

Hoja de comparación de proveedores de DPP

Solo se marca con una cruz las funciones ya existentes y verificables; no se incluyen anuncios ni declaraciones de intenciones. La columna «Transpareo» ya está rellena; las dos columnas vacías las rellenará usted al evaluar a otros proveedores. Al final del documento encontrará explicaciones y fuentes para cada criterio.

Fecha: 10.09.2026

Obligatorio por ley

Criterio	Transpareo		
Intercambio de datos en un formato abierto y estandarizado Los datos de los pases están disponibles mediante estándares abiertos, de modo que cualquier sistema autorizado puede leerlos, no solo el software de un único proveedor. EN 18216	☒	☐	☐
Identificador único y portátil, independiente del proveedor El identificador del producto forma parte del producto, no de la plataforma: al cambiar de proveedor, el pase conserva su identidad. EN 18219	☒	☐	☐
Soporte físico, legible de forma permanente El código QR que aparece en el producto te lleva a la ficha del producto en cualquier navegador, sin necesidad de una aplicación ni de una cuenta, y desde cualquier smartphone. EN 18220	☒	☐	☐

Criterio	Transpareo		
Conservación y archivo durante el plazo mínimo Todas las versiones publicadas permanecerán disponibles durante el plazo establecido por la ley, incluidas las versiones anteriores, no solo la actual. EN 18221	☒	☐	☐
API para la gestión del ciclo de vida y la capacidad de búsqueda Una interfaz de programación que lee, crea y busca pasaportes; no es solo una interfaz web en la que hay que hacer clic. EN 18222	☒	☐	☐
Modelo de datos interoperable Los datos de los pasaportes siguen un modelo común que otros sistemas pueden leer sin necesidad de reformatearlos. EN 18223	☒	☐	☐
Modelo de derechos de acceso de tres niveles Los datos públicos, autorizados y administrativos están claramente separados: cada uno ve exactamente aquello a lo que tiene derecho. EN 18239	☒	☐	☐
Autenticidad e integridad verificables de los datos Cada versión cuenta con doble firma y se puede verificar en el navegador, sin necesidad de confiar en nosotros, basándose únicamente en los datos. EN 18246	☒	☐	☐
Conexión con el registro de la Comisión Europea Registro con documento oficial acreditativo, tan pronto como la UE publique la interfaz técnica. Todavía no está disponible, por lo que ningún proveedor puede cumplir este requisito en la actualidad.	☐	☐	☐
Conservación de los datos de registro más allá del plazo legal Un archivo inalterable de diez años: ni el fabricante ni Transpareo pueden modificar una versión a posteriori.	☒	☐	☐

Criterio	Transpareo		
Datos de los productos en las lenguas oficiales de cada mercado de destino La información obligatoria aparece en las lenguas oficiales de cada país en el que se comercializa el producto; por lo tanto, en el caso de la distribución en toda la UE, en las 24 lenguas oficiales, y no solo en el mercado nacional.	☒	☐	☐

Recomendado para el funcionamiento de una base de datos DPP

Criterio	Transpareo		
Idiomas más allá de la UE 16 idiomas más, además de las 24 lenguas oficiales de la UE: 40 en total, para mercados objetivo fuera de la Unión.	☒	☐	☐
Control de versiones e historial de cambios Cada modificación genera una nueva versión trazable, con la fecha y el autor, a lo largo de todo el ciclo de vida del producto.	☒	☐	☐
Planta de producción a gran escala y adaptable para familias de productos Sube los datos de los productos en formato Excel o CSV y asígnalos a los campos obligatorios; para grandes volúmenes, también hay disponible una API de importación masiva.	☒	☐	☐
Gestión interna de derechos basada en roles Está regulado quién puede gestionar o compartir qué datos en la empresa, incluyendo accesos muy limitados y temporales para personas externas.	☒	☐	☐
Conservación de los datos más allá de la fecha de finalización del contrato Si cancela su suscripción, sus pases publicados seguirán estando disponibles en el archivo inalterable de diez años.	☒	☐	☐

