

DPP-palveluntarjoajien vertailulomake

Vain jo olemassa olevat, todennettavissa olevat toiminnot merkitään ruutuun – ei ilmoituksia tai aiejulistuksia. Sarake "Transpareo" on esitätetty; täytätte kaksi tyhjää saraketta, kun tarkastelette muita palveluntarjoajia. Selitykset ja lähteet kustakin kriteeristä löytyvät asiakirjan lopusta.

Tilanne: 10.09.2026

Lain mukaan pakollista

Kriteeri	Transpareo		
Tietojen vaihto avoimessa, standardoidussa muodossa Passin tiedot ovat saatavilla avoimien standardien kautta – ne ovat luettavissa kaikissa valtuutetuissa järjestelmissä, eivätkä vain yhden toimittajan ohjelmistossa. EN 18216	☒	☐	☐
Yksiselitteinen, siirrettävä tunniste, joka ei ole sidottu tiettyyn palveluntarjoajaan Tuotteen tunniste liittyy tuotteeseen, ei alustaan – palveluntarjoajaa vaihdettaessa passi säilyttää identiteettinsä. EN 18219	☒	☐	☐
Fyysinen tallennusväline, pysyvästi luettavissa Tuotteen QR-koodi avaa Passin missä tahansa selaimessa – ilman sovellusta, ilman tiliä, millä tahansa älypuhelimella. EN 18220	☒	☐	☐
Tallennus ja arkistointi vähimmäissäilytysajan ajan Jokainen julkaistu versio pysyy saatavilla lain edellyttämän ajan – myös vanhemmat versiot, ei pelkästään nykyinen. EN 18221	☒	☐	☐

Kriteeri	Transpareo		
Elinkaaren hallinnan ja hakukelpoisuuden sovellusrajapinta (API) Ohjelmointirajapinta lukee, luo ja hakee passeja – se ei ole pelkkä klikkauspohjainen verkkokäyttöliittymä. EN 18222	☒	☐	☐
Yhteentoimiva tietomalli Passin tiedot noudattavat yhteistä mallia, jota muut järjestelmät voivat lukea ilman muotoilun muuttamista. EN 18223	☒	☐	☐
Kolmivaiheinen käyttöoikeusmalli Julkiset, valtuutetut ja viranomaisten tiedot on erotettu selkeästi toisistaan – jokainen näkee tarkalleen sen, mihin hänellä on oikeus. EN 18239	☒	☐	☐
Todennettavissa oleva tietojen aitous ja eheys Jokainen versio on kaksinkertaisesti allekirjoitettu, ja sen aitous voidaan tarkistaa selaimessa – ilman, että sinun tarvitsee luottaa meihin, pelkästään tietojen perusteella. EN 18246	☒	☐	☐
Yhteys EU:n komission rekisteriin Rekisteröinti ja virallinen todistus – heti kun EU julkaisee teknisen rajapinnan. Sitä ei ole vielä saatavilla, joten yksikään palveluntarjoaja ei voi täyttää tätä vaatimusta tällä hetkellä.	☐	☐	☐
Rekisteritietojen säilyttäminen lakisääteisen määräajan jälkeen Muuttumaton kymmenen vuoden arkisto – sen sisältöä ei voi muuttaa jälkikäteen sen enempää valmistaja kuin Transpareo.	☒	☐	☐
Tuotetiedot kunkin kohdemarkkinan virallisilla kielillä Pakolliset tiedot on esitettävä jokaisen sen maan virallisilla kielillä, jossa tuotetta myydään – eli EU:n laajuudessa jakelussa kaikilla 24 virallisella kielellä, ei pelkästään kotimarkkinoilla.	☒	☐	☐

Hyödyllistä DPP-tietokannan ylläpidossa

Kriteeri	Transpareo		
Kielet EU:n ulkopuolella 16 muuta kieltä EU:n 24 virallisen kielen lisäksi - yhteensä 40 kieltä, jotka on tarkoitettu unionin ulkopuolella sijaitseville kohdemarkkinoille.	☒	☐	☐
Versiointi ja muutoshistoria Jokainen muutos luo uuden, jäljitettävän version, jossa on merkitty ajankohta ja tekijä - tuotteen koko elinkaaren ajan.	☒	☐	☐
Skaalautuva massatuotantolaitos tuoteperheille Tuotetietojen lataaminen Excel- tai CSV-tiedostona ja niiden kohdistaminen pakollisiin kenttiin - suurille määrille on lisäksi käytettävissä Bulk-API.	☒	☐	☐
Roolipohjainen sisäinen käyttöoikeuksien hallinta Yrityksessä on määritelty, kuka saa ylläpitää tai jakaa mitään tietoja - mukaan lukien tiukasti rajoitetut, määräaikaisten käyttöoikeudet ulkopuolisille.	☒	☐	☐
Säilytys sopimuksen päättymisen jälkeen Jos irtisanoudut, julkaisemasi passit pysyvät saatavilla muuttumattomana kymmenen vuoden arkistossa.	☒	☐	☐
Allekirjoitus omalla salausavaimella Bring Your Own Key: Te pidätte yksityisavainta itse, me lisäämme siihen vain riippumattoman vastasignatuurin.	☒	☐	☐
Näytteilleasettajan identiteetti riippumatta alustasta Näyttelijän tunnuksesi sijaitsee DID:web-palveluna omalla verkkotunnuksellasi, ei meidän verkkotunnuksellamme - palveluntarjoajan vaihto tarkoittaa DNS-siirtoa.	☒	☐	☐
Kolmannen osapuolen suorittama tarkastettavuus, täysin ilman palveluntarjoajaa Avoimen lähdekoodin renderöintiohjelma tarkistaa hajautusarvot ja allekirjoitukset selaimessa - ottamatta yhteyttä palvelimeemme.	☒	☐	☐

