış olur.

Kaynak: EN 18246 (Taslak, nihai kabul aşamasında): DPP verilerinin özgünlüğü, güvenilirliği ve bütünlüğü kanıtlanabilir olmalıdır.

AB Komisyonu Kayıt Sistemi ile entegrasyon

Kayıt zorunluluğu bulunan her pasaport, bundan böyle merkezi AB kayıt sistemine kaydedilmek zorundadır; bu sistem, kalıcı bir kayıt kimliği ve resmi bir kayıt belgesi düzenler. AB, bunun için gerekli teknik arayüzü henüz yayınlamamıştır; bu nedenle şu anda hiçbir sağlayıcı bu bağlantıyı kanıtlayamaz; bir sağlayıcı böyle bir iddiada bulunursa, bunu sorgulamalısınız.

Transpareo, arayüz olmadan mümkün olduğu ölçüde bu bağlantıyı hazırlamıştır: Bunun için gerekli alanlar (kayıt kimliği, sabit yedek adres, sürüm hash'i) veri modelinde halihazırda oluşturulmuştur. AB arayüzü yayınlar yayınlamaz, sizlerin sistemlerinizi yeniden yapılandırmanıza gerek kalmadan kaydı etkinleştireceğiz. O zamana kadar bu konu belirsizliğini koruyacaktır – hem bizde hem de her dürüst sağlayıcıda olduğu gibi.

Kaynak: DPP Kayıt Uygulama Yönetmeliği Taslağı (Ares(2026)4424976).

Kayıt verilerinin yasal süreden daha uzun süre saklanması

Kayıtlı pasaport verileri, yasal süre boyunca – genellikle kayıttan itibaren on yıl – üreticinin iflası veya faaliyetine son vermesi durumunda bile değiştirilmeden erişilebilir durumda kalmalıdır. Dolayısıyla bu yükümlülük, bir sağlayıcıyla yaptığınız sözleşmeden ve sağlayıcının kendisinden daha uzun süre geçerlidir.

Transpareo, bu amaçla, bir kez kaydedilen sürümü ne üreticinin ne de bizim tarafımızdan sonradan değiştirilemeyecek veya silinemeyecek şekilde, değiştirilemez bir arşiv tutmaktadır. Arşiv, AB kaydıyla birlikte otomatik olarak devreye girer. Transpareo'nun bir gün ortadan kalkması durumunda bile arşivin erişilebilir kalması için, İsviçre'de noter nezdinde bir emanet yoluyla arşivin devamlılığı güvence altına alınmıştır.

Kaynak: DPP Kayıt Uygulama Yönetmeliği, Madde 10(3) (on yıl süreyle saklama).

Her hedef pazarın resmi dillerinde ürün bilgileri

Bir pasaportun zorunlu bilgileri, ürünün piyasaya sunulduğu her üye devletin resmi dillerinde bulunmalıdır – yalnızca üreticinin merkezinin bulunduğu ülkenin dilinde değil. Yalnızca kendi iç pazarına hizmet verenler, diğer tüm hedef pazarlar için bu yükümlülüğü yerine getirmiş sayılmaz.

Transpareo, her bir pasaportu çok dilli olarak hazırlar ve zorunlu içeriği 24 AB resmi dilinin tamamında sunar. İçeriği tek seferde girersiniz; dil versiyonları, her dil için ek ücret ödemenize veya ayrı pasaportlar hazırlamanıza gerek kalmadan bu içerikten otomatik olarak oluşturulur. Böylece pasaport, her hedef pazarda mevzuata uygun şekilde okunabilir hale gelir.

Kaynak: Pil Yönetmeliği (AB) 2023/1542: Ürünün piyasaya sürüldüğü üye devletlerin resmi dillerinde verilen bilgiler.

AB'nin ötesindeki diller

Yasal yükümlülüğün ötesinde, bir pasaportun AB dışındaki dilleri de kapsamı faydalıdır – ihracat pazarları, uluslararası ticaret ortakları ve Birliğin resmi dillerinden hiçbirini konuşmayan tüketiciler için.