Criterio	Transpareo		
Firma con clave criptográfica propia «Bring Your Own Key»: Usted es quien conserva la clave privada; nosotros solo añadimos una contrasignatura independiente.	☒	☐	☐
Identidad del expositor independiente de la plataforma Su identidad de expositor, DID:web, se aloja en su propio dominio, no en el nuestro; cambiar de proveedor supone un traslado de DNS.	☒	☐	☐
Verificabilidad por parte de terceros, sin necesidad alguna de recurrir al proveedor Un renderizador de código abierto comprueba los hash y las firmas en el navegador, sin necesidad de ponerse en contacto con ninguno de nuestros servidores.	☒	☐	☐

Funciones adicionales deseables

Criterio	Transpareo		
Cambio de proveedor sin pérdida de datos Al realizar el cambio, se lleva consigo todo el inventario de pases en formatos abiertos – firmados y con auto-comprobación – ; al finalizar el contrato, los pases obligatorios siguen estando disponibles en un archivo inalterable de diez años, sin pérdida de datos.	☒	☐	☐
Integración con los sistemas existentes en lugar de crear una «isla de datos» Los webhooks firmados y una API masiva permiten integrar Pass en sus sistemas; no se trata de un conector predefinido para un ERP concreto.	☒	☐	☐
Importación y exportación por lotes más allá de las obligaciones mínimas de la UE Se pueden transferir grandes volúmenes de datos en ambas direcciones, no solo los campos obligatorios.	☒	☐	☐

Seguridad y protección de datos

Criterio	Transpareo		
Base de datos independiente y clave propia Sus datos se almacenan en una base de datos propia, cifrados con una clave propia, y se mantienen separados tanto a nivel de base de datos como a nivel de cifrado.	☒	☐	☐
Cifrado y copias de seguridad TLS para todas las conexiones, cifrado AES de los datos confidenciales y copias de seguridad cifradas con rotación de claves.	☒	☐	☐
Registro de incidentes de seguridad Los intentos de inicio de sesión, las solicitudes de autenticación multifactorial (MFA) y la actividad relacionada con las claves API se registran y se conservan durante un año.	☒	☐	☐
Autenticación multifactorial Aplicación de autenticación, clave de acceso o llave física para todos los usuarios, con códigos de seguridad en caso de pérdida.	☒	☐	☐
Alojamiento web certificado según la norma ISO 27001 en Alemania Servidores ubicados en Alemania con estrictas medidas de seguridad físicas y organizativas.	☒	☐	☐

Cuestiones económicas y organizativas

Criterio	Transpareo		
¿Se encarga el proveedor de tramitar el registro en la UE por ti? Nos encargaremos del registro, incluido el certificado oficial, tan pronto como la UE publique la interfaz; así, usted no tendrá que hacer nada.	☒	☐	☐

Criterio	Transpareo		
Normativa clara sobre el esfuerzo y los costes de asistencia técnica En Transpareo, la asistencia técnica está incluida en el precio: no hay ningún contrato de asistencia técnico por separado ni costes adicionales.	☒	☐	☐
Estructura de precios transparente Cuatro tarifas públicas para empresas de cualquier tamaño, periodo de prueba gratuito, cancelable en cualquier momento, sin costes adicionales ocultos por idioma, producto o llamada a la API.	☒	☐	☐

Notas explicativas y fuentes

Intercambio de datos en un formato abierto y estandarizado EN 18216

La norma exige que los pasaportes digitales de los productos sean accesibles a través de protocolos abiertos y estandarizados, de modo que las autoridades, los socios y sus propios sistemas puedan leer los datos sin estar vinculados al software de un proveedor concreto. Un formato propietario sería una «isla»: sin el proveedor, ya no podría acceder a sus propios datos. La norma figura en el Diario Oficial de la UE desde el 15 de julio de 2026 (Decisión de Ejecución (UE) 2026/1736) y, por lo tanto, goza de la presunción de conformidad con el ESPR.