Toivottavia lisätoimintoja

Kriteeri	Transpareo		
Palveluntarjoajan vaihto ilman tietojen menetystä Siirtymävaiheessa otatte mukaan koko passikannan avoimissa tiedostomuodoissa – allekirjoitettuna ja itse tarkistettavissa; sopimuksen päättyessä pakolliset passit pysyvät saatavilla muuttumattomassa kymmenen vuoden arkistossa ilman tietojen menetystä.	☒	☐	☐
Yhteys olemassa oleviin järjestelmiin tietosaaren sijaan Allekirjoitetut webhookit ja Bulk-API integroivat Passin järjestelmiisi – ei valmiita liitäntöjä tiettyä ERP-järjestelmää varten.	☒	☐	☐
Erämuotoinen tuonti ja vienti EU:n lakisäätteisten vaatimusten lisäksi Suurempia tietomääriä voidaan siirtää molempiin suuntiin – ei pelkästään pakollisia kenttiä.	☒	☐	☐

Turvallisuus ja tietosuoja

Kriteeri	Transpareo		
Erillinen tietokanta ja oma avain Tietonne sijaitsevat omassa tietokannassamme, ja ne on salattu omalla avaimella – erillään sekä tietokanta- että salaus tasolla.	☒	☐	☐
Salaus ja varmuuskopiot TLS kaikissa yhteyksissä, arkaluonteisten tietojen AES-salaus sekä salatut varmuuskopiot, joissa käytetään avainten kierrätystä.	☒	☐	☐
Turvallisuustapahtumaloki Kirjautumisyriitykset, MFA-haasteet ja API-avainten käyttö kirjataan lokiin ja säilytetään yhden vuoden ajan.	☒	☐	☐
Monivaiheinen tunnistautuminen Authenticator-sovellus, salasanakoodi tai laitteistokoodi kaikille käyttäjille, sekä varakoodit katoamistapauksia varten.	☒	☐	☐

Kriteeri	Transpareo		
ISO 27001 –sertifioitu webhotelli Saksassa Saksassa sijaitseva palvelin, jossa noudatetaan tiukkoja fyysisiä ja organisatorisia turvatoimenpiteitä.	☒	☐	☐

Taloudelliset ja organisatoriset kysymykset

Kriteeri	Transpareo		
Hoitaako palveluntarjoaja EU-rekisteröinnin puolestasi? Hoidamme rekisteröinnin ja virallisen todistuksen heti, kun EU julkaisee rajapinnan – teille ei aiheudu siitä mitään vaivaa.	☒	☐	☐
Selkeät säännöt tukityön laajuudesta ja tukikustannuksista Transpareossa tuki sisältyy hintaan – ei erillistä tukisopimusta, ei lisäkustannuksia.	☒	☐	☐
Läpinäkyvä hinnoittelurakenne Neljä julkista hinnoittelupakettia kaikenkokoisille yrityksille, ilmainen kokeilujakso, irtisanottavissa milloin tahansa – ilman piilokustannuksia kielen, tuotteen tai API-kutsun mukaan.	☒	☐	☐

Selitykset ja lähteet

Tietojen vaihto avoimessa, standardoidussa muodossa **EN 18216**

Standardi edellyttää, että digitaaliset tuotepassit ovat saatavilla avoimien, standardoitujen protokollien kautta – jotta viranomaiset, yhteistyökumppanit ja omat järjestelmänsä voivat lukea tietoja ilman, että ne ovat sidottuja yhden palveluntarjoajan ohjelmistoon. Suljettu formaatti olisi erillinen saari: ilman palveluntarjoajaa ette enää pääsisi käsiksi omiin tietoihinne. Standardi on julkaistu EU:n virallisessa lehdessä 15. heinäkuuta 2026 (täytäntöönpanopäätös (EU) 2026/1736), ja sen vuoksi sille myönnetään ESPR-vaatimustenmukaisuusolettama.

Transpareo toimittaa kaikki passitiedot ja rajapinnat standardinmukaisen HTTPS-yhteyden kautta jäsennellyssä, koneellisesti luettavassa muodossa – ilman erikoisohjelmistoja tai omistusoikeudellisia

protokollia. Jokainen julkaistu versio on lisäksi allekirjoitettu, jotta vastaanottaja voi paitsi lukea tiedot myös varmistaa, että ne ovat muuttumattomia. Se, mitä näet käyttöliittymässä, on sama tietojoukko, jonka jokainen valtuutettu järjestelmä hakee avoimien rajapintojen kautta.

