

Fiche comparative des fournisseurs de DPP

Seules les fonctionnalités existantes et vérifiables sont cochées - pas les annonces ni les déclarations d'intention. La colonne « Transpareo » est préremplie ; vous complétez les deux colonnes vides lorsque vous évaluez d'autres prestataires. Vous trouverez des explications et des sources pour chaque critère à la fin du document.

Mise à jour : 10.09.2026

Obligatoire en vertu de la loi

critère	Transpareo		
Échange de données dans un format ouvert et normalisé Les données de passeport sont accessibles via des normes ouvertes : elles sont lisibles par tout système autorisé, et pas uniquement par le logiciel d'un fournisseur donné. EN 18216	☒	☐	☐
Identifiant unique et portable, indépendant du fournisseur L'identifiant du produit est associé au produit et non à la plateforme : en cas de changement de fournisseur, le Pass conserve son identité. EN 18219	☒	☐	☐
Support physique, lisible de manière permanente Le code QR figurant sur le produit permet d'accéder au Pass depuis n'importe quel navigateur : sans application, sans compte, avec n'importe quel smartphone. EN 18220	☒	☐	☐

critère	Transpareo		
Conservation et archivage au-delà de la durée minimale Chaque version publiée reste accessible pendant la durée prévue par la loi, y compris les versions antérieures, et pas seulement la version actuelle. EN 18221	☒	☐	☐
API pour la gestion du cycle de vie et la recherche Une interface de programmation permet de lire, de créer et de rechercher des passeports - bien plus qu'une simple interface Web où l'on clique. EN 18222	☒	☐	☐
Modèle de données interopérable Les données des passeports suivent un modèle commun que d'autres systèmes peuvent lire sans avoir à les reformater. EN 18223	☒	☐	☐
Modèle de droits d'accès à trois niveaux Les données publiques, autorisées et administratives sont clairement séparées : chacun ne voit que ce à quoi il a accès. EN 18239	☒	☐	☐
Authenticité et intégrité vérifiables des données Chaque version est doublement signée et peut être vérifiée dans le navigateur, sans qu'il soit nécessaire de nous faire confiance, uniquement à partir des données. EN 18246	☒	☐	☐
Interconnexion avec le registre de la Commission européenne Enregistrement accompagné d'un justificatif officiel - dès que l'UE aura publié l'interface technique. Celle-ci n'est pas encore disponible ; aucun prestataire ne peut donc satisfaire à cette exigence à l'heure actuelle.	☐	☐	☐
Conservation des données d'enregistrement au-delà du délai légal Une archive inaltérable couvrant dix ans : ni le fabricant ni Transpareo ne peuvent modifier une version a posteriori.	☒	☐	☐

critère	Transpareo		
Données sur les produits dans les langues officielles de chaque marché cible Les informations obligatoires doivent figurer dans les langues officielles de chaque pays où le produit est commercialisé ; dans le cas d'une commercialisation à l'échelle de l'Union européenne, cela concerne donc les 24 langues officielles, et pas uniquement celles du marché national.	☒	☐	☐

Utile pour l'exploitation d'une base de données DPP

critère	Transpareo		
Les langues au-delà de l'UE 16 langues supplémentaires en plus des 24 langues officielles de l'UE, soit 40 au total, destinées aux marchés cibles situés en dehors de l'Union.	☒	☐	☐
Gestion des versions et historique des modifications Chaque modification génère une nouvelle version traçable, avec indication de la date et de l'auteur, et ce tout au long du cycle de vie du produit.	☒	☐	☐
Installation de production à grande échelle et évolutive pour des familles de produits Importer les données produit via Excel ou CSV et les attribuer aux champs obligatoires - pour les volumes importants, une API de traitement en masse est également disponible.	☒	☐	☐
Gestion interne des droits basée sur les rôles Les règles définissent qui, au sein de l'entreprise, est autorisé à gérer ou à partager quelles données, y compris les accès strictement limités et temporaires accordés aux personnes externes.	☒	☐	☐
Conservation au-delà de la fin du contrat Si vous résiliez votre abonnement, vos fiches publiées resteront accessibles dans les archives inaltérables couvrant une période de dix ans.	☒	☐	☐

