TPSA

THIRD-PARTY SUPPLIER ACCOUNTABILITY

T P S A - 0 1

Norme de divulgation des fournisseurs

Cadre de responsabilité des fournisseurs tiers

Document de spécifications

Version 1.0 Avril 2026

Auteur : Sébastien Poitrasson, Arthur Koenig Conseil

AK ARTHURKOENIG

1. Introduction

1.1 Objectif

Ce document définit la **norme TPSA-01 : Norme de divulgation des fournisseurs** , premier volet du cadre de responsabilité des fournisseurs tiers (TPSA). Il précise la structure, le contenu, le format et les exigences de mise à jour de la **fiche de divulgation du fournisseur**, document normalisé par lequel un fournisseur communique son niveau de sécurité à ses clients.

La fiche de déclaration du fournisseur est l'élément fondamental du cadre TPSA. Tous les autres composants, le protocole de dialogue sur les risques (TPSA-02), la matrice de correspondance réglementaire (TPSA-03) et le système d'étiquetage et de certification (TPSA-04), dépendent de la fiche de déclaration comme principale source de données.

1.2 Portée

La norme TPSA-01 s'applique à toute organisation fournissant des services, plateformes, infrastructures ou logiciels TIC à d'autres organisations et souhaitant démontrer une responsabilité structurée en matière de sécurité. Cela inclut, sans s'y limiter : les fournisseurs de services cloud (IaaS, PaaS, SaaS), les fournisseurs de services gérés (MSP/MSSP), les éditeurs de logiciels, les exploitants de centres de données, les fournisseurs de télécommunications et tout tiers traitant, stockant ou transmettant des données client.

La norme est, par sa conception même **, indépendante de toute technologie** et **de toute réglementation** . Elle peut être mise en œuvre quels que soient l'environnement technologique du fournisseur, son modèle d'hébergement ou sa situation géographique. Des correspondances réglementaires (DORA, NIS2, ISO 27001, contrôles CIS) sont fournies dans la norme TPSA-03 à titre de référence complémentaire.

1.3 Références normatives

- **ISO/IEC 27001:2022,** Systèmes de gestion de la sécurité de l'information
- **ISO/IEC 27002:2022,** Contrôles de sécurité de l'information
- **Normes ISO/CEI 27036-1 à 27036-4,** Sécurité de l'information dans les relations avec les fournisseurs
- **Contrôles CIS v8,** Contrôles de sécurité critiques du Centre pour la sécurité Internet
- **DORA (Règlement 2022/2554),** Loi sur la résilience opérationnelle numérique
- **Directive NIS2 (2022/2555),** Directive relative à la sécurité des réseaux et de l'information
- **Gestionnaire de risques EBIOS,** Méthodologie d'analyse des risques ANSSI
- **MITRE ATT&CK,** Tactiques, techniques et connaissances communes en matière d'adversaires
- **TIBER-EU,** Équipe rouge éthique basée sur le renseignement sur les menaces

1.4 Termes et définitions

Les termes définis dans le document de position sur l’Accord de libre-échange transpacifique (version 1.0, avril 2026) s’appliquent. Autres termes propres au présent document :

- **Fiche de divulgation** : document structuré défini par cette norme, publié par un fournisseur pour un client donné ou comme référence commune.
- **Information commune** : la partie d'une fiche d'information qui décrit l'infrastructure, les contrôles et les pratiques partagés applicables à tous les clients.
- **Annexe spécifique au client** : la partie d’une fiche de divulgation adaptée à un client spécifique, détaillant les actifs, la classification des données et les mesures propres à cette relation.
- **Champ obligatoire** : champ qui doit être rempli pour que la fiche de divulgation soit considérée comme conforme à n'importe quel niveau de maturité TPSA.
- **Champ conditionnel** : un champ qui devient obligatoire lorsque des conditions spécifiques sont remplies (par exemple, environnement multi-locataires, client réglementé par DORA).
- **Champ facultatif** : champ qui apporte une transparence supplémentaire mais qui n’est pas requis pour la conformité.

2. Structure de la fiche de divulgation

2.1 Aperçu de l'architecture

Une fiche de divulgation fournisseur est un document structuré composé d'une **section d'en-tête** (métadonnées, versionnage, périmètre) et **de sept domaines de divulgation** , chacun contenant un ensemble défini de champs. La fiche est divisée en une couche **de divulgation commune** et **des annexes facultatives spécifiques au client** .