Lähde: EN 18216, Tietojenvaihtoprotokollia koskevat vaatimukset: ”Standardoidussa DPP-käytössä on käytettävä määriteltyjä tietojenvaihtoprotokollia.”

Yksiselitteinen, siirrettävä tunniste, joka ei ole sidottu tiettyyn palveluntarjoajaan EN 18219

Jokaisella tuotepassilla on oltava yksilöllinen tunniste, joka viittaa pysyvästi samaan tuotteeseen eikä edellytä tiettyä toimittajaa. Jos toimittaja sitoo tunnisteeseen omaan infrastruktuuriinsa, menetätte passienne identiteetin toimittajaa vaihtaessanne – jokainen painettu koodi ja jokainen rekisteröinti menettäisivät silloin merkityksensä. Standardi on julkaistu EU:n virallisessa lehdessä 15. heinäkuuta 2026 alkaen.

Transpareo myöntää tunnisteeseen GS1 Digital Link -muodossa yhdessä GTIN-koodin kanssa – tämä on avoin teollisuusstandardi, joka kuuluu tuotteelle, ei alustalle – ja tarkistaa jokaisen tunnisteeseen hyväksytyjen standardijärjestelmien mukaisesti. Allekirjoituksen identiteetti sijaitsee DID:web-muodossa omalla verkkotunnuksellanne, ei meidän. Tunniste pysyy voimassa, vaikka jokin järjestelmä menisikin epäkuntoon: pysyvä varayhteysosoite jatkaa sen ratkaisemista, ja passi säilyttää identiteettinsä palveluntarjoajan vaihtuessa.

Lähde: EN 18219, kohta 4.6.2(3): ”Yksilöllinen tunniste ei saa johtaa palveluntarjoajaan sitoutumiseen.”

Fyysinen tallennusväline, pysyvästi luettavissa EN 18220

Tuotteen mukana on oltava koneellisesti luettava tietoväline, johon kuka tahansa pääsee käsiksi ilman erityisohjelmistoja – ja joka pysyy luettavissa tuotteen koko elinkaaren ajan, myös käytön ja korjausten jälkeen. Tietoväline, joka edellyttää tiettyä sovellusta tai tiliä, sulkee osan yleisöstä ulkopuolelle. Standardi on julkaistu EU:n virallisessa lehdessä 15. heinäkuuta 2026 alkaen.

Transpareo luo ISO/IEC 18004 -standardin mukaisen QR-koodin, joka sisältää GS1 Digital Link -osoitteen ja avaa passin suoraan missä tahansa selaimessa – ilman kirjautumista, ilman lataamista, millä tahansa älypuhelimella. Malli, erä ja tuote on jo sisällytetty koodattuun osoitteeseen, joten skannaus vie suoraan oikealle tasolle. Koska osoite pysyy vakaana pysyvän vara-resoluution ansiosta, kerran tulostettu koodi pysyy voimassa tuotteen koko elinkaaren ajan.

Lähde: EN 18220, Tietovälineille asetetut vaatimukset (kohta 5): Symboliikka, koodaus, tulostuslaatu ja kestävyys; tietovälineen on oltava luettavissa myös useiden käyttö- ja korjauskierrosten jälkeen.

Tallennus ja arkistointi vähimmäissäilytysajan ajan EN 18221

Standardi edellyttää, että standardi ja sen versiohistoria säilytetään sääntelyn edellyttämän ajan ja että ne ovat saatavilla muuttumattomina. Jos vain kulloinkin voimassa oleva versio säilytetään, aikaisempien tietojen jäljitettävyyden menetetään – ja juuri tämän jäljitettävyyden talouden toimijan on kyettävä osoittamaan viranomaisille. Säilytysaika määräytyy kunkin alan lainsäädännön mukaan, mutta se on vähintään kymmenen vuotta. Standardi on julkaistu EU:n virallisessa lehdessä 15. heinäkuuta 2026 alkaen.

Transpareo tallentaa jokaisen julkaisun jäädytettynä ja allekirjoitettuna versiona muuttumattomaan arkistoon, josta kukaan ei voi myöhemmin muuttaa tai poistaa sitä – ei te eikä me. Vanhemmat versiot ovat saatavilla nykyisen version rinnalla, ja jokaisessa versiossa on aikaleima ja allekirjoitus. Näin voidaan todentaa milloin tahansa, mitä passissa oli kyseisenä ajankohtana.

Lähde: EN 18221: ”Digitaalinen tuotepassi on pidettävä valtuutettujen käyttäjien saatavilla sen koko elinkaaren ajan.”