critère	Transpareo		
Signature à l'aide d'une clé cryptographique propre « Bring Your Own Key » : vous conservez vous-même la clé privée, nous nous contentons d'ajouter une contre-signature indépendante.	☒	☐	☐
Identité de l'exposant indépendante de la plateforme Votre identité d'exposant DID:web est hébergée sur votre propre domaine, et non sur le nôtre : changer de fournisseur revient à effectuer un transfert DNS.	☒	☐	☐
Vérifiabilité par des tiers, sans aucune intervention du fournisseur Un moteur de rendu open source vérifie les hachages et les signatures directement dans le navigateur, sans contacter aucun de nos serveurs.	☒	☐	☐

Fonctionnalités supplémentaires souhaitables

critère	Transpareo		
Changer de fournisseur sans perte de données Lors du changement, vous emportez l'intégralité de votre base de données de passeports dans des formats ouverts – signés et vérifiables par vous-même ; à la fin du contrat, les passeports obligatoires restent accessibles dans les archives inaltérables sur dix ans, sans perte de données.	☒	☐	☐
Intégration aux systèmes existants plutôt que création d'îlots de données Des webhooks signés et une API de traitement en masse permettent d'intégrer Pass à vos systèmes – il n'y a pas de connecteur prêt à l'emploi pour un ERP spécifique.	☒	☐	☐
Importation et exportation par lots : au-delà des simples obligations de l'UE Il est possible de transférer de grandes quantités de données dans les deux sens, et pas seulement les champs obligatoires.	☒	☐	☐

Sécurité et protection des données

critère	Transpareo		
Une base de données distincte et une clé propre à celle-ci Vos données sont stockées dans une base de données dédiée, chiffrées à l'aide d'une clé unique, et séparées tant au niveau de la base de données qu'au niveau du chiffrement.	☒	☐	☐
Chiffrement et sauvegardes TLS pour toutes les connexions, chiffrement AES des données sensibles et sauvegardes chiffrées avec rotation des clés.	☒	☐	☐
Journal des événements de sécurité Les tentatives de connexion, les défis d'authentification multifactorielle (MFA) et l'activité liée aux clés API sont consignés et conservés pendant un an.	☒	☐	☐
Authentification multifactorielle Application d'authentification, clé d'accès ou clé matérielle pour tous les utilisateurs, avec des codes de secours en cas de perte.	☒	☐	☐
Hébergement certifié ISO 27001 en Allemagne Serveurs situés en Allemagne et soumis à des mesures de sécurité physiques et organisationnelles strictes.	☒	☐	☐

Questions économiques et organisationnelles

critère	Transpareo		
Le fournisseur se charge-t-il de l'enregistrement auprès de l'UE à votre place ? Nous nous chargeons de l'enregistrement, y compris de l'attestation officielle, dès que l'UE aura publié l'interface ; vous n'aurez donc rien à faire.	☒	☐	☐

critère	Transpareo		
Une réglementation claire concernant les efforts et les coûts liés à l'assistance Chez Transpareo, l'assistance est comprise dans le prix : pas de contrat d'assistance distinct, pas de frais supplémentaires.	☒	☐	☐
Structure tarifaire transparente Quatre formules publiques adaptées à toutes les tailles d'entreprise, période d'essai gratuite, résiliable à tout moment – sans frais supplémentaires cachés par langue, produit ou appel d'API.	☒	☐	☐

Explications et sources

Échange de données dans un format ouvert et normalisé **EN 18216**

La norme exige que les passeports numériques des produits soient accessibles via des protocoles ouverts et normalisés, afin que les autorités, les partenaires et vos propres systèmes puissent lire les données sans être liés au logiciel d'un fournisseur. Un format propriétaire constituerait un « îlot » : sans le fournisseur, vous ne pourriez plus accéder à vos propres données. La norme est publiée au Journal officiel de l'Union européenne depuis le 15 juillet 2026 (décision d'exécution (UE) 2026/1736) et bénéficie ainsi de la présomption de conformité au RGPD.