Transpareo, 24 AB resmi dili de dahil olmak üzere toplam 40 dil sürümünü yönetmektedir. İçeriği tek seferde girip, dil başına ek ücret ödmeden istediğiniz her dilde yayınlatabilirsiniz. Pasaportlarınızı yönettiğiniz arayüz (Uygulama Yöneticisi) de 40 dilin tümüne çevrilmiştir ve mevcut dillerin herhangi birinde bilgi girebilirsiniz.

Sürüm Yönetimi ve Değişiklik Geçmişi

Bir geçiş belgesi, ürünün kullanım ömrü boyunca değişikliklere uğrar; eksiksiz bir sürüm geçmişi olmadan, daha sonra hangi sürümün ne zaman geçerli olduğu kanıtlanamaz. Bu nedenle standart, geçiş belgesinde yapılan tüm değişikliklerin arşivlenmesini şart koşar.

Transpareo, her bir yayını ayrı, imzalanmış bir sürüm olarak dondurur ve bunu kimin, ne zaman ve hangi alanlarda değişiklik yaparak oluşturduğunu kaydeder. Böylelikle her bilgi geriye dönük olarak doğrulanabilir ve daha sonra yapılan bir düzeltme geçmiş silmez, aksine geçmiş devam ettirir.

Kaynak: EN 18221: «Dijital Ürün Pasaportu'nda yapılan tüm değişiklikler arşivlenmelidir.»

Ürün aileleri için ölçeklenebilir seri üretim tesisi

Benzer ürünleri çok sayıda satan bir işletme, her bir ürün kartını tek tek manuel olarak oluşturamaz; işlevsel bir sistem, tüm ürün ailelerini tek seferde kaydetmenin bir yoluna ihtiyaç duyar.

Transpareo, ürün verilerini Excel veya CSV formatında yüklemenize ve zorunlu alanlara atamanıza olanak tanır; çok büyük miktarlar için ayrıca, ürün kartlarını program kontrollü olarak oluşturan bir toplu API de mevcuttur. Böylelikle, ürün kartı oluşturma işlemi bir düzine karttan on binlerce karta kadar ölçeklenebilir.

Rol tabanlı dahili hak yönetimi

Şirketteki herkesin her geçiş kartı içeriğini düzenleme veya onaylama yetkisi olmamalıdır; standart, erişimlerin kaydedildiği rol tabanlı bir yetki yönetimi gerektirmektedir.

Transpareo, hakları rol ve kullanıcı grubuna göre tahsis eder ve her değişikliği kaydeder. Atölyeler veya geri dönüşümcüleri gibi harici taraflar da yalnızca çok sınırlı ve süreli erişim haklarına sahip olur; resmi kurumlar ise her erişimi denetim günlüğünde işaretleyen, ayrı ve yalnızca okuma amaçlı bir arayüz üzerinden erişim sağlar.

Kaynak: EN 18239 (Taslak), Erişim Hakları Yönetimi: Hangi paydaşların DPP verilerini güncelleyebileceğini ve paylaşabileceğini belirler.

Sözleşme süresinin bitiminden sonra saklama

Saklama yükümlülüğü sözleşmenin sona ermesiyle bitmez: Kayıtlı bir kimlik kartı, sağlayıcıdan ayrılırsanız bile yasal süre boyunca geçerliliğini korumalıdır. Fesihle birlikte kimlik kartlarını devre dışı bırakan bir sağlayıcı, size bir uyum sorunu yaratır.

Transpareo, kayıt verileriyle aynı, değiştirilemez on yıllık arşiv aracılığıyla bu yükümlülüğü üstlenir - sözleşmenin feshinden sonra kalıcı bir yedek adres, kimlik kartlarını dağıtmaya devam eder ve resmi kurum arayüzü, sözleşme sonrası arşivden aynı veri setini okur. Daha önce basılmış QR kodları geçerliliğini korur.

Kaynak: EN 18221: Arşiv sürümleri, yedekleme hizmeti sağlayıcısında da saklanır.

Kendi kriptografik anahtarıyla imza

Özel imza anahtarını elinde bulunduran kişi, düzenleyicinin adına pasaportlar oluşturabilir; bu nedenle, düzenleyicinin bu anahtarı sağlayıcıya emanet etmek yerine kendisinde tutması daha güvenlidir.