Transpareo proporciona todos los datos de pases e interfaces a través de HTTPS estándar en un formato estructurado y legible por máquina, sin software especial ni protocolos propietarios. Además, cada versión publicada está firmada, de modo que el destinatario no solo puede leer los datos, sino también comprobar que no han sido modificados. Lo que se ve en la interfaz es el mismo conjunto de datos que cualquier sistema autorizado recupera a través de las interfaces abiertas.

Fuente: EN 18216, Requisitos para los protocolos de intercambio de datos: «Para el acceso estandarizado al DPP, deben utilizarse los protocolos de intercambio de datos establecidos».

Identificador único y portátil, independiente del proveedor EN 18219

Cada pasaporte de producto debe tener un identificador único que remita de forma permanente al mismo producto y que no dependa de ningún proveedor. Si un proveedor vincula el identificador a su propia infraestructura, en caso de cambio perderá la identidad de sus pasaportes: cada código impreso y cada registro quedarían entonces sin referencia. La norma figura en el Diario Oficial de la UE desde el 15 de julio de 2026.

Transpareo asigna el identificador como GS1 Digital Link junto con su GTIN - un estándar industrial abierto que pertenece al producto, no a la plataforma - y comprueba cada identificador según los esquemas normativos autorizados. La identidad de la firma se encuentra como DID:web en su propio dominio, no en el nuestro. El identificador sigue siendo válido incluso si un sistema falla: una dirección de respaldo permanente sigue resolviéndolo, y el pase conserva su identidad independientemente de cualquier cambio de proveedor.

Fuente: EN 18219, apartado 4.6.2(3): «El identificador único no debe dar lugar a una vinculación con un proveedor».

Soporte físico, legible de forma permanente EN 18220

El pasaporte debe estar disponible en el producto a través de un soporte de datos legible por máquina, al que cualquiera pueda acceder sin necesidad de software especial, y que siga siendo legible durante toda la vida útil del producto, incluso tras su uso y reparación. Un soporte de datos que requiera una aplicación o una cuenta concretas excluye a una parte del público. La norma figura en el Diario Oficial de la UE desde el 15 de julio de 2026.

Transpareo genera un código QR conforme a la norma ISO/IEC 18004, que contiene una dirección GS1 Digital Link y que, en cualquier navegador, redirige directamente al pasaporte: sin necesidad de iniciar sesión, sin descargas y compatible con cualquier smartphone. El modelo, el lote y el artículo ya están incluidos en la dirección codificada, de modo que al escanearla se accede directamente al nivel correcto. Dado que la dirección se mantiene estable gracias a una resolución de respaldo permanente, un código impreso una sola vez sigue siendo válido durante toda la vida útil del producto.

Fuente: EN 18220, Requisitos para los soportes de datos (apartado 5): simbología, codificación, calidad de impresión y durabilidad; el soporte de datos debe seguir siendo legible incluso tras varios ciclos de uso y reparación.

Conservación y archivo durante el plazo mínimo EN 18221

La norma exige que una especificación, junto con su historial de versiones, se conserve durante el plazo establecido por la normativa y permanezca accesible sin modificaciones. Si solo se conserva la versión actual, se pierde la trazabilidad de los datos anteriores, que es precisamente lo que un agente económico debe poder demostrar ante las autoridades. El plazo de conservación se rige por la legislación sectorial correspondiente, siendo como mínimo de diez años. La norma figura en el Diario Oficial de la UE desde el 15 de julio de 2026.

Transpareo guarda cada publicación como una versión congelada y firmada en un archivo inalterable, en el que nadie podrá modificarla ni borrarla posteriormente, ni usted ni nosotros. Las versiones anteriores siguen estando disponibles junto a la actual, y cada versión lleva un sello de fecha y hora y una firma. De este modo, se puede demostrar en cualquier momento qué datos figuraban en el pasaporte en ese momento.

Fuente: EN 18221: «El pasaporte digital del producto debe estar a disposición de los usuarios autorizados durante toda su vida útil».