Transpareo fournit toutes les données de passeport et interfaces via HTTPS standard sous une forme structurée et lisible par machine – sans logiciel spécialisé, sans protocoles propriétaires. Chaque version publiée est en outre signée, ce qui permet au destinataire non seulement de lire les données, mais aussi de vérifier qu'elles n'ont pas été modifiées. Ce que vous voyez dans l'interface correspond exactement au même ensemble de données que celui récupéré par tout système autorisé via les interfaces ouvertes.

Source : EN 18216, Exigences relatives aux protocoles d'échange de données : « Pour l'accès DPP normalisé, il convient d'utiliser les protocoles d'échange de données définis. »

Identifiant unique et portable, indépendant du fournisseur **EN 18219**

Chaque passeport produit doit disposer d'un identifiant unique qui renvoie de manière permanente au même produit et qui ne soit pas lié à un fournisseur en particulier. Si un fournisseur lie cet identifiant à sa propre infrastructure, vous perdrez l'identité de vos passeports en cas de changement de fournisseur :

chaque code imprimé et chaque enregistrement deviendraient alors sans objet. La norme est publiée au Journal officiel de l'Union européenne depuis le 15 juillet 2026.

Transpareo attribue l'identifiant sous la forme d'un GS1 Digital Link associé à votre GTIN – une norme industrielle ouverte qui appartient au produit, et non à la plateforme – et vérifie chaque identifiant par rapport aux schémas normatifs approuvés. L'identité de signature se trouve sous la forme DID:web sur votre propre domaine, et non sur le nôtre. L'identifiant reste valide même en cas de panne d'un système : une adresse de secours permanente continue de le résoudre, et le passe conserve son identité quel que soit le changement de fournisseur.

Source : EN 18219, section 4.6.2(3) : « L'identifiant unique ne doit pas entraîner de dépendance vis-à-vis d'un fournisseur. »

Support physique, lisible de manière permanente EN 18220

Le passeport doit être accessible via un support de données lisible par machine intégré au produit, que tout le monde peut consulter sans logiciel spécifique, et qui reste lisible pendant toute la durée de vie du produit, même après utilisation et réparation. Un support de données nécessitant une application ou un compte spécifique exclut une partie du public. La norme est publiée au Journal officiel de l'Union européenne depuis le 15 juillet 2026.

Transpareo génère un code QR conforme à la norme ISO/IEC 18004, qui contient une adresse GS1 Digital Link et redirige directement vers le passeport dans n'importe quel navigateur – sans connexion, sans téléchargement, sur n'importe quel smartphone. Le modèle, le lot et l'article sont déjà intégrés dans l'adresse codée, de sorte qu'un simple scan renvoie directement à la page correspondante. L'adresse restant stable grâce à une résolution de secours permanente, un code imprimé une seule fois reste valable pendant toute la durée de vie du produit.

Source : EN 18220, Exigences relatives aux supports de données (section 5) : symboles, codage, qualité d'impression et durabilité ; le support de données doit rester lisible même après plusieurs cycles d'utilisation et de réparation.

Conservation et archivage au-delà de la durée minimale EN 18221

La norme exige qu'un passeport, ainsi que l'historique de ses versions, soit conservé pendant la durée prescrite par la réglementation et reste accessible sans modification. Si seule la version actuelle est conservée, la traçabilité des informations antérieures est perdue – or, c'est précisément cette traçabilité qu'un acteur économique doit pouvoir prouver aux autorités. La durée de conservation dépend de la législation sectorielle applicable, mais elle est d'au moins dix ans. La norme est publiée au Journal officiel de l'Union européenne depuis le 15 juillet 2026.

Transpareo enregistre chaque publication sous forme de version figée et signée dans une archive inviolable, dans laquelle personne ne pourra plus la modifier ni la supprimer par la suite – ni vous, ni nous. Les

versions antérieures restent accessibles aux côtés de la version actuelle, et chaque version est horodatée et signée. Il est ainsi possible de prouver, pour n'importe quel moment, ce que le passeport indiquait à cette date.