"Bring Your Own Key" (Kendi Anahtarınızı Getirin) özelliği ile şirketiniz kendi imza uç noktasını işletir; Transpareo hiçbir zaman özel anahtarı elinde tutmaz ve yalnızca bağımsız bir karşı imza ekler. Böylece her sürüm birbirinden bağımsız iki imza taşır ve düzenleyici imzanız, Transpareo'nun kendisinin oluşturamayacağı bir imzadır.

Platformdan bağımsız katılımcı kimliği

Bir denetçinin açık anahtarlarınızı bulabilmesi için, sertifikanın yayınlanmış bir düzenleyici kimliği olması gerekir. Bu kimlik sağlayıcının etki alanında bulunuyorsa, sizi ona bağlar: Sağlayıcıyı değiştirmeniz halinde, halihazırda basılmış tüm kodlar geçersiz hale gelir.

Transpareo, kimliğinizi DID olarak yayınlar:web'de kendi alan adınızda, bizimkinde değil - böylece sağlayıcı değişikliği bir DNS taşıma işlemine dönüşür ve önceden basılmış kodlar ile bunların doğrulamaları geçerliliğini korur. Ayrıca, her açık anahtarı yayınlandığı anda kalıcı bir adrese yansıtıyoruz; böylece orijinal barındırıcı ortadan kalksa bile her sürüm doğrulanabilir olmaya devam eder.

Kaynak: EN 18219, Bölüm 4.2.2 (Kalıcılık): Kimlikler yaşam döngüsü boyunca korunur; web alan adları devredilebilir veya yönlendirilebilir.

Üçüncü taraflarca doğrulanabilirlik, sağlayıcıya hiç ihtiyaç duyulmadan

Güven açısından belirleyici test, üçüncü bir tarafın sağlayıcının altyapısını kullanmadan paspoyu doğrulayabilmesidir. Standart, geçerlilik ve bütünlük kontrolünün denetleyici için ücretsiz ve herhangi bir kısıtlama olmaksızın gerçekleştirilebilmesini şart koşturmaktadır.

Transpareo, bu amaçla herhangi bir kaynaktan bir sürümün baytlarını yükleyen, hash değerini yeniden hesaplayan ve her iki imzayı da Pas'ta belirtilen açık anahtarlarla karşılaştıran açık kaynaklı bir renderer yayınlamaktadır - oturum açmaya gerek yok, bizi aramaya gerek yok, çalışan bir platforma bağımlılık yok. Şüphe duyanlar kaynak kodunu inceleyebilir.

Kaynak: EN 18246 (Taslak): «DPP verilerinin geçerliliğinin ve bütünlüğünün kontrolü, denetçi için ücretsiz ve herhangi bir kısıtlama olmaksızın mümkün olmalıdır.»

Veri kaybı olmadan operatör değiştirme

Değişimi zorlaştıran bir sağlayıcı, sizi kendi verilerinizle bağlar - ve sözleşme sona erdiğinde verilere ne olacağı, serbestçe sağlayıcı değiştirebilmenizi belirler. Bu nedenle standart, verilerin sağlayıcıya bağlı olmaksızın açık, birlikte çalışabilir bir ağ üzerinden aktarılabilir olmasını gerektirir.

Transpareo, düzenleyici belgeleri baştan itibaren açık, kamuya yansıtılabilir bir alana kaydeder: Basit bir senkronizasyon, bizim herhangi bir müdahaleye gerek kalmadan, yayınlanan anahtarlara göre kendi kendini doğrulayan eksiksiz, imzalı bir kopya oluşturur. Tam olay arşivini, imzalanmış ve süreli bir indirme adresi aracılığıyla size veya yeni sağlayıcınıza, önceki ürün kataloğunu ise ek olarak JSON-LD ve CSV formatlarında sunuyoruz. Sözleşme sona erdiğinde, kayıtlı zorunlu belgeler değiştirilemez on yıllık arşiv

aracılığıyla erişilebilir olmaya devam eder: Kamuya açık yansıma ve arşiv senkronize kalır ve aynı veri setini aktarır; önceden basılmış QR kodları kalıcı yedek adres üzerinden çözülmeye devam eder ve kayıt referansı yeni adrese yönlendirilir. Böylece sözleşme, veri kaybı olmadan ve yasal saklama yükümlülüğüne aykırı bir durum oluşmadan sona erer.