Couche	Contenu	Public
En-tête	Identité du fournisseur, version de la fiche, période de validité, définition du périmètre, coordonnées.	Toutes les parties prenantes. Métadonnées lisibles par machine pour le traitement automatisé.
Divulgation courante	Infrastructure, contrôles, certifications et pratiques partagés applicables à tous les clients. Domaines D1–D7.	Tous les clients. Publication unique, maintenance centralisée par le fournisseur.
Annexe spécifique au client	Ressources dédiées au client, dérogations à la classification des données, contrôles personnalisés, SLA spécifiques. Superposition par client sur les données D1 à D7.	Client particulier. Confidentialité assurée entre le fournisseur et le client.

2.2 Section d'en-tête

La section d'en-tête fournit les métadonnées nécessaires à l'identification, au versionnage et au traitement automatisé de la fiche de divulgation.

IDENTIFIANT	Champ	Type	Req.	Description
H-01	**Nom du fournisseur**	String	M	Dénomination sociale de l'organisation fournisseur.
H-02	**Identifiant du fournisseur**	String	M	Identifiant unique (par exemple, LEI, DUNS, SIREN/SIRET, numéro d'enregistrement de l'entreprise).
H-03	**Version fiche**	SemVer	M	Numéro de version suivant le versionnage sémantique (MAJOR.MINOR.PATCH).
H-04	**Date d'émission**	ISO 8601	M	Date de publication de cette version.
H-05	**Valable jusqu'au**	ISO 8601	M	Date d'expiration. Validité maximale : 12 mois à compter de la date d'émission.
H-06	**Description du périmètre**	Text	M	Description narrative des services, plateformes et infrastructures couverts par cette fiche de divulgation.
H-07	**Type de fiche**	Enum	M	COMMUNE (référence partagée) ou SPÉCIFIQUE AU CLIENT (annexe client). Une fiche SPÉCIFIQUE AU CLIENT doit faire référence à sa fiche COMMUNE parente.
H-08	**Référence de la fiche parent**	String	C	Référence (ID + version) de la fiche COMMON parente. Obligatoire lorsque le type de fiche est CLIENT_SPECIFIC.
H-09	**Nom du client**	String	C	Nom du client. Obligatoire lorsque le type de fiche est défini sur CLIENT_SPECIFIC.
H-10	**Niveau TPSA**	Enum	M	Niveau de maturité déclaré du TPSA : BASIQUE, AMÉLIORÉ ou COMPLET.
H-11	**Contact, Sécurité**	Objet	M	Coordonnées de l'équipe de sécurité : nom, rôle, adresse e-mail, référence de la clé PGP ou du certificat S/MIME.
H-12	**Contact, Conformité**	Objet	O	Contact de l'équipe Conformité/GRC pour les questions d'audit et de certification.
H-13	**Signature numérique**	ED25519	M	Signature ED25519 du contenu de la fiche, permettant la vérification de l'intégrité et la non-répudiation.

M = Obligatoire | C = Conditionnel | O = Facultatif

3. Domaines de divulgation

La fiche de divulgation est organisée en sept domaines (D1 à D7), chacun abordant une dimension essentielle de la sécurité du fournisseur pour ses clients. Les champs de chaque domaine sont classés comme obligatoires (M), conditionnels (C) ou facultatifs (O).

3.1 Domaine D1 : Inventaire des actifs et cartographie des données

Ce domaine identifie les actifs qui traitent, stockent ou transmettent les données client. Il constitue le fondement de tous les domaines suivants et du protocole de dialogue sur les risques (TPSA-02). Une identification précise des actifs est essentielle pour la définition du périmètre des tests TIBER-EU conformément à l'article 26 de la DORA.

ID	Champ	Type	Req.	Description
D1-01	**Registre des actifs**	Array	M	Liste de tous les actifs (infrastructures, plateformes, applications, bases de données) nécessaires à la fourniture des services au client. Chaque actif comprend : un identifiant unique, son nom, son type (serveur, base de données, application, périphérique réseau, système de stockage, etc.) et une brève description fonctionnelle.
D1-02	**Emplacement de l'actif**	Objet	M	Pour chaque ressource : localisation géographique (pays, région, identifiant du centre de données) et localisation logique (zone réseau, VPC/VLAN, région cloud/AZ). Ces informations sont requises pour la conformité à la résidence des données.
D1-03	**Modèle d'hébergement**	Enum	M	Pour chaque ressource : DÉDIÉE ou PARTAGÉE (mutualisée). Si PARTAGÉE, le fournisseur doit décrire le mécanisme d’isolation (logique, physique, au niveau de l’hyperviseur, au niveau du conteneur).
D1-04	**Types de données hébergés**	Array	M	Pour chaque actif : catégories de données client traitées ou stockées (ex. : données personnelles, données financières, données de santé, identifiants d’authentification, journaux, métadonnées). Conformément à la classification des données de D2.
D1-05	**Diagramme de flux de données**	Référence	C	Référence à un diagramme de flux de données illustrant la circulation des données client entre les ressources, y compris les points d'entrée/sortie et les communications inter-systèmes. Obligatoire aux niveaux AMÉLIORÉ et COMPLET.
D1-06	**Sous-processeurs**	Array	C	Liste des sous-traitants (tiers) impliqués dans le traitement des données client, précisant leur identité, leur rôle, leur localisation et les clauses contractuelles applicables. Cette liste est obligatoire en cas de recours à des sous-traitants.
D1-07	**Classification des actifs**	Enum	M	Classification de chaque actif par le fournisseur (ex. : public, interne, confidentiel, restreint). Sous réserve d’une revalorisation de la classification suite aux commentaires du client (voir section 4).
D1-08	**Propriétaire d'actifs**	String	M	Rôle ou équipe désigné(e) responsable de la sécurité et de la maintenance de chaque actif.