Source : EN 18221 : « Le passeport numérique du produit doit rester accessible aux utilisateurs autorisés pendant toute sa durée de vie. »

API pour la gestion du cycle de vie et la recherche EN 18222

Outre l'affichage dans le navigateur, la norme exige une interface de programmation permettant de créer, lire, mettre à jour et effectuer des recherches dans les passeports à l'aide d'identifiants de produit. Sans une telle interface, tout traitement en masse reste manuel, et les autres systèmes ne peuvent pas exploiter automatiquement le fichier des passeports. La norme est publiée au Journal officiel de l'Union européenne depuis le 15 juillet 2026.

Transpareo prend en charge les méthodes normalisées prescrites via une interface standardisée et versionnée : les passeports peuvent être créés, lus, mis à jour et parcourus page par page à l'aide d'identifiants de produit, le tout de manière automatisée. Le passeport signé est livré tel quel : l'interface renvoie exactement les octets dont la signature peut être vérifiée par un contrôleur.

Source : EN 18222 : interface de programmation standardisée (API) pour la gestion du cycle de vie et la consultabilité du DPP, conformément aux exigences de l'ESPR.

Modèle de données interopérable EN 18223

Afin d'assurer la compatibilité des fiches entre les systèmes et tout au long de la chaîne d'approvisionnement, la norme impose un modèle de données commun avec une signification uniforme des champs. Un modèle propre à un fournisseur oblige chaque partenaire à effectuer sa propre traduction - et chaque traduction est une source d'erreurs. La norme est publiée au Journal officiel de l'Union européenne depuis le 15 juillet 2026.

Transpareo s'appuie sur une couche terminologique horizontale comprenant des vocabulaires techniques parallèles et reconnus (GS1, EPCIS et autres) et décrit chaque élément de données en faisant référence à son dictionnaire et à son type de données. Un système destinataire apprend ainsi non seulement comment s'appelle un champ, mais aussi ce qu'il signifie : le passeport reste lisible sans reformatage.

Source : EN 18223 : modèle de données sémantique commun pour l'interopérabilité du système DPP.

Modèle de droits d'accès à trois niveaux EN 18239

Un passeport produit contient des informations publiques, des données destinées aux opérateurs économiques autorisés et des données réservées aux autorités ; la norme exige que ces niveaux soient distincts et réglementés pour chaque champ de données. Les données publiques doivent être acces-

sibles sans authentification, les autres uniquement après vérification. La norme EN 18239 est en phase d'adoption finale.

Transpareo gère la visibilité comme une propriété propre à chaque champ de données : le niveau public est accessible sans authentification, les niveaux supérieurs sont protégés par une interface dédiée aux autorités, avec un accès en lecture seule et une journalisation des opérations, et chaque accès aux données protégées est consigné dans le journal d'audit. Le modèle à trois niveaux de la norme est ainsi déjà intégré dès aujourd'hui dans l'architecture, et non pas ajouté a posteriori.

Source : EN 18239 (projet, en phase d'adoption finale) : « L'accès aux données publiques doit être possible pour les acteurs de l'UE et hors UE sans authentification supplémentaire » ; les données contrôlées nécessitent un accès authentifié et traçable.

Authenticité et intégrité vérifiables des données EN 18246

La norme exige que l'authenticité et l'intégrité d'un passeport puissent être vérifiées et que cette vérification soit possible librement et sans restriction. La confiance ne doit pas dépendre de la pérennité du fournisseur, mais doit être liée à l'ensemble de données lui-même ; sinon, chaque passeport n'aurait que la crédibilité de l'entreprise qui l'héberge à un moment donné. La norme EN 18246 est en phase d'adoption finale.

Transpareo signe chaque version publiée à l'aide de deux clés indépendantes (émetteur et Transpareo) et enchaîne les versions via leur hachage, de sorte que l'historique ne puisse pas non plus être modifié à l'insu de tous. Un rendu open source vérifie les deux signatures directement dans le navigateur, sans contacter l'un de nos serveurs : la preuve signée et auto-vérifiable requise est ainsi déjà mise en œuvre.

Source : EN 18246 (projet, en phase d'adoption finale) : l'authenticité, la fiabilité et l'intégrité des données DPP doivent pouvoir être démontrées.