API para la gestión del ciclo de vida y la capacidad de búsqueda EN 18222

Además de la visualización en el navegador, la norma exige una interfaz de programación que permita crear, leer y actualizar pasaportes, así como realizar búsquedas mediante identificadores de producto. Sin dicha interfaz, cualquier procesamiento masivo debe realizarse manualmente, y otros sistemas no pueden utilizar automáticamente el registro de pasaportes. La norma se publicó en el Diario Oficial de la UE el 15 de julio de 2026.

Transpareo cumple con los métodos normativos prescritos a través de una interfaz estandarizada y con control de versiones: Los pasaportes pueden crearse, leerse, actualizarse y buscarse página por página mediante identificadores de producto, todo ello controlado por programa. El pasaporte firmado se entrega sin modificaciones: la interfaz devuelve exactamente los bytes cuya firma puede verificar un auditor.

Fuente: EN 18222: interfaz de programación de aplicaciones (API) estandarizada para la gestión del ciclo de vida y la capacidad de búsqueda del DPP, tal y como exige el ESPR.

Modelo de datos interoperable EN 18223

Para que los países sean compatibles entre sistemas y a lo largo de las cadenas de suministro, la norma establece un modelo de datos común con un significado uniforme de los campos. Un modelo propio de cada proveedor obliga a cada socio a realizar su propia traducción, y cada traducción es una fuente de errores. La norma figura en el Diario Oficial de la UE desde el 15 de julio de 2026.

Transpareo se basa en una capa de vocabulario horizontal con vocabularios técnicos paralelos y reconocidos (GS1, EPCIS y otros) y describe cada punto de datos haciendo referencia a su diccionario y a su tipo de datos. De este modo, un sistema receptor no solo sabe cómo se llama un campo, sino también qué significa; el pasaporte sigue siendo legible sin necesidad de reformatearlo.

Fuente: EN 18223: modelo de datos semántico común para la interoperabilidad del sistema DPP.

Modelo de derechos de acceso de tres niveles EN 18239

Un pasaporte de producto contiene información pública, datos destinados a los agentes económicos autorizados y datos reservados exclusivamente a las autoridades; la norma exige que estos niveles se mantengan separados y se regulen por cada campo de datos. Los datos públicos deben ser accesibles sin necesidad de registrarse, mientras que el resto solo tras una verificación. La norma EN 18239 se encuentra en fase de aprobación definitiva.

Transpareo gestiona la visibilidad como una propiedad de cada campo de datos: el nivel público se facilita sin necesidad de autenticación, los niveles superiores están protegidos mediante una interfaz

específica para las autoridades, con acceso exclusivamente de lectura y registrada en un protocolo, y cada acceso a los datos protegidos queda registrado en el registro de auditoría. De este modo, el modelo de tres niveles de la norma ya está integrado en la arquitectura actual, y no se ha añadido a posteriori.

Fuente: EN 18239 (borrador, en fase de aprobación definitiva): «El acceso a los datos públicos debe ser posible para los agentes de la UE y de fuera de la UE sin necesidad de autenticación adicional»; los datos controlados requieren un acceso autenticado y verificable.

Autenticidad e integridad verificables de los datos EN 18246

La norma exige que la autenticidad y la integridad de un pasaporte sean verificables y que su comprobación sea libre e ilimitada. La confianza no debe depender de la continuidad del proveedor, sino que debe basarse en el propio conjunto de datos; de lo contrario, cada pasaporte tendría tanta credibilidad como la empresa que lo aloja en cada momento. La norma EN 18246 se encuentra en fase de aprobación definitiva.

Transpareo firma cada versión publicada con dos claves independientes (la del emisor y la de Transpareo) y encadena las versiones mediante su hash, de modo que tampoco se pueda reescribir el historial sin que se detecte. Un renderizador de código abierto comprueba ambas firmas directamente en el navegador, sin necesidad de ponerse en contacto con ninguno de nuestros servidores; de este modo, ya se cumple el requisito de una prueba firmada y autocomprobable.

Fuente: EN 18246 (borrador, en fase de aprobación definitiva): La autenticidad, la fiabilidad y la integridad de los datos del DPP deben poder demostrarse.