Elinkaaren hallinnan ja hakukelpoisuuden sovellusrajapinta (API) EN 18222

Selainnäytön lisäksi standardi edellyttää ohjelmointirajapintaa, jonka kautta passeja voidaan luoda, lukea, päivittää ja hakea tuotetunnisteiden perusteella. Ilman tällaista rajapintaa kaikki massakäsittely jää manuaaliseksi, eivätkä muut järjestelmät voi hyödyntää passikantaa automaattisesti. Standardi on julkaistu EU:n virallisessa lehdessä 15. heinäkuuta 2026 alkaen.

Transpareo tukee vaadittuja standardimenetelmiä versionoidun, standardoidun rajapinnan kautta: Passeja voidaan luoda, lukea, päivittää ja hakea sivukohtaisesti tuotetunnisteiden avulla ohjelmoidusti. Allekirjoitettu passi toimitetaan tällöin muuttumattomana – rajapinta palauttaa tarkalleen ne tavut, joiden allekirjoituksen tarkastaja voi laskea uudelleen.

Lähde: EN 18222: standardoitu ohjelmointirajapinta (API) DPP:n elinkaaren hallintaan ja hakukelpoisuuteen, kuten ESPR:ssä vaaditaan.

Yhteentoimiva tietomalli EN 18223

Jotta passit olisivat yhteensopivia järjestelmien välillä ja toimitusketjujen yli, standardi määrää yhteisen tietomallin, jossa kenttien merkitykset ovat yhtenäiset. Toimittajakohtainen malli pakottaa jokaisen kumppanin tekemään oman käännöksensä – ja jokainen käännös on virhelähde. Standardi on julkaistu EU:n virallisessa lehdessä 15. heinäkuuta 2026 alkaen.

Transpareo perustuu horisontaaliseen sanastokerrokseen, jossa on rinnakkaisia, tunnustettuja erikoisalan sanastoja (GS1, EPCIS ja muut), ja se kuvaa jokaisen datapisteen viittaamalla sen sanakirjaan ja tietotyyppiin. Tämän ansiosta vastaanottava järjestelmä saa tietää paitsi kentän nimen myös sen merkityksen – passi pysyy luettavissa ilman uudelleenmuotoilua.

Lähde: EN 18223: yhteinen semanttinen tietomalli DPP:n järjestelmien yhteentoimivuutta varten.

Kolmivaiheinen käyttöoikeusmalli EN 18239

Tuotepassi sisältää julkisia tietoja, valtuutetuille talouden toimijoille tarkoitettuja tietoja sekä yksinomaan viranomaisille tarkoitettuja tietoja; standardi edellyttää, että nämä tasot pidetään erillään ja että niitä säännellään tietokenttäkohtaisesti. Julkisten tietojen on oltava saatavilla ilman kirjautumista, kaikkien muiden tietojen saatavuus edellyttää tunnistautumista. EN 18239 -standardi on viimeisessä hyväksymisvaiheessa.

Transpareo käsittelee näkyvyyttä kunkin tietokentän ominaisuutena: julkinen taso toimitetaan ilman todennusta, korkeammat tasot on suojattu omalla, lokitiedostoihin tallennettavalla viranomaisrajapinnalla, jossa on yksinomaan lukuoikeus, ja jokainen pääsy suojattuihin tietoihin kirjataan tarkastuslokiin. Standardin kolmitasoinen malli on siten jo nyt kuvattu arkkitehtuurissa, eikä sitä ole lisätty jälkikäteen.

Lähde: EN 18239 (luonnos, lopullisessa hyväksymisvaiheessa): "Julkisiin tietoihin pääsyn on oltava mahdollista sekä EU:n että EU:n ulkopuolisten toimijoiden osalta ilman lisääntöntä"; valvotut tiedot edellyttävät autentikoitua ja todistettavaa pääsyä.

Todennettavissa oleva tietojen aitous ja eheys EN 18246

Standardi edellyttää, että passin aitous ja ehyys ovat todennettavissa ja että tarkastus on mahdollista vapaasti ja rajoituksetta. Luottamus ei saa riippua palveluntarjoajan olemassaolosta, vaan sen on perustuttava itse tietueeseen – muuten jokainen passi olisi vain yhtä luotettava kuin yritys, joka sitä kulloinkin ylläpitää. EN 18246 on viimeisessä hyväksymisvaiheessa.

Transpareo allekirjoittaa jokaisen julkaistun version kahdella riippumattomalla avaimella (myöntäjä ja Transpareo) ja linkittää versiot niiden hajautusarvon avulla, jotta myöskään historiaa ei voida muuttaa huomaamatta. Avoimen lähdekoodin renderöntiohjelma tarkistaa molemmat allekirjoitukset suoraan selaimessa ottamatta yhteyttä palvelimeemme – näin vaadittu allekirjoitettu, itsetarkistettava todiste on jo toteutettu.

Lähde: EN 18246 (luonnos, lopullisessa hyväksymisvaiheessa): DPP-tietojen aitous, luotettavuus ja eheys on voitava todentaa.

