



Fournisseurs Microsoft

Guide du programme d'assurance de la
sécurité et de la confidentialité des
fournisseurs (SSPA)

Version 10

Septembre 2024

Table des matières

Vue d'ensemble du programme SSPA.....	3
Profil de traitement des données.....	3
Champ d'application :	8
Données personnelles par type	8
Données confidentielles de Microsoft.....	11
Lieu du traitement	12
Rôle dans le cadre du traitement des données.....	12
Traitement de cartes de paiement	13
Exigence de certification de conformité aux normes de sécurité de l'industrie des cartes de paiement (PCI DSS).....	13
Logiciel à la demande (SaaS)	14
Utilisation de sous-traitants ultérieurs.....	14
Hébergement de sites Web	15
Soins de santé.....	15
Systèmes d'intelligence artificielle (IA)	15
Vue d'ensemble du processus SSPA	16
Qu'est-ce que le SSPA ?	16
Diagramme du processus SSPA – Inscription des nouveaux fournisseurs	17
Diagramme du processus SSPA – Reconduction annuelle du fournisseur	17
Exigence en matière d'assurance	17
Auto-Attestation de conformité au DPR	18
Exigence d'évaluation indépendante.....	19
Profils nécessitant une assurance indépendante supplémentaire :	20
Incidents relatifs aux données	20

Vue d'ensemble du programme SSPA

Le programme d'assurance de la sécurité et de la confidentialité des fournisseurs (« **SSPA** ») est un partenariat entre les services Fournisseurs, Affaires Publiques, Externes et Juridiques, Sécurité