Interconnexion avec le registre de la Commission européenne

À l'avenir, tout passeport soumis à l'obligation d'enregistrement devra être inscrit dans le registre central de l'UE, qui délivrera un identifiant d'enregistrement permanent et un certificat d'enregistrement officiel. L'UE n'a pas encore publié l'interface technique nécessaire à cet effet ; c'est pourquoi aucun prestataire ne peut aujourd'hui prouver cette connexion ; si un prestataire affirme le contraire, vous devriez lui demander des précisions.

Transpareo a préparé cette connexion autant que possible sans disposer de l'interface : les champs nécessaires (identifiant d'enregistrement, adresse de sauvegarde stable, hachage de version) sont déjà créés dans le modèle de données. Dès que l'UE publiera l'interface, nous activerons l'enregistrement sans que vous ayez à modifier vos passeports. D'ici là, cette case restera cochée - chez nous comme chez tout prestataire honnête.

Source : projet de décret d'application relatif au registre DPP (Ares(2026)4424976).

Conservation des données d'enregistrement au-delà du délai légal

Les données d'enregistrement des passeport doivent rester disponibles sans modification au-delà du délai légal – généralement dix ans à compter de l'enregistrement –, même en cas d'insolvabilité ou de cessation d'activité du fabricant. Cette obligation perdure donc au-delà de votre contrat avec un fournisseur et même au-delà de l'existence du fournisseur lui-même.

À cette fin, Transpareo tient à jour une archive inviolable dans laquelle, une fois enregistrée, aucune version ne peut être modifiée ou supprimée a posteriori, ni par le fabricant ni par nous-mêmes. Les archives sont automatiquement activées lors de l'enregistrement auprès de l'UE. Et pour qu'elles restent accessibles même si Transpareo venait un jour à disparaître, leur pérennité est garantie par un dépôt notarié en Suisse.

Source : Décret d'application du registre DPP, art. 10, paragraphe 3 (conservation pendant dix ans).

Données sur les produits dans les langues officielles de chaque marché cible

Les informations obligatoires figurant sur un passeport doivent être disponibles dans les langues officielles de chaque État membre dans lequel le produit est commercialisé, et pas uniquement dans la langue du siège social du fabricant. Une entreprise qui ne dessert que son marché national ne satisfait pas à cette obligation pour tous les autres marchés cibles.

Transpareo gère chaque passeport en plusieurs langues et fournit le contenu obligatoire dans les 24 langues officielles de l'UE. Vous saisissez le contenu une seule fois ; les versions linguistiques sont générées à partir de celui-ci, sans que vous ayez à payer de supplément par langue ni à gérer des passeports distincts. Le passeport est ainsi lisible et conforme à la réglementation sur chaque marché cible.

Source : Règlement (UE) 2023/1542 relatif aux piles et accumulateurs : données dans les langues officielles des États membres dans lesquels le produit est mis sur le marché.

Les langues au-delà de l'UE

Au-delà de l'obligation légale, il est utile qu'un passeport couvre également des langues hors de l'UE, notamment pour les marchés d'exportation, les partenaires commerciaux internationaux et les consommateurs qui ne parlent aucune des langues officielles de l'Union.

Transpareo gère au total 40 versions linguistiques, dont les 24 langues officielles de l'UE. Vous saisissez le contenu une seule fois et le diffusez dans toutes les langues souhaitées, sans frais supplémentaires par langue. L'interface dans laquelle vous gérez vos fiches techniques (le gestionnaire d'applications) est également traduite dans les 40 langues, et vous pouvez saisir des informations dans n'importe laquelle des langues disponibles.

Gestion des versions et historique des modifications

Un passeport évolue tout au long de la durée de vie du produit ; sans historique complet des versions, il est impossible de prouver ultérieurement quelle version était en vigueur à quel moment. La norme exige donc que toutes les modifications apportées au passeport soient archivées.

Transpareo consigne chaque publication sous la forme d'une version distincte et signée, en précisant qui l'a générée, à quelle date et avec quels champs modifiés. Ainsi, chaque information reste vérifiable rétroactivement, et une correction ultérieure ne remplace pas l'historique, mais le prolonge.