Yhteys EU:n komission rekisteriin

Jokainen rekisteröintivelvollisuuden alainen passi on jatkossa rekisteröitävä EU:n keskusrekisteriin, joka myöntää pysyvän rekisteröintitunnuksen ja virallisen rekisteröintitodistuksen. EU ei ole vielä julkaissut tätä varten tarvittavaa teknistä rajapintaa – siksi yksikään palveluntarjoaja ei voi tällä hetkellä osoittaa tämän yhteyden toimivuutta; jos joku palveluntarjoaja väittää niin, sinun tulisi kysyä asiasta tarkemmin.

Transpareo on valmistellut yhteyden siinä määrin kuin se on mahdollista ilman rajapintaa: tarvittavat kentät (rekisteröintitunnus, vakaa varakohde, version hash-arvo) on jo luotu tietomalliin. Heti kun EU

julkaisee rajapinnan, aktivoimme rekisteröinnin ilman, että teidän tarvitsee muuttaa passejanne. Siihen asti tämä kohta jää avoimeksi – niin meillä kuin kaikilla rehellisillä palveluntarjoajilla.

Lähde: DPP-rekisterin täytäntöönpanoasetuksen luonnos (Ares(2026)4424976).

Rekisteritietojen säilyttäminen lakisääteisen määräajan jälkeen

Rekisteröidyt passitiedot on säilytettävä muuttumattomina lakisääteisen määräajan ajan – yleensä kymmenen vuotta rekisteröinnistä – myös valmistajan konkurssin tai toiminnan lopettamisen jälkeen. Velvollisuus on siis voimassa sekä palveluntarjoajan kanssa tehdyn sopimuksen että palveluntarjoajan itsensä jälkeen.

Transpareo ylläpitää tätä varten muuttumatonta arkistoa, jossa kertaa tallennettua versiota kukaan ei voi jälkikäteen muuttaa tai poistaa – ei valmistaja eikä me. Arkisto otetaan käyttöön automaattisesti EU-rekisteröinnin yhteydessä. Ja jotta se pysyy saatavilla myös siinä tapauksessa, että Transpareo jonain päivänä lakkaisi olemasta, sen säilymisen turvaa notaarin toimesta Sveitsissä tehty talletus.

Lähde: DPP-rekisterin täytäntöönpanoasetus, 10 §:n 3 momentti (säilytysaika kymmenen vuotta).

Tuotetiedot kunkin kohdemarkkinan virallisilla kielillä

Passin pakollisten tietojen on oltava saatavilla jokaisen sen jäsenvaltion virallisilla kielillä, jossa tuote tuodaan markkinoille – ei pelkästään valmistajan kotipaikan kielellä. Pelkästään kotimarkkinoita palveleva yritys ei täytä vaatimusta kaikkien muiden kohdemarkkinoiden osalta.

Transpareo ylläpitää jokaista passia monikielisenä ja toimittaa pakollisen sisällön kaikilla 24 EU:n virallisella kielellä. Syötätte sisällön kerran; kieliversiot luodaan siitä ilman, että joudutte maksamaan lisämaksua kielikohtaisesti tai ylläpitämään erillisiä passeja. Passi on siten luettavissa säännösten mukaisesti jokaisella kohdemarkkinalla.

Lähde: Akkuasetus (EU) 2023/1542: Tiedot niiden jäsenvaltioiden virallisilla kielillä, joissa tuote saatetaan markkinoille.

Kielet EU:n ulkopuolella

Lakisääteisen veloitteen lisäksi on hyödyllistä, jos tuoteseloste kattaa myös EU:n ulkopuoliset kielet – vientimarkkinoiden, kansainvälisten kauppakumppaneiden ja kuluttajien vuoksi, jotka eivät puhu unionin virallista kieltä.

Transpareo ylläpitää yhteensä 40 kieliversiota, mukaan lukien 24 EU:n virallista kieltä. Syötätte sisällön kerran ja tuotatte sen haluamallanne kielellä ilman kielikohtaisia lisämaksuja. Myös käyttöliittymä, jossa hallinnoitte passejanne (sovellushallinta), on käännetty kaikille 40 kielelle, ja voitte syöttää tietoja millä tahansa käytettävissä olevalla kielellä.

Versiointi ja muutoshistoria

Passi muuttuu tuotteen elinkaaren aikana; ilman aukotonta versiohistoriaa ei voida myöhemmin todistaa, mikä versio oli voimassa milloin. Standardi edellyttää siksi, että kaikki passiin tehdyt muutokset arkistoidaan.

Transpareo tallentaa jokaisen julkaisun erillisenä, allekirjoitettuna versiona ja kirjaa ylös, kuka sen on luonut, milloin ja mitkä kentät on muutettu. Näin jokainen tieto voidaan tarkistaa takautuvasti, eikä myöhempi korjaus korvaa historiaa, vaan jatkaa sitä.

Lähde: EN 18221: "Kaikki digitaaliseen tuotepassiin tehdyt muutokset on arkistoitava."