Conexión con el registro de la Comisión Europea

En el futuro, todos los pasaportes sujetos a registro deberán figurar en el registro central de la UE, que expedirá un número de identificación de registro permanente y un certificado oficial de registro. La UE aún no ha publicado la interfaz técnica necesaria para ello, por lo que, a día de hoy, ningún proveedor puede demostrar que dispone de esta conexión; si algún proveedor lo afirma, debería preguntarle al respecto.

Transpareo ha preparado la conexión en la medida de lo posible sin disponer aún de la interfaz: los campos necesarios para ello (identificador de registro, dirección de respaldo estable, hash de versión) ya están creados en el modelo de datos. En cuanto la UE publique la interfaz, activaremos el registro sin que tenga que modificar sus pases. Hasta entonces, esta cuestión seguirá pendiente, tanto para nosotros como para cualquier proveedor honesto.

Fuente: Proyecto de Reglamento de aplicación del Registro de la DPP (Ares(2026)4424976).

Conservación de los datos de registro más allá del plazo legal

Los datos de registro deben permanecer disponibles sin modificaciones durante el plazo legal – por regla general, diez años a partir del registro –, incluso en caso de insolvencia o cese de la actividad del fabricante. Por lo tanto, esta obligación perdura tanto más allá de su contrato con un proveedor como más allá de la propia existencia del proveedor.

Para ello, Transpareo mantiene un archivo inalterable en el que, una vez guardada una versión, nadie puede modificarla ni borrarla posteriormente, ni el fabricante ni nosotros. El archivo entra en vigor automáticamente con el registro de la UE. Y para garantizar que siga siendo accesible incluso si algún día Transpareo dejara de existir, su continuidad está asegurada mediante un depósito notarial en Suiza.

Fuente: Reglamento de aplicación del Registro DPP, art. 10, apartado 3 (conservación durante diez años).

Datos de los productos en las lenguas oficiales de cada mercado de destino

Los datos obligatorios de un pasaporte deben figurar en las lenguas oficiales de cada Estado miembro en el que se comercialice el producto, y no solo en la lengua del país donde tiene su sede el fabricante. Quien solo comercialice en su mercado nacional no cumple con la obligación para todos los demás mercados de destino.

Transpareo gestiona cada pasaporte en varios idiomas y proporciona el contenido obligatorio en las 24 lenguas oficiales de la UE. Solo tiene que introducir el contenido una vez; las versiones lingüísticas se generan a partir de ahí, sin que tenga que pagar un suplemento por cada idioma ni gestionar pasaportes separados. De este modo, el pasaporte se puede leer de conformidad con la normativa en cada mercado de destino.

Fuente: Reglamento sobre baterías (UE) 2023/1542: datos en las lenguas oficiales de los Estados miembros en los que se comercializa el producto.

Idiomas más allá de la UE

Más allá de la obligación legal, resulta útil que un folleto incluya también idiomas ajenos a la UE, para los mercados de exportación, los socios comerciales internacionales y los consumidores que no hablan ninguna de las lenguas oficiales de la Unión.

Transpareo gestiona un total de 40 versiones lingüísticas, incluidas las 24 lenguas oficiales de la UE. Solo tiene que introducir el contenido una vez y podrá publicarlo en cualquier idioma que desee, sin tener que pagar un suplemento por cada idioma. Además, la interfaz en la que gestiona sus pases (el gestor de aplicaciones) está traducida a los 40 idiomas, y puede introducir información en cualquiera de los idiomas disponibles.

Control de versiones e historial de cambios

Un pasaporte sufre modificaciones a lo largo de la vida útil del producto; sin un historial completo de versiones, no se podrá demostrar posteriormente qué versión estaba vigente y en qué momento. Por ello, la norma exige que se archiven todas las modificaciones realizadas en el pasaporte.

Transpareo congela cada publicación como una versión independiente y firmada, y registra quién la ha generado, cuándo y con qué campos modificados. De este modo, cada dato puede verificarse de forma retroactiva, y una corrección posterior no sobrescribe el historial, sino que lo continúa.