3.2 Domaine D2 : Protection des données

Ce domaine décrit les mesures appliquées pour protéger les données client au repos, en transit et pendant le traitement, notamment la gestion des clés, la ségrégation des données et les politiques de conservation/suppression.

ID	Champ	Type	Req.	Description
D2-01	**Chiffrement au repos**	Object	M	Algorithmes, longueurs de clés et étendue du chiffrement des données client stockées. Par actif ou par type de données si des normes différentes s'appliquent.
D2-02	**Chiffrement en transit**	Object	M	Protocoles (version TLS, suites de chiffrement), portée (client-fournisseur, inter-services, intra-DC) et pratiques de gestion des certificats.
D2-03	**Gestion des clés**	Object	M	Génération des clés, stockage (HSM, KMS, logiciel), fréquence de rotation, contrôles d'accès sur le matériel clé et possibilité pour le client d'apporter ses propres clés (BYOK) ou de conserver ses propres clés (HYOK).
D2-04	**Ségrégation des données**	Object	C	Mécanismes garantissant l'isolation des données client dans les environnements mutualisés : au niveau de la base de données, du schéma, du chiffrement ou de l'application. Obligatoire lorsque D1-03 = PARTAGÉ.
D2-05	**Politique de conservation des données**	Object	M	Durée de conservation par type de données, base juridique de la conservation et processus de suppression automatisée/manuelle à la fin de la période de conservation ou à la résiliation du contrat.
D2-06	**Processus de suppression des données**	Object	M	Procédures de suppression/destruction sécurisée : méthode (effacement cryptographique, destruction physique, écrasement), mécanisme de vérification et délai entre la demande et la finalisation.
D2-07	**Schéma de classification des données**	Object	M	Les niveaux de classification des données du fournisseur et leurs définitions. Il s'agit du point de référence sur lequel fonctionne Classification Uplift (voir section 4).
D2-08	**Transferts transfrontaliers**	Object	C	Mécanismes de transfert international de données (clauses contractuelles types, décisions d'adéquation, règles d'entreprise contraignantes). Obligatoires lorsque les actifs sont répartis sur plusieurs juridictions.

3.3 Domaine D3 : Sauvegarde et récupération

Ce domaine décrit la stratégie de sauvegarde du fournisseur, ses capacités de restauration et, surtout, les preuves de restauration testée. Une sauvegarde qui n'a jamais été testée n'est pas une sauvegarde.

ID	Champ	Type	Req.	Description
D3-01	**Politique de sauvegarde**	Object	M	Périmètre (quels actifs/données sont sauvegardés), fréquence (temps réel/quotidienne/hebdomadaire), type (complète/incrémentale/différentielle) et période de conservation des sauvegardes.
D3-02	**Emplacement de sauvegarde**	Object	M	Emplacement géographique et logique du stockage de sauvegarde. Distance par rapport au site principal. État des sauvegardes : hors ligne (isolation physique) ou en ligne.
D3-03	**Cryptage de sauvegarde**	Object	M	Normes de chiffrement appliquées aux données de sauvegarde, gestion des clés de chiffrement des sauvegardes.
D3-04	**RTO déclaré**	Durée	M	Objectif de temps de rétablissement : temps maximal tolérable pour rétablir le service après une interruption, par service/ressource.
D3-05	**RPO déclaré**	Durée	M	Objectif de point de récupération : perte de données maximale tolérable mesurée en temps, par service/actif.
D3-06	**Dernier test de restauration**	Object	M	Date du test de restauration de sauvegarde le plus récent, étendue du test, résultat (succès/partiel/échec) et problèmes identifiés.
D3-07	**Rétablir la fréquence des tests**	Enum	M	Fréquence des tests de restauration de sauvegarde : mensuelle, trimestrielle, semestrielle, annuelle.
D3-08	**Référence du plan de reprise après sinistre**	Référence	C	Référence au plan de reprise d'activité du fournisseur applicable aux services clients. Obligatoire aux niveaux AMÉLIORÉ et COMPLET.
D3-09	**Résultats du test DR**	Object	C	Date et résultat du dernier test/exercice DR. Obligatoire aux niveaux AMÉLIORÉ et COMPLET.