Skaalautuva massatuotantolaitos tuoteperheille

Jos valikoimassa on paljon samankaltaisia tuotteita, kaikkia tuotetietoja ei voi luoda yksitellen käsin; toimiva järjestelmä tarvitsee tavan tallentaa kokonaisia tuoteryhmiä kerralla.

Transpareon avulla voit ladata tuotetietoja Excel- tai CSV-tiedostoina ja kohdistaa ne pakollisiin kenttiin; erittäin suurille määriille on lisäksi käytettävissä Bulk-API, joka luo tuotetiedot ohjelmoidusti. Näin järjestelmä skaalautuu kymmenestä tuotetiedosta jopa kymmeneen tuhansiin.

Roolipohjainen sisäinen käyttöoikeuksien hallinta

Kaikilla yrityksen työntekijöillä ei tule olla oikeutta muokata tai hyväksyä kaikkia passin sisältöjä; standardi edellyttää roolipohjaista käyttöoikeuksien hallintaa, jossa käyttöoikeudet kirjataan lokiin.

Transpareo myöntää käyttöoikeudet roolin ja käyttäjäryhmän mukaan ja kirjaa jokaisen muutoksen. Myös ulkopuoliset tahot, kuten korjaamot tai kierrättäjät, saavat vain tiukasti rajoitettuja, määräaikaista käyttöoikeuksia; viranomaiset pääsevät järjestelmään erillisen, yksinomaan lukuoikeuksin varustetun rajapinnan kautta, joka merkitsee jokaisen käyttökerran auditointilokiin.

Lähde: EN 18239 (luonnos), Käyttöoikeuksien hallinta: määrittelee, mitkä toimijat saavat ylläpitää ja jakaa DPP-tietoja.

Säilytys sopimuksen päättymisen jälkeen

Säilytysvelvollisuus ei pääty sopimuksen päättyessä: rekisteröity passi on säilyttävä lakisääteisen määräajan ajan, vaikka lopettaisitkin palveluntarjoajan palvelujen käytön. Palveluntarjoaja, joka poistaa passit käytöstä sopimuksen irtisanomisen yhteydessä, aiheuttaa sinulle sääntöjen noudattamiseen liittyvän ongelman.

Transpareo huolehtii tästä samalla muuttumattomalla kymmenen vuoden arkistolla kuin rekisteröintitietojakin – irtisanomisen jälkeen pysyvä varasivusto toimittaa passit edelleen, ja viranomaisten rajapinta lukee saman tietueen sopimuksen päättymisen jälkeisestä arkistosta. Jo tulostetut QR-koodit pysyvät voimassa.

Lähde: EN 18221: Arkistoversiot tallennetaan myös varmuuskopiointipalveluntarjoajan palvelimille.

Allekirjoitus omalla salausavaimella

Se, jolla on hallussaan yksityinen allekirjoitusavain, voi luoda passeja myöntäjän nimissä; siksi on turvallisempaa, että myöntäjä säilyttää tämän avaimen itse sen sijaan, että luovuttaisi sen palveluntarjoajalle.

Bring Your Own Key -ratkaisun avulla yrityksesi ylläpitää omaa allekirjoituspäätelaitetta – Transpareo ei koskaan säilytä yksityistä avainta, vaan lisää vain riippumattoman vastallekirjoituksen. Näin jokaisessa versiossa on kaksi toisistaan riippumatonta allekirjoitusta, ja myöntäjän allekirjoitus on sellainen, jota Transpareo ei itse voi luoda.

Näytteilleasettajan identiteetti riippumatta alustasta

Jotta tarkastaja löytää julkiset avaimesi, passissa on oltava julkaistu myöntäjän identiteetti. Jos se sijaitsee palveluntarjoajan verkkotunnuksella, se sitoo sinut kyseiseen palveluntarjoajaan: palveluntarjoajan vaihtaminen mitätöisi kaikki jo tulostetut koodit.

Transpareo julkaisee identiteettisi DID-tunnuksena: verkossa omalla verkkotunnuksellasi, ei meidän verkkotunnuksellamme – palveluntarjoajan vaihto on siten vain DNS-siirto, ja jo painetut koodit sekä niiden varmennus pysyvät voimassa. Lisäksi peilaamme jokaisen julkisen avaimen julkaisuhetkellä pysyvään osoitteeseen, jotta jokainen versio pysyy todennettavissa, vaikka alkuperäinen isäntä katoaisikin.

Lähde: EN 18219, kohta 4.2.2 (Pysyvyys): Tunnisteet säilyvät koko elinkaaren ajan; verkkotunnukset ovat siirrettävissä tai uudelleenohjattavissa.

Kolmannen osapuolen suorittama tarkastettavuus, täysin ilman palveluntarjoajaa

Luottamuksen ratkaiseva testi on se, voiko kolmas osapuoli tarkistaa passin ilman palveluntarjoajan infrastruktuuria. Standardi edellyttää, että voimassaolon ja eheyden tarkistaminen on tarkastajalle maksutonta ja rajoituksetta mahdollista.