Fuente: EN 18221: «Se deben archivar todas las modificaciones realizadas en el pasaporte digital del producto».

Planta de producción a gran escala y adaptable para familias de productos

Quien tenga muchos productos similares no puede crear cada ficha manualmente una por una; un sistema viable necesita una forma de registrar familias enteras de productos de una sola vez.

Transpareo te permite cargar datos de productos mediante Excel o CSV y asignarlos a los campos obligatorios; para volúmenes muy grandes, también hay disponible una API masiva que crea las fichas de forma automatizada. De este modo, el sistema se adapta a un volumen que va desde una docena hasta decenas de miles de fichas.

Gestión interna de derechos basada en roles

No todos los empleados de la empresa deben poder editar o autorizar todos los contenidos de los pases; la norma exige una gestión de derechos basada en roles con accesos registrados.

Transpareo asigna derechos por función y grupo de usuarios y registra cada modificación. Incluso los usuarios externos, como talleres o empresas de reciclaje, solo reciben accesos muy limitados y de duración determinada; las autoridades acceden a través de una interfaz independiente, exclusivamente de lectura, que marca cada acceso en el registro de auditoría.

Fuente: EN 18239 (borrador), Gestión de derechos de acceso: regula qué actores pueden gestionar y compartir datos DPP.

Conservación de los datos más allá de la fecha de finalización del contrato

La obligación de conservación no finaliza con el contrato: un pase registrado debe seguir existiendo más allá del plazo legal, incluso si deja de utilizar los servicios del proveedor. Un proveedor que desactive los pases al rescindir el contrato le deja con un problema de cumplimiento normativo.

Transpareo se encarga de ello mediante el mismo archivo inalterable de diez años que los datos de registro: tras una rescisión, una dirección de respaldo permanente sigue entregando los pases, y la

interfaz con las autoridades lee el mismo registro de datos del archivo posterior al contrato. Los códigos QR ya impresos siguen siendo válidos.

Fuente: EN 18221: Las versiones de archivo también se almacenan en el proveedor de servicios de copia de seguridad.

Firma con clave criptográfica propia

Quien posea la clave privada de firma puede generar pases a nombre del emisor; por eso es más seguro que el emisor conserve él mismo esta clave, en lugar de confiarla al proveedor.

Con «Bring Your Own Key», su empresa gestiona su propio punto final de firma: Transpareo nunca conserva la clave privada y solo añade una contrafirma independiente. De este modo, cada versión cuenta con dos firmas independientes entre sí, y su firma como emisor es una que ni siquiera la propia Transpareo puede generar.

Identidad del expositor independiente de la plataforma

Para que un verificador pueda encontrar sus claves públicas, el pase debe incluir una identidad de emisor publicada. Si esta se encuentra en el dominio del proveedor, le vincula a él: un cambio invalidaría todos los códigos ya impresos.

Transpareo publica su identidad como DID: en la web, en su propio dominio, no en el nuestro; de este modo, cambiar de proveedor se convierte en un simple traslado de DNS, y los códigos ya impresos, junto con su verificación, siguen siendo válidos. Además, en el momento de la publicación, reflejamos cada clave pública en una dirección permanente, de modo que cada versión siga siendo verificable, incluso si el servidor original desaparece.

Fuente: EN 18219, apartado 4.2.2 (Persistencia): los identificadores se mantienen a lo largo de todo el ciclo de vida; los dominios web son transferibles o redirigibles.

Verificabilidad por parte de terceros, sin necesidad alguna de recurrir al proveedor

La prueba decisiva para la confianza es si un tercero puede verificar el pase sin necesidad de la infraestructura del proveedor. La norma exige que la verificación de la validez y la integridad sea gratuita para el verificador y se pueda realizar sin restricciones.