Source : EN 18221 : « Toutes les modifications apportées au passeport numérique du produit doivent être archivées. »

Installation de production à grande échelle et évolutive pour des familles de produits

Lorsque l'on propose de nombreux produits similaires, il n'est pas possible de créer chaque fiche produit manuellement ; un système efficace doit permettre de saisir des familles entières de produits en une seule fois.

Transpareo vous permet d'importer des données produit via Excel ou CSV et de les associer aux champs obligatoires ; pour les très grands volumes, une API de traitement en masse est également disponible, qui crée les fiches de manière automatisée. La création de fiches peut ainsi s'adapter à des volumes allant d'une douzaine à plusieurs dizaines de milliers de fiches.

Gestion interne des droits basée sur les rôles

Au sein de l'entreprise, tout le monde ne doit pas être autorisé à modifier ou à valider le contenu de chaque passeport ; la norme exige une gestion des droits basée sur les rôles, avec un journal des accès.

Transpareo attribue des droits par rôle et par groupe d'utilisateurs et consigne chaque modification. Même les intervenants externes, tels que les ateliers ou les entreprises de recyclage, ne bénéficient que d'un accès strictement limité et temporaire ; les autorités accèdent au système via une interface distincte, en lecture seule, qui enregistre chaque accès dans le journal d'audit.

Source : EN 18239 (projet), gestion des droits d'accès : définit quels acteurs sont autorisés à gérer et à partager les données DPP.

Conservation au-delà de la fin du contrat

L'obligation de conservation ne prend pas fin avec le contrat : un passe enregistré doit être conservé au-delà du délai légal, même si vous quittez le prestataire. Un prestataire qui désactive les passes lors de la résiliation vous expose à un problème de conformité.

Transpareo assure cette continuité grâce à la même archive inaltérable de dix ans que celle des données d'enregistrement : après une résiliation, une adresse de secours permanente continue de délivrer les passeports, et l'interface avec les autorités lit le même ensemble de données à partir de l'archive post-contractuelle. Les codes QR déjà imprimés restent valides.

Source : EN 18221 : les versions archivées sont également stockées chez le prestataire de services de sauvegarde.

Signature à l'aide d'une clé cryptographique propre

Quiconque détient la clé de signature privée peut générer des certificats au nom de l'émetteur ; c'est pourquoi il est plus sûr que l'émetteur conserve lui-même cette clé plutôt que de la confier au prestataire.

Avec « Bring Your Own Key », votre entreprise gère son propre point de terminaison de signature : Transpareo ne conserve jamais la clé privée et se contente d'ajouter une contre-signature indépendante. Ainsi, chaque version comporte deux signatures indépendantes l'une de l'autre, et votre signature d'émetteur est une signature que Transpareo ne peut pas générer lui-même.

Identité de l'exposant indépendante de la plateforme

Pour qu'un vérificateur puisse trouver vos clés publiques, le Pass doit comporter une identité d'émetteur publiée. Si celle-ci se trouve sur le domaine du fournisseur, elle vous lie à ce dernier : un changement de fournisseur invaliderait tous les codes déjà imprimés.

Transpareo publie votre identité sous forme de DID : sur le Web, sur votre propre domaine et non sur le nôtre. Changer de fournisseur revient ainsi à un transfert DNS, et les codes déjà imprimés, ainsi que leur vérification, restent valides. De plus, nous répercutons chaque clé publique vers une adresse permanente au moment de sa publication, afin que chaque version reste vérifiable, même si l'hébergeur d'origine disparaît.

Source : EN 18219, section 4.2.2 (Stabilité) : les identifiants sont conservés tout au long de leur cycle de vie ; les noms de domaine sont transférables ou redirigeables.

Vérifiabilité par des tiers, sans aucune intervention du fournisseur

Le critère déterminant pour établir la confiance est de savoir si un tiers peut vérifier le passeport sans recourir à l'infrastructure du fournisseur. La norme exige que la vérification de la validité et de l'intégrité puisse être effectuée gratuitement et sans restriction par le vérificateur.