Transpareo julkaisee tätä varten avoimen lähdekoodin renderöintiohjelman, joka lataa version tavut mistä tahansa lähteestä, laskee hajautusarvon uudelleen ja tarkistaa molemmat allekirjoitukset passissa mainittuja julkisia avaimia vastaan – ilman kirjautumista, ilman puhelua meille, ilman riippuvuutta käynnissä olevasta alustasta. Epäileväinen voi lukea lähdekoodin.

Lähde: EN 18246 (luonnos): ”Tarkastajan on voitava tarkistaa DPP-tietojen oikeellisuus ja eheys ilman kustannuksia ja rajoituksia.”

Palveluntarjoajan vaihto ilman tietojen menetystä

Palveluntarjoaja, joka vaikeuttaa palvelun vaihtamista, pitää sinut kiinni omien tietojesi avulla – ja se, mitä tiedoille tapahtuu sopimuksen päättyessä, ratkaisee, voitko vaihtaa palveluntarjoajaa vapaasti.

Standardi edellyttää siksi, että tiedot ovat siirrettävissä avoimen, yhteentoimivan verkon kautta ilman sidonnaisuutta tiettyyn palveluntarjoajaan.

Transpareo tallentaa sääntelyyn liittyvät tiedot alusta alkaen avoimeen, julkisesti peilattavaan alueeseen: yksinkertainen synkronointi luo täydellisen, allekirjoitetun kopion, joka tarkistaa itsensä julkaistujen avainten avulla ilman meidän toimiamme. Toimitamme täydellisen tapahtuma-arkiston allekirjoitetun, ajallisesti rajoitetun latausosoitteen kautta sinulle tai uudelle palveluntarjoajallesi, ja sitä edeltävän tuoteluettelon lisäksi JSON-LD- ja CSV-muodoissa. Sopimuksen päättyessä rekisteröidyt pakolliset tiedot ovat edelleen saatavilla muuttumattomassa kymmenen vuoden arkistossa: Julkinen peilaus ja arkisto pysyvät synkronoituna ja välittävät samaa tietokantaa, jo tulostetut QR-koodit toimivat edelleen pysyvän varasivun osoitteen kautta, ja rekisteriviite osoittaa uuteen osoitteeseen. Näin sopimus päättyy ilman tietojen menetystä ja lakisääteisen säilytysvelvollisuuden rikkomista.

Lähde: EN 18216: Tietojen on oltava ”siirrettävissä avoimen, yhteentoimivan verkon kautta ilman sitoutumista tiettyyn palveluntarjoajaan”.

Yhteys olemassa oleviin järjestelmiin tietosaaren sijaan

Vain palveluntarjoajan käyttöliittymässä toimiva Pass muuttuu muiden järjestelmienne rinnalla toimivaksi tietosaareksi – jokainen muutos on tällöin tehtävä kahteen kertaan.

Transpareo ilmoittaa tapahtumista allekirjoitettujen webhookkien kautta ja mahdollistaa tietojen tuonnin ja viennin Bulk-API:n kautta, jolloin voit integroida Passin omaan järjestelmäympäristösi. Emme tarkoituksella toimita valmiita liitäntöjä tiettyjä ERP-järjestelmiä varten – avoimet, allekirjoitetut rajapinnat sopivat mihin tahansa järjestelmään sen sijaan, että suosittaisimme yhtä tiettyä järjestelmää.

Erämuotoinen tuonti ja vienti EU:n lakisääteisten vaatimusten lisäksi

Jos haluat käyttää kerättyjä tietoja myös passin ulkopuolella, tarvitset tuonti- ja vientitoimintoja, jotka kattavat muutakin kuin lakisääteiset pakolliset kentät.

Transpareo vastaanottaa suuria tietomääriä Excelin, CSV-tiedostojen ja Bulk-API:n kautta ja toimittaa ne takaisin samassa laajuudessa. Näin järjestelmä ei palvele pelkästään EU:n velvoitteiden täyttämistä, vaan myös omaa tietojenhallintaa.

Erillinen tietokanta ja oma avain

Jaetussa tietokannassa tietosi ovat yhteydessä muiden asiakkaiden tietoihin; selkeä ja todistettavissa oleva erottelu on tällöin lähes mahdotonta – ja GDPR:n 17 artiklan mukaista oikeutta tietojen poistamiseen on vaikea osoittaa.

Transpareossa jokaisella asiakkaalla on oma tietokanta, joka on salattu omalla avaimella – erottelu tapahtuu sekä tietokanta- että salaus tasolla. Tämä täyttää poistamisoikeuden vaatimukset todennettavalla poistamisella; palvelin sijaitsee Saksassa, ja tietojenkäsittelysopimus (AVV) sisältyy pakettiin.

Lähde: GDPR:n 17 artikla (oikeus tietojen poistamiseen), joka täytetään erillisellä tietokannalla, omalla avaimella ja todennettavissa olevalla poistamisella.

Salaus ja varmuuskopiot

Palveluntarjoajan on suojattava tiedot sekä siirron aikana että lepotilassa ja varmistettava niiden saatavuus; GDPR edellyttää tätä varten tekniikan tasoa vastaavia toimenpiteitä.