Kaynak: EN 18216: Veriler, «sağlayıcıya bağlı olmayan, açık ve birbiriyle uyumlu bir ağ üzerinden aktarılabilir» olmalıdır.

Veri adacığı yerine mevcut sistemlere entegrasyon

Sadece sağlayıcının arayüzünde bulunan bir Pass, diğer sistemlerinizin yanında bir veri adacığına dönüşür; bu durumda her değişiklik iki kez güncellenmek zorunda kalır.

Transpareo, imzalı webhook'lar aracılığıyla olayları bildirir ve verilerin toplu API üzerinden okunup yazılmasını sağlar; böylece Pass'ı kendi sistem ortamınıza entegre edebilirsiniz. Belirli bir ERP sistemi için hazır bir konektör sunmamayı bilinçli olarak tercih ediyoruz; açık ve imzalı arayüzlerimiz, tek bir sistemi tercih etmek yerine her sisteme uyum sağlar.

AB'nin zorunlu kıldığı sınırların ötesinde toplu içe aktarma ve dışa aktarma

Kaydedilen verileri pasaport dışında da kullanmak isteyenler, yasal olarak zorunlu alanların ötesinde bir içe ve dışa aktarma işlevine ihtiyaç duyar.

Transpareo, Excel, CSV ve Toplu API aracılığıyla büyük hacimli verileri alır ve aynı kapsamda geri verir. Böylelikle sistem, yalnızca AB yükümlülüğünün yerine getirilmesine değil, aynı zamanda kendi veri yönetimi ihtiyaçlarınıza da hizmet eder.

Ayrı bir veritabanı ve kendine özgü anahtar

Paylaşımlı bir veritabanında, verileriniz diğer müşterilerin verileriyle birbirine bağlıdır; bu durumda net ve kanıtlanabilir bir ayırım yapmak neredeyse imkansızdır - ve GDPR'nin 17. maddesine göre silme hakkı zorlukla kanıtlanabilir.

Transpareo'da her müşteri, kendine ait bir anahtarla şifrelenmiş ayrı bir veritabanında yer alır; ayırım hem veritabanı hem de şifreleme düzeyinde sağlanır. Bu, doğrulanabilir silme yoluyla silme hakkını yerine getirir; barındırma hizmeti Almanya'da yer alır ve Veri İşleme Sözleşmesi (VİS) dahildir.

Kaynak: GDPR Madde 17 (Silme hakkı); ayrı bir veritabanı, özel anahtar ve doğrulanabilir silme işlemiyle bu hüküm yerine getirilmektedir.

Şifreleme ve yedeklemeler

Bir hizmet sağlayıcı, verileri aktarım sırasında ve depolandıkları sırada korumalı ve arızalara karşı güvence altına almalıdır; GDPR bu amaçla en son teknolojiye uygun önlemlerin alınmasını şart koşmaktadır.

Transpareo, tüm bağlantıları TLS ile, hassas uygulama verilerini ise AES ile şifreler. Yedeklemeler GPG ile şifrelenir, düzenli anahtar rotasyonu ile yenilenir, her dört saatte bir oluşturulur ve on iki ay boyunca ayrı bir sunucuda saklanır.

Kaynak: GDPR Madde 32 (İşlemenin Güvenliği): TLS, AES ve rotasyonlu şifreli yedeklemeler.

Güvenlik Olay Günlüğü

Güvenlikle ilgili olayların izlenebilirliği sağlanmalıdır – kimin ne zaman oturum açtığı ve anahtarların nasıl kullanıldığı gibi. NIS-2 Direktifi, buna uygun denetim günlüklerini zorunlu kılmaktadır.

Transpareo, oturum açma denemeleri, çok faktörlü kimlik doğrulama (MFA) sorguları ve API anahtarlarının kullanımına ilişkin bir güvenlik olay günlüğü tutar ve bunu bir yıl boyunca saklar. Böylelikle NIS-2'nin denetim günlüklerine ilişkin gereklilikleri karşılanmış olur.