3.4 Domaine D4 : Contrôle d’accès et gestion des identités

Ce domaine décrit comment le fournisseur contrôle l'accès aux actifs et aux données pertinents pour le client, y compris l'accès privilégié, les mécanismes d'authentification et les processus de révision.

ID	Champ	Type	Req.	Description
D4-01	**Mécanismes d'authentification**	Object	M	Méthodes d'authentification pour l'accès interne aux ressources pertinentes pour le client : type MFA, politique de mot de passe, intégration SSO, authentification par certificat.
D4-02	**Gestion des accès privilégiés**	Object	M	Gestion des comptes privilégiés (administrateur, root, DBA) : outils PAM, enregistrement des sessions, accès juste à temps, procédures d'urgence.
D4-03	**Cycle d'examen d'accès**	Object	M	Fréquence et étendue des examens des droits d'accès. Preuve de la date et du résultat du dernier examen.
D4-04	**Politique du moindre privilège**	Text	M	Description de la manière dont le principe du moindre privilège est appliqué : modèle RBAC/ABAC, séparation des tâches, attitude de refus par défaut.
D4-05	**Accès client**	Object	M	Contrôles des interfaces destinées aux clients : authentification API, accès au portail, sécurité de la console d’administration, fonctionnalités de liste blanche d’adresses IP.
D4-06	**Accès par des tiers**	Object	C	Contrôle de l'accès aux données et systèmes clients par les sous-traitants, prestataires ou personnel de support du fournisseur. Obligatoire en cas d'accès par un tiers.
D4-07	**Journalisation et surveillance**	Object	M	Quels événements d'accès sont enregistrés, quelle est la durée de conservation des journaux d'accès, comment sont surveillés/alertes en cas de schémas d'accès anormaux et si les journaux sont disponibles pour le client ?

3.5 Domaine D5 : Gestion et tests de vulnérabilité

Ce domaine décrit l'approche du fournisseur en matière d'identification, d'évaluation et de correction des vulnérabilités des actifs pertinents pour le client. Il comprend les calendriers et les résultats des tests d'intrusion, qui sont directement liés à la coordination des tests TIBER-EU dans le cadre de l'accord TPSA-02.

ID	Champ	Type	Req.	Description
D5-01	**Analyse des vulnérabilités**	Object	M	Outils, fréquence, portée (interne/externe, infrastructure/application) et SLA pour la remédiation par gravité (critique/élevée/moyenne/faible).
D5-02	**Gestion des correctifs**	Object	M	Processus de déploiement des correctifs, SLA par niveau de gravité (par exemple, Critique : 24 h, Élevé : 72 h, Moyen : 30 j) et processus d'exception/de report.
D5-03	**Tests d'intrusion**	Object	M	Portée, méthodologie (boîte noire/grise/blanche), fréquence et prestataire (interne/externe). Date du dernier test d'intrusion et résumé des principaux résultats.
D5-04	**Correction des tests d'intrusion**	Object	M	État d'avancement des mesures correctives suite au test d'intrusion le plus récent : nombre d'anomalies par gravité, nombre d'anomalies corrigées, nombre d'anomalies acceptées, échéancier pour les points en suspens.
D5-05	**Programme de primes aux bogues**	Object	O	Que le fournisseur gère un programme de primes aux bogues ou de divulgation des vulnérabilités, sa portée et ses indicateurs de réactivité.
D5-06	**Disponibilité SBOM**	booléen	C	La nomenclature logicielle est-elle maintenue et disponible pour les applications destinées aux clients ? Obligatoire au niveau FULL.
D5-07	**Préparation de TIBER-UE**	Object	C	Le fournisseur a-t-il participé ou est-il prêt à participer aux exercices TIBER-EU/TLPT ? Date de la dernière participation, le cas échéant. Obligatoire au niveau FULL.

3.6 Domaine D6 : Gestion et notification des incidents

Ce domaine décrit les capacités du fournisseur en matière de détection, de réponse et de notification des incidents. Les délais de notification sont conformes aux exigences de l'article 19 de la loi DORA pour les fournisseurs tiers de services TIC critiques.