Para ello, Transpareo publica un renderizador de código abierto que carga los bytes de una versión procedente de cualquier fuente, vuelve a calcular el hash y comprueba ambas firmas con las claves públicas indicadas en el pase: sin necesidad de iniciar sesión, sin llamarnos por teléfono y sin depender de que la plataforma esté en funcionamiento. Quien tenga dudas puede consultar el código fuente.

Fuente: EN 18246 (borrador): «La verificación de la validez y la integridad de los datos del DPP debe poder realizarse sin coste alguno para el verificador y sin restricciones.»

Cambio de proveedor sin pérdida de datos

Un proveedor que dificulte el cambio le retiene a través de sus propios datos, y lo que ocurra con esos datos al finalizar el contrato determina si podrá cambiar libremente de proveedor. Por ello, la norma exige que los datos sean transferibles a través de una red abierta e interoperable, sin vinculación a ningún proveedor.

Transpareo almacena desde el principio los artefactos normativos en un espacio abierto y replicable públicamente: una simple sincronización genera una copia completa y firmada que se verifica automáticamente con las claves publicadas, sin necesidad de intervención por nuestra parte. Le facilitamos a usted o a su nuevo proveedor el archivo completo de eventos a través de una dirección de descarga firmada y de duración limitada; además, el catálogo de productos anterior se proporciona también en formato JSON-LD y CSV. Al finalizar el contrato, los datos obligatorios registrados siguen estando disponibles a través del archivo inalterable de diez años: La réplica pública y el archivo permanecen sincronizados y transmiten el mismo conjunto de datos; los códigos QR ya impresos siguen resolviéndose a través de la dirección de respaldo permanente, y la referencia del registro apunta a la nueva dirección. De este modo, el contrato finaliza sin pérdida de datos y sin incumplir los requisitos legales de conservación.

Fuente: EN 18216: Los datos deben ser «transferibles a través de una red abierta e interoperable, sin dependencia de un proveedor concreto».

Integración con los sistemas existentes en lugar de crear una «isla de datos»

Un pase que solo existe en la interfaz del proveedor se convierte en una «isla de datos» al margen del resto de sus sistemas; en ese caso, cada modificación debe actualizarse por duplicado.

Transpareo notifica eventos a través de webhooks firmados y permite importar y exportar datos mediante una API masiva, de modo que puedas integrar el pase en tu propio entorno de sistemas. Hemos optado deliberadamente por no ofrecer un conector preconfigurado para un sistema ERP concreto: las interfaces abiertas y firmadas se adaptan a cualquier sistema, en lugar de dar preferencia a uno solo.

Importación y exportación por lotes más allá de las obligaciones mínimas de la UE

Quien desee utilizar los datos registrados también fuera del pasaporte digital necesitará funciones de importación y exportación que vayan más allá de los campos obligatorios por ley.

Transpareo acepta grandes volúmenes de datos a través de Excel, CSV y la API masiva, y los devuelve en la misma cantidad. De este modo, el sistema no solo sirve para cumplir con la normativa de la UE, sino también para gestionar sus propios datos.

Base de datos independiente y clave propia

En una base de datos compartida, sus datos están vinculados a los de otros clientes; en ese caso, resulta prácticamente imposible lograr una separación clara y demostrable, y es difícil acreditar el derecho de supresión previsto en el artículo 17 del RGPD.

En Transpareo, cada cliente se encuentra en su propia base de datos, cifrada con una clave propia; la separación se produce tanto a nivel de la base de datos como a nivel de cifrado. Esto garantiza el derecho de supresión mediante una supresión verificable; el alojamiento se encuentra en Alemania y el contrato de encargado del tratamiento (AVV) está incluido.

Fuente: Artículo 17 del RGPD (derecho de supresión), que se cumple mediante una base de datos independiente, una clave propia y una supresión verificable.

Cifrado y copias de seguridad

Un proveedor debe proteger los datos tanto durante su transmisión como en reposo, y garantizar su seguridad frente a posibles fallos; el RGPD exige para ello medidas acordes con el estado actual de la técnica.