Kaynak: NIS-2 Direktifi (Denetim Günlüklerine İlişkin Gereklilikler): kaydedilen güvenlik olayları, bir yıl süreyle saklama.

Çok faktörlü kimlik doğrulama

Tek bir şifre, erişimi yeterince korumaz; NIS-2 yönergesi, çok faktörlü kimlik doğrulama ile erişim kontrolü yapılmasını şart koşar.

Transpareo, Uygulama Yöneticisi'nin tüm kullanıcıları için çok faktörlü kimlik doğrulama sunar – Authenticator uygulaması, şifre anahtarı veya donanım anahtarı yoluyla – ve kayıp durumuna karşı yedek kodlar da dahil. MFA zorunluluğu, hesabınız için etkinleştirilebilir.

Kaynak: NIS-2 Direktifi (Erişim Kontrolü ve Çok Faktörlü Kimlik Doğrulama).

Almanya'da ISO 27001 sertifikalı barındırma hizmeti

Sunucuların bulunduğu yer ve veri merkezinin nasıl korunduğu, verilerinizin fiziksel güvenliğini ve hangi yasalara tabi olduklarını belirler.

Transpareo, Almanya'da ISO 27001 sertifikalı sunucularda barındırma hizmeti sunmaktadır ve bu sunucular, sıkı fiziksel ve organizasyonel güvenlik önlemlerine tabidir. Almanya'daki konum, verilerinizin tamamen Avrupa hukuku kapsamında kalmasını sağlar.

Kaynak: ISO/IEC 27001 (Bilgi Güvenliği Yönetimi), Almanya'da sertifikalı veri merkezi.

Sağlayıcı, sizin adınıza AB kaydını üstleniyor mu?

AB Kayıt Sistemi'ne kayıt yaptırmak ve resmi belgenin alınması, bir hizmet sağlayıcının sizin adınıza üstlenebileceği tekrarlayan bir işlemdir. Kayıt Yönetmeliği bunu açıkça öngörmektedir: Bir hizmet sağlayıcı, kayıt işlemini sizin adınıza üstlenebilir; ancak yasal sorumluluk ekonomik aktöre aittir.

Transpareo, AB teknik arayüzü yayınlar yayınlamaz sizin adınıza pasaportlarınızı kaydeder – siz hukuki açıdan sorumlu ekonomik aktör olmaya devam edersiniz, ancak operasyonel yükü üstlenmezsiniz. Arayüz hazır olana kadar kimse bu hizmeti sunamaz; biz bunun için gerekli verileri şimdiden hazırladık.

Kaynak: DPP Kayıt Uygulama Yönetmeliği (Taslak), Madde 19: Kayıt işlemi, bir hizmet sağlayıcı tarafından vekaleten gerçekleştirilebilir; ancak sorumluluk ekonomik aktöre aittir.

Destek çalışmaları ve destek maliyetlerine ilişkin net düzenleme

Bazı sağlayıcılar, hizmet kullanımını destek hizmetinden ayırır ve yardım hizmetini ayrı olarak faturalandırır; sonuç olarak, bu durum işbirliğinin maliyetini hesaplamayı zorlaştırır.

Transpareo’da destek, tarifeye dahildir – ayrı bir destek sözleşmesi yoktur, harcanan zamana göre faturalandırılan ek saatler de yoktur. İhtiyacınız olan tüm destek hizmetleri, belirtilen fiyata zaten dahildir.

Şeffaf fiyat yapısı

Satış görüşmesi sırasında ancak ortaya çıkan ya da dil, ürün ve arayüz çağrısı başına sonradan hesaplanan bir fiyat yapısı, gerçek maliyetleri öngörülemez hale getirir.

Transpareo, her şirket büyüklüğü için dört farklı tarifeyi web sitesinde açık bir şekilde yayınlar; bu tarifeler ücretsiz deneme süresi ve istediğiniz zaman iptal etme imkanı sunar. Dil, ürün veya arayüz çağrısı başına gizli ek maliyetler yoktur – belirtilen fiyat, ödenecek fiyattır.