À cette fin, Transpareo publie un rendu open source qui charge les octets d'une version provenant de n'importe quelle source, recalcule le hachage et vérifie les deux signatures par rapport aux clés publiques mentionnées dans le passeport – sans connexion, sans appel chez nous, sans dépendance

vis-à-vis d'une plateforme en fonctionnement. Les personnes méfiantes peuvent consulter le code source.

Source : EN 18246 (projet) : « La vérification de la validité et de l'intégrité des données DPP doit pouvoir être effectuée gratuitement et sans restriction par le vérificateur. »

Changer de fournisseur sans perte de données

Un fournisseur qui complique le changement vous retient par le biais de vos propres données – et ce qu'il advient de ces données à la fin du contrat détermine si vous pouvez changer librement de fournisseur. La norme exige donc que les données soient transférables via un réseau ouvert et interopérable, sans lien avec un fournisseur particulier.

Transpareo stocke d'emblée les artefacts réglementaires dans un espace ouvert et publiquement accessible : une simple synchronisation génère une copie complète et signée qui s'autovérifie par rapport aux clés publiées, sans aucune intervention de notre part. Nous vous transmettons, à vous ou à votre nouveau fournisseur, l'archive complète des événements via une adresse de téléchargement signée et à durée limitée ; le catalogue de produits en amont est également fourni au format JSON-LD et CSV. À la fin du contrat, les documents obligatoires enregistrés restent accessibles via l'archive inaltérable de dix ans : le miroir public et les archives restent synchronisés et transmettent le même ensemble de données ; les codes QR déjà imprimés continuent de s'afficher via l'adresse de secours permanente, et le lien vers le registre renvoie vers la nouvelle adresse. Ainsi, le contrat prend fin sans perte de données et sans violation des obligations légales de conservation.

Source : EN 18216 : les données doivent être « transférables via un réseau ouvert et interopérable, sans dépendance vis-à-vis d'un fournisseur ».

Intégration aux systèmes existants plutôt que création d'îlots de données

Un passe qui n'existe que dans l'interface du fournisseur devient un îlot de données isolé de vos autres systèmes : chaque modification doit alors être effectuée deux fois.

Transpareo signale les événements via des webhooks signés et permet d'importer et d'exporter des données via une API en masse, ce qui vous permet d'intégrer le Pass à votre propre environnement système. Nous ne fournissons délibérément pas de connecteur prêt à l'emploi pour un système ERP spécifique : les interfaces ouvertes et signées s'adaptent à tous les systèmes, sans en privilégier aucun.

Importation et exportation par lots : au-delà des simples obligations de l'UE

Si vous souhaitez utiliser les données saisies en dehors du passeport, vous aurez besoin de fonctions d'importation et d'exportation allant au-delà des champs obligatoires prévus par la loi.

Transpareo accepte des volumes importants de données via Excel, CSV et l'API Bulk, et les restitue dans le même format. Ainsi, le système ne sert pas seulement à respecter les obligations de l'UE, mais

aussi à gérer vos propres données.

Une base de données distincte et une clé propre à celle-ci

Dans une base de données partagée, vos données sont associées à celles d'autres clients ; il est alors pratiquement impossible d'assurer une séparation claire et vérifiable, et le droit à l'effacement prévu à l'article 17 du RGPD est difficile à faire valoir.

Chez Transpareo, chaque client dispose de sa propre base de données, chiffrée à l'aide d'une clé unique : la séparation s'effectue tant au niveau de la base de données qu'au niveau du chiffrement. Cela garantit le respect du droit à l'effacement grâce à une suppression vérifiable ; l'hébergement est situé en Allemagne et le contrat de sous-traitance (AVV) est inclus.

Source : article 17 du RGPD (droit à l'effacement), respecté grâce à une base de données distincte, une clé unique et un effacement vérifiable.

Chiffrement et sauvegardes

Un prestataire doit protéger les données lors de leur transmission et au repos, et les sécuriser contre toute défaillance ; le RGPD exige à cet effet des mesures conformes à l'état actuel de la technique.