ID	Champ	Type	Req.	Description
D6-01	**Capacités de détection**	Object	M	Outils de surveillance de sécurité (SIEM, EDR, NDR, SOC), étendue de la couverture et SLA de détection (temps moyen de détection).
D6-02	**Plan d'intervention en cas d'incident**	Référence	M	Se référer au plan de réponse aux incidents du fournisseur. Éléments clés : système de classification, matrice d’escalade, rôles et responsabilités.
D6-03	**SLA de notification client**	Object	M	Délai maximal entre la détection d'un incident et la notification au client, selon sa gravité. Les fournisseurs soumis à la réglementation DORA doivent respecter les délais prévus par l'article 19 (notification initiale dans les 4 heures pour les incidents majeurs).
D6-04	**Contenu de la notification**	Object	M	Format défini et contenu minimal des notifications d'incident : actifs affectés, évaluation de l'impact sur les données, mesures de confinement, chronologie, point de contact.
D6-05	**Examen post-incident**	Object	M	Processus d’analyse post-incident : chronologie de l’analyse des causes profondes, plan d’actions correctives, enseignements tirés et communication des conclusions aux clients concernés.
D6-06	**Historique des incidents**	Array	C	Résumé des incidents de sécurité ayant affecté les données/services clients au cours des 24 derniers mois : date, gravité, impact, résolution. Obligatoire aux niveaux AMÉLIORÉ et COMPLET.
D6-07	**Canal de communication**	Object	M	Canal sécurisé dédié aux communications en cas d'incident : méthode de communication hors bande, contacts d'escalade, PGP/S/MIME pour les notifications chiffrées.

3.7 Domaine D7 : État de conformité et de certification

Ce domaine offre une transparence totale sur les certifications existantes du fournisseur, les résultats d'audit et son statut de conformité réglementaire. Il permet aux clients d'évaluer le niveau de maturité initial du fournisseur et d'identifier tout écart par rapport à leurs propres exigences réglementaires.

ID	Champ	Type	Req.	Description
D7-01	**Certifications détenues**	Array	M	Liste des certifications actuelles : norme (ISO 27001, SOC 2, etc.), domaine d'application, organisme émetteur, dates de validité, numéro de référence du certificat.
D7-02	**Étendue de la certification**	Text	M	Une description claire du périmètre de chaque certification est requise. Les clients doivent pouvoir vérifier que les services qu'ils utilisent relèvent bien du périmètre certifié.
D7-03	**Résumé des conclusions de l'audit**	Object	C	Résumé des conclusions du dernier audit de certification : nombre de non-conformités par type (majeures/mineures/observations), état des actions correctives. Obligatoire aux niveaux AMÉLIORÉ et COMPLET.
D7-04	**Statut réglementaire**	Object	C	État de conformité aux réglementations applicables (DORA, NIS2, RGPD, réglementations sectorielles). Auto-évaluation ou vérification indépendante.
D7-05	**Exclusions et lacunes**	Text	O	Lacunes connues dans le périmètre de la certification ou la couverture de la conformité. La transparence concernant les exclusions renforce la confiance et permet aux clients de prendre des décisions éclairées.
D7-06	**Couverture d'assurance**	Object	O	Couverture d'assurance cyber : assureur, limites de couverture, étendue. Facultatif, mais pertinent pour l'évaluation des risques du client.

4. Mécanisme d'amélioration de la classification

L'amélioration de la classification est une propriété émergente du cadre TPSA qui tire parti de la divulgation bidirectionnelle pour améliorer la posture de sécurité dans les environnements multi-locataires.

4.1 Mécanisme

Lorsqu'un client consulte la fiche de divulgation (notamment les sections D1-07 : Classification des actifs et D2-07 : Schéma de classification des données), il peut constater que la classification d'un actif partagé par le fournisseur est inférieure à sa propre classification des données hébergées sur cet actif. Par exemple, un fournisseur peut classer une baie de stockage partagée comme « Interne » tandis qu'un client du secteur bancaire classe les données qui y sont stockées comme « Confidentielles ».

Dans le cadre du TPSA, le client soumet une **demande de reclassement** par le biais de l'annexe spécifique au client, informant le fournisseur que ses données sur l'actif identifié nécessitent un niveau de classification supérieur.

4.2 Obligations du fournisseur

Dès réception d'une demande de reclassement, le fournisseur doit :

- **Accuser réception** de la demande dans un délai de 10 jours ouvrables.
- **Évaluer** l'impact de la hausse sur les contrôles existants et sur les autres clients partageant le même actif.
- **Appliquer** la classification supérieure à l'actif si cela est techniquement et opérationnellement possible, ou **proposer** des mesures alternatives (par exemple, migration vers un actif dédié, couche de chiffrement supplémentaire, amélioration de l'isolation logique).
- **Mettre à jour** la fiche de divulgation commune pour refléter la nouvelle classification, le cas échéant.
- **Informer** les autres clients utilisant le même actif partagé du changement de classification (sans divulguer l'identité du client demandeur).