Transpareo salaa kaikki yhteydet TLS:llä ja arkaluonteiset sovellustiedot AES:llä. Varmuuskopiot on salattu GPG:llä, niitä päivitetään säännöllisellä avainvaihdolla, ne luodaan neljän tunnin välein ja säilytetään 12 kuukauden ajan erillisellä palvelimella.

Lähde: GDPR:n 32 artikla (käsittelyn turvallisuus): TLS, AES ja salatut varmuuskopiot, joissa käytetään kierrätystä.

Turvallisuustapahtumaloki

Turvallisuuden kannalta merkittävien tapahtumien on oltava jäljitettävissä – kuka on kirjautunut sisään milloin ja miten avaimia on käytetty. NIS-2-direktiivi edellyttää vastaavia tarkastuslokeja.

Transpareo pitää turvallisuustapahtumalokia kirjautumisyryksistä, monivaiheisen todennuksen (MFA) haasteista ja API-avainten käytöstä sekä säilyttää sitä yhden vuoden ajan. Näin NIS-2-direktiivin auditointilokeja koskevat vaatimukset täyttyvät.

Lähde: NIS-2-direktiivi (auditointilokeja koskevat vaatimukset): kirjattavat tietoturvatapahtumat, säilytysaika yksi vuosi.

Monivaiheinen tunnistautuminen

Yksi ainoa salasana tarjoaa vain heikon suojan; NIS-2-direktiivi edellyttää pääsynvalvontaa monivaiheisen todennuksen avulla.

Transpareo tarjoaa monivaiheisen todennuksen kaikille sovellushallinnan käyttäjille – joko Authenticator-sovelluksen, Passkey-avaimen tai laitteistokoodin avulla – sekä varakoodit kadotustapauksia varten. Monivaiheisen todennuksen käyttö voidaan asettaa pakolliseksi tilillesi.

Lähde: NIS-2-direktiivi (pääsynvalvonta ja monivaiheinen todennus).

ISO 27001 –sertifioitu webhotelli Saksassa

Palvelimien sijainti ja tietokeskuksen suojaus ratkaisevat tietojenne fyysisen turvallisuuden – sekä sen, minkä lainsäädännön alaisuudessa ne ovat.

Transpareo ylläpitää palvelimiaan Saksassa sijaitsevilla ISO 27001 –sertifoiduilla palvelimilla, joihin sovelletaan tiukkoja fyysisiä ja organisatorisia turvatoimenpiteitä. Saksan sijainti takaa lisäksi, että tietojasi käsitellään täysin eurooppalaisen lainsäädännön mukaisesti.

Lähde: ISO/IEC 27001 (tietoturvan hallinta), sertifioitu tietokeskus Saksassa.

Hoitaako palveluntarjoaja EU–rekisteröinnin puolestasi?

Rekisteröityminen EU–rekisteriin ja virallisen todistuksen hankkiminen ovat toistuvia tehtäviä, jotka palveluntarjoaja voi hoitaa puolestanne. Rekisteriasetuksessa määrätään tästä nimenomaisesti: palveluntarjoaja saa hoitaa rekisteröinnin toimeksiannosta, mutta oikeudellinen vastuu säilyy talouden toimijalla.

Transpareo rekisteröi passisi puolestasi heti, kun EU julkaisee teknisen rajapinnan – sinä pysyt oikeudellisesti vastuullisena talouden toimijana, mutta et joudu kantamaan operatiivista työmäärää. Ennen kuin rajapinta on käytettävissä, kukaan ei voi tarjota tätä palvelua; olemme jo valmistelleet tarvittavat tiedot tätä varten.

Lähde: DPP–rekisterin täytäntöönpanoasetus (luonnos), 19 §: Palveluntarjoaja voi hoitaa rekisteröinnin toimeksiannosta; vastuu säilyy talouden toimijalla.

Selkeät säännöt tukityön laajuudesta ja tukikustannuksista

Jotkut palveluntarjoajat erottavat palvelun käytön ja tuen toisistaan ja laskuttavat tuesta erikseen; lopputuloksena yhteistyön kustannuksia on vaikea arvioida.

Transpareolla tuki sisältyy hintaan – ei erillistä tukisopimusta, ei työmäärän mukaan laskutettavia lisätunteja. Tarvitsemasi tuki sisältyy jo ilmoitettuun hintaan.

Läpinäkyvä hinnoittelurakenne

Hintarakenne, joka selviää vasta myyntineuvottelussa tai jota laskutetaan kielen, tuotteen ja rajapintakutsun mukaan, tekee todellisista kustannuksista arvaamattomia.

Transpareo julkaisee verkkosivuillaan avoimesti neljä hintapakettia kaikenkokoisille yrityksille, joihin sisältyy ilmainen kokeilujakso ja jotka voidaan irtisanoa milloin tahansa. Kielikohtaisia, tuotekohtaisia tai rajapintakutsukohtaisia piilokustannuksia ei ole – ilmoitettu hinta on lopullinen hinta.