Transpareo chiffre toutes les connexions à l'aide du protocole TLS et les données sensibles des applications à l'aide de l'algorithme AES. Les sauvegardes sont chiffrées avec GPG, les clés sont renouvelées régulièrement, elles sont effectuées toutes les quatre heures et conservées pendant douze mois sur un serveur distinct.

Source : RGPD, art. 32 (Sécurité du traitement) : TLS, AES et sauvegardes chiffrées avec rotation.

Journal des événements de sécurité

Les événements liés à la sécurité doivent rester traçables : qui s'est connecté, à quel moment, et comment les clés ont été utilisées. La directive NIS 2 exige la mise en place de journaux d'audit correspondants.

Transpareo tient un journal des événements de sécurité répertoriant les tentatives de connexion, les défis d'authentification multifactorielle (MFA) et l'activité des clés API, et le conserve pendant un an. Les exigences de la directive NIS-2 en matière de journaux d'audit sont ainsi satisfaites.

Source : directive NIS 2 (exigences relatives aux journaux d'audit) : événements de sécurité consignés, conservation pendant un an.

Authentification multifactorielle

Un mot de passe unique n'offre qu'une protection insuffisante ; la directive NIS-2 exige un contrôle d'accès avec authentification multifactorielle.

Transpareo propose l'authentification multifactorielle à tous les utilisateurs de l'Application Manager – via une application d'authentification, une clé d'accès ou une clé matérielle –, ainsi que des codes de secours en cas de perte. L'obligation d'utiliser l'authentification multifactorielle peut être activée pour votre compte.

Source : directive NIS 2 (contrôle d'accès et authentification multifactorielle).

Hébergement certifié ISO 27001 en Allemagne

L'emplacement des serveurs et le niveau de sécurisation du centre de données déterminent la sécurité physique de vos données, ainsi que la législation à laquelle elles sont soumises.

Transpareo héberge ses données sur des serveurs certifiés ISO 27001 situés en Allemagne, où sont mises en œuvre des mesures de sécurité physiques et organisationnelles rigoureuses. De plus, l'Allemagne garantit que vos données sont entièrement soumises au droit européen.

Source : ISO/IEC 27001 (gestion de la sécurité de l'information), centre de données certifié en Allemagne.

Le fournisseur se charge-t-il de l'enregistrement auprès de l'UE à votre place ?

L'inscription au registre de l'UE, ainsi que l'obtention du certificat officiel, constituent une charge administrative récurrente qu'un prestataire peut prendre en charge pour vous. Le règlement relatif au registre le prévoit expressément : un prestataire de services peut se charger de l'enregistrement pour votre compte, mais la responsabilité juridique incombe à l'opérateur économique.

Transpareo enregistrera vos passeports pour votre compte dès que l'UE aura publié l'interface technique ; vous resterez l'opérateur économique légalement responsable, mais vous n'aurez pas à supporter la charge opérationnelle. Tant que l'interface n'est pas disponible, personne ne peut fournir ce service ; nous avons déjà préparé les données nécessaires à cet effet.

Source : Décret d'application relatif au registre DPP (projet), art. 19 : l'enregistrement peut être effectué par un prestataire de services pour le compte de l'opérateur économique ; la responsabilité incombe toutefois à ce dernier.

Une réglementation claire concernant les efforts et les coûts liés à l'assistance

Certains prestataires dissocient l'utilisation du service d'assistance et facturent l'aide séparément ; au final, cela rend la collaboration difficile à chiffrer.

Chez Transpareo, l'assistance est comprise dans le forfait : pas de contrat d'assistance distinct, pas d'heures supplémentaires facturées au temps passé. Tout ce dont vous avez besoin en matière d'assistance est déjà inclus dans le prix indiqué.

Structure tarifaire transparente

Une structure tarifaire qui n'apparaît qu'au moment de l'entretien commercial ou qui est facturée a posteriori par langue, par produit et par appel d'interface rend les coûts réels imprévisibles.

Transpareo publie ouvertement sur son site web quatre formules adaptées à chaque taille d'entreprise, avec une période d'essai gratuite et une résiliation possible à tout moment. Il n'y a pas de frais supplémentaires cachés par langue, par produit ou par appel d'interface : le prix affiché est le prix définitif.