4.3 Effet de marée montante

L'amélioration de la classification crée un **cercle vertueux** dans les environnements mutualisés. Le client le plus exigeant renforce le niveau de sécurité, et tous les autres clients bénéficient de contrôles améliorés. À terme, les ressources partagées convergent vers le niveau de classification le plus élevé de tous les locataires, ce qui représente une sécurité optimale.

Ce mécanisme inverse la dynamique actuelle du marché, où les environnements mutualisés tendent à adopter le plus petit dénominateur commun. Dans le cadre du TPSA, les fournisseurs sont incités à répondre aux exigences des clients, car l'effort supplémentaire est amorti entre tous les « locataires ».

5. Cycle de vie de la fiche de divulgation

5.1 Publication

Le fournisseur publie la fiche d'information initiale dès l'adoption de l'accord de partage de données (TPSA). La fiche d'information commune est publiée en premier ; des annexes spécifiques au client sont créées en fonction des besoins liés à la relation client.

Format de publication : la fiche de déclaration doit être disponible au **format JSON** conforme au schéma JSON TPSA-01 (voir annexe A). Des formats lisibles par l'humain (PDF, HTML) peuvent être générés à partir de la représentation JSON canonique. Le document JSON doit être signé numériquement à l'aide du formulaire ED25519 (champ H-13).

5.2 Gestion des versions

Les fiches de divulgation suivent **le versionnage sémantique** :

- **majeure** de la version : modifications structurelles de la fiche(nouveaux domaines, suppressions de champs, modifications du schéma).
- **mineure** de version : mises à jour de contenu qui modifient le niveau de sécurité (nouveaux actifs, contrôles modifiés, résultats de tests d'intrusion mis à jour).
- **PATCH** : corrections, clarifications ou modifications de formatage sans impact sur la sécurité.

Chaque modification de version doit mettre à jour la date de publication (H-04) et être signée à nouveau (H-13). Un journal des modifications doit être tenu.

5.3 Cycle d'évaluation

Les fiches de divulgation doivent être revues et mises à jour au minimum :

- **TPSA de base** : annuellement.
- **TPSA amélioré** : semestriellement et dans les 30 jours suivant tout changement important (nouvel actif, incident important, changement de certification).
- **TPSA complet** : mis à jour en continu, avec des mises à jour publiées dans les 15 jours suivant tout changement important.

5.4 Révocation

Une fiche de divulgation peut être révoquée par le fournisseur si les services décrits sont interrompus ou si son contenu devient matériellement inexact en attendant sa mise à jour. La révocation doit être communiquée à tous les clients disposant d'annexes spécifiques actives. Une fiche révoquée ne peut être utilisée à des fins de conformité.

6. Exigences de conformité

Une fiche de divulgation est conforme à la norme TPSA-01 lorsqu'elle répond aux critères suivants :

6.1 Conformité structurelle

- La fiche est publiée au format JSON valide, conforme au schéma JSON TPSA-01.
- Tous les champs obligatoires (M) sont remplis avec un contenu substantiel.
- Tous les champs conditionnels (C) applicables sont remplis lorsque leurs conditions de déclenchement sont remplies.
- La fiche est signée numériquement à l'aide de ED25519 (H-13) et la signature est vérifiable.
- La version fiche(H-03) suit les conventions de versionnement sémantique.

6.2 Conformité du contenu

- Les valeurs des champs sont exactes et à jour à la date de publication.
- Les inventaires d’actifs (D1) sont complets, aucun actif impliqué dans le traitement des données client n’est omis.
- Les dates (dernier test d'intrusion, dernier test de restauration, dernière revue d'accès) sont précises et vérifiables, et non vagues ou approximatives.
- Les statuts de remédiation (D5-04, D7-03) reflètent l'état réel, et non les résultats planifiés ou souhaités.

6.3 Exigences relatives au niveau de maturité

Critère	BASIC	ENHANCED	FULL
Champs obligatoires	Tous les champs M	Tous les champs M + tous les champs C applicables	Tous les champs M + C + O recommandés
Cycle d'examen	Annuel	Semestriel + événementiel (30 jours)	En continu (15 jours après le changement de matériau)
Soutien de l'annexe	Divulgation courante uniquement	Annexes communes et spécifiques au client	Processus d'amélioration commun + spécifique au client + classification
Signature	ED25519 requis	ED25519 requis	ED25519 requis + contresignature de l'auditeur
TIBER-UE	Non requis	Déclaration de préparation	Capacité de participation active démontrée

Annexe A : Schéma JSON (Extrait)

Voici un extrait du schéma JSON TPSA-01 définissant la structure de la fiche de divulgation. Le schéma complet est publié sous forme de fichier autonome lisible par machine (tpsa-01-schema.json).

```
{
  "$schema": "https://json-schema.org/draft/2020-12/schema",
  "$id": "https://tpsa.org/schemas/tpsa-01/v1.0",
  "title": "TPSA-01 Supplier Disclosure Card",
  "type": "object",
  "required": ["header", "domains"],
  "properties": {
    "header": {
      "type": "object",
      "required": ["supplier_name", "supplier_id", "card_version",
                   "issue_date", "valid_until", "scope_description",
                   "card_type", "tpsa_level", "contact_security",
                   "digital_signature"],
      "properties": {
        "supplier_name": { "type": "string" },
        "supplier_id": {
          "type": "object",
          "properties": {
            "type": { "enum": ["LEI","DUNS","SIREN","OTHER"] },
            "value": { "type": "string" }
          }
        },
        "card_version": { "type": "string", "pattern": "^\\d+\\.\\d+\\.\\d+$" },
        "issue_date": { "type": "string", "format": "date" },
        "valid_until": { "type": "string", "format": "date" },
        "card_type": { "enum": ["COMMON", "CLIENT_SPECIFIC"] },
        "tpsa_level": { "enum": ["BASIC", "ENHANCED", "FULL"] },
        "contact_security": { "$ref": "#/$defs/contact" },
        "digital_signature": { "$ref": "#/$defs/ed25519_sig" }
      }
    },
    "domains": {
      "type": "object",
      "required": ["d1_assets","d2_data_protection","d3_backup",
                   "d4_access_control","d5_vulnerability_mgmt",
                   "d6_incident_mgmt","d7_compliance"],
      "properties": {
        "d1_assets": { "$ref": "#/$defs/domain_d1" },
        "d2_data_protection": { "$ref": "#/$defs/domain_d2" },
        "d3_backup": { "$ref": "#/$defs/domain_d3" },
        "d4_access_control": { "$ref": "#/$defs/domain_d4" },
        "d5_vulnerability_mgmt": { "$ref": "#/$defs/domain_d5" },
        "d6_incident_mgmt": { "$ref": "#/$defs/domain_d6" },
        "d7_compliance": { "$ref": "#/$defs/domain_d7" }
      }
    }
  }
}
```

Annexe B : Exemple de fiche de divulgation

Voici un exemple fictif, mais réaliste, de fiche de divulgation commune pour un fournisseur SaaS de taille moyenne. Il illustre la manière dont chaque domaine est renseigné en pratique.

En-tête

Champ	Valeur
Nom du fournisseur	CloudWorks SAS
ID du fournisseur	SIRÈNE : 987 654 321
Version fiche	1.2.0
Date d'émission	2026-04-01
Valable jusqu'au	31 mars 2027
Portée	Plateforme de gestion documentaire CloudWorks (DMP), Application SaaS hébergée sur une infrastructure dédiée chez Equinix PA3 (Paris) et Equinix FR5 (Francfort). Elle couvre l'ensemble des composants de la plateforme : application web, passerelle API, stockage de documents, indexation de recherche et services d'authentification.
Type de fiche	COMMUN
Niveau TPSA	ENHANCED
Contact, Sécurité	Marie Dupont, RSSI, security@cloudworks.example.com, PGP : 0xABCD1234

D1 : Inventaire des actifs (extrait)

ID de l'actif	Nom	Type	Emplacement	Hébergement	Classification	Types de données
CW-SRV-01	Cluster d'applications DMP	Cluster Kubernetes	Équinix PA3, FR	Mutualisé	Confidentiel	Logique, données de session
CW-DB-01	Base de données principale (PostgreSQL)	Base de données	Équinix PA3, FR	Mutualisé	Confidentiel	Métadonnées client, comptes utilisateurs, index des documents
CW-STO-01	Stockage de documents (compatible S3)	Stockage d'objets	Équinix PA3, FR	Mutualisé	Limité	Documents clients (cryptés par client)
CW-STO-02	Stockage de sauvegarde	Stockage d'objets	Equinix FR5, DE	Mutualisé	Limité	Répliques de sauvegarde chiffrées

D3 : Sauvegarde et restauration (extrait)

Champ	Valeur
Politique de sauvegarde	Sauvegarde quotidienne complète de CW-DB-01 à 02h00 UTC. Réplication continue de CW-STO-01 vers CW-STO-02 (Equinix FR5). Sauvegardes incrémentielles du journal des transactions toutes les 15 minutes. Durée de conservation : 30 jours pour les sauvegardes quotidiennes, 90 jours pour les sauvegardes hebdomadaires et 1 an pour les sauvegardes mensuelles.
Emplacement de sauvegarde	CW-STO-02, Equinix FR5 Francfort, Allemagne. À 450 km du site principal. Réplication en ligne hebdomadaire avec instantané hors ligne toutes les 4 heures sur bande LTO-9.
RTO déclaré	Services de la plateforme : 4 heures. Accès aux documents : 8 heures. Reprise complète des opérations : 24 heures.
RPO déclaré	Base de données : 15 minutes (journal des transactions). Stockage des documents : < 1 heure (délai de réplication continue).
Dernier test de restauration	15/02/2026. Restauration complète de CW-DB-01 à partir de la sauvegarde quotidienne vers un environnement isolé. Résultat : SUCCÈS. Durée de la restauration : 2 h 47 (RTO inférieur à 4 h). Intégrité des données vérifiée par comparaison de sommes de contrôle. 100 % des enregistrements ont été récupérés.
Rétablir la fréquence des tests	Trimestriel. Prochaine échéance : 15 mai 2026.

D5 : Gestion des vulnérabilités (extrait)

Champ	Valeur
Analyse des vulnérabilités	Externe : hebdomadaire (Qualys). Interne : quotidienne (Wazuh). Images de conteneurs : à chaque compilation (Trivy). SLA : Critique 24 h, Élevée 72 h, Moyenne 30 j, Faible 90 j.
Tests d'intrusion	Test d'intrusion externe annuel réalisé par Synacktiv (boîte grise). Dernier test : du 20/01/2026 au 07/02/2026. Périmètre : surface d'attaque externe + API + flux d'authentification. Méthodologie : OWASP WSTG + PTES.
Correction des tests d'intrusion	Résultats : 0 critique, 2 élevée, 5 moyenne, 8 faible. Élevée : 2/2 traitées (28/02/2026). Moyenne : 4/5 traitées, 1 acceptée avec mesures compensatoires (documentées). Faible : 6/8 traitées, 2 programmées pour le deuxième trimestre 2026.
Préparation de TIBER-UE	Participation non encore enregistrée. Évaluation de l'état de préparation terminée en mars 2026. Documentation de cadrage préparée. Disponible pour les exercices TLPT initiés par le client à partir du troisième trimestre 2026.

D6 : Gestion des incidents (extrait)

Champ	Valeur
Capacités de détection	SOC : interne (8h/24 et 5j/7), Sekoia.io MDR (24h/24 et 7j/7). SIEM : Wazuh. EDR : CrowdStrike Falcon sur tous les terminaux. NDR : Suricata sur le périmètre réseau. Délai moyen de détection (MTTD) : < 15 minutes pour les alertes critiques.
SLA de notification client	Incident critique/majeur : notification initiale dans les 4 heures suivant la détection (conformément à la loi DORA). Incident significatif : notification dans les 24 heures. Incident mineur : inclus dans le prochain rapport de sécurité périodique. Format de notification : courriel structuré (chiffré PGP) avec modèle d'incident TPSA.
Historique des incidents (24 min)	12/09/2025 : Incident de gravité moyenne. Tentative d'accès non autorisé à la passerelle API (attaque par force brute). Détectée en 8 minutes, bloquée automatiquement. Aucune donnée n'a été compromise. Cause première : absence de limitation de débit sur le point de terminaison existant. Corrigé le 14/09/2025 (limitation de débit déployée). Aucune donnée client n'a été affectée.

D7 : Conformité et certification (extrait)

Champ	Valeur
Certifications détenues	ISO 27001:2022, Domaine d'application : Exploitation et développement de la plateforme DMP. Organisme certificateur : LSTI. Période de validité : du 1er juin 2025 au 31 mai 2028. Certificat : LSTI-27001-2025-0847. SOC 2 Type II, Domaine d'application : Critères de confiance en matière de sécurité et de disponibilité. Période de validité : du 1er janvier 2025 au 31 décembre 2025. Auditeur : Mazars.
Constatations de l'audit	Audit de surveillance ISO 27001 (janvier 2026) : 0 non-conformité majeure, 1 non-conformité mineure (preuves incomplètes de l'examen de sécurité des fournisseurs pour un sous-traitant). Action corrective terminée le 15 février 2026.
Exclusions et lacunes	L'informatique d'entreprise (messagerie interne, systèmes RH) n'est pas couverte par la norme ISO 27001. La certification HDS (Hébergement de Données de Santé) n'est pas détenue ; les données de santé ne doivent pas être stockées sur la plateforme sans accord préalable et contrôles supplémentaires.