Transpareo cifra todas las conexiones con TLS y los datos sensibles de las aplicaciones con AES. Las copias de seguridad están cifradas con GPG, se renuevan mediante una rotación periódica de claves, se crean cada cuatro horas y se conservan durante doce meses en un servidor independiente.

Fuente: Artículo 32 del RGPD (Seguridad del tratamiento): TLS, AES y copias de seguridad cifradas con rotación.

Registro de incidentes de seguridad

Los incidentes relacionados con la seguridad deben poder rastrearse: quién ha iniciado sesión, cuándo lo ha hecho y cómo se han utilizado las claves. La Directiva NIS-2 exige que se mantengan los registros de auditoría correspondientes.

Transpareo mantiene un registro de eventos de seguridad sobre los intentos de inicio de sesión, los retos de autenticación multifactorial (MFA) y la actividad de las claves API, y lo conserva durante un año. De este modo, se cumplen los requisitos de la Directiva NIS-2 en materia de registros de auditoría.

Fuente: Directiva NIS-2 (requisitos relativos a los registros de auditoría): eventos de seguridad registrados, conservación durante un año.

Autenticación multifactorial

Una sola contraseña ofrece una protección insuficiente para el acceso; la directiva NIS-2 exige un control de acceso con autenticación multifactorial.

Transpareo ofrece autenticación multifactorial para todos los usuarios del gestor de aplicaciones - mediante la aplicación Authenticator, una clave de acceso o una llave de hardware - , junto con códigos de respaldo en caso de pérdida. La autenticación multifactorial puede activarse de forma obligatoria para su cuenta.

Fuente: Directiva NIS-2 (control de acceso y autenticación multifactorial).

Alojamiento web certificado según la norma ISO 27001 en Alemania

La ubicación de los servidores y el nivel de seguridad del centro de datos determinan la seguridad física de sus datos, así como la legislación a la que están sujetos.

Transpareo aloja sus datos en servidores certificados según la norma ISO 27001 en Alemania, con estrictas medidas de seguridad tanto físicas como organizativas. Además, al estar ubicados en Alemania, sus datos están sujetos íntegramente a la legislación europea.

Fuente: ISO/IEC 27001 (Gestión de la seguridad de la información), centro de datos certificado en Alemania.

¿Se encarga el proveedor de tramitar el registro en la UE por ti?

La inscripción en el registro de la UE, incluida la obtención del certificado oficial, supone una carga administrativa recurrente de la que un proveedor puede encargarse por usted. El Reglamento del Registro lo establece expresamente: un proveedor de servicios puede encargarse del registro en su nombre, pero la responsabilidad jurídica recae en el agente económico.

Transpareo registrará sus certificados en su nombre tan pronto como la UE publique la interfaz técnica; usted seguirá siendo el agente económico legalmente responsable, pero no tendrá que asumir la carga operativa. Hasta que la interfaz esté disponible, nadie puede prestar este servicio; nosotros ya hemos preparado los datos necesarios para ello.

Fuente: Reglamento de aplicación del Registro DPP (borrador), art. 19: Un prestador de servicios puede encargarse del registro en nombre del operador económico; la responsabilidad recae en este último.

Normativa clara sobre el esfuerzo y los costes de asistencia técnica

Algunos proveedores separan el uso del servicio de asistencia y facturan la ayuda por separado; en definitiva, esto hace que la colaboración resulte difícil de calcular.

En Transpareo, la asistencia técnica está incluida en la tarifa: sin contrato de asistencia por separado ni horas adicionales facturadas según el tiempo dedicado. Todo lo que necesite en materia de asistencia ya está incluido en el precio indicado.

Estructura de precios transparente

Una estructura de precios que solo se revela durante la conversación de venta o que se calcula a posteriori por idioma, producto y llamada a la interfaz hace que los costes reales sean impredecibles.

Transpareo publica abiertamente en su página web cuatro tarifas para empresas de cualquier tamaño, con un periodo de prueba gratuito y la posibilidad de dar de baja el servicio en cualquier momento. No hay costes adicionales ocultos por idioma, producto o llamada a la interfaz: el precio indicado es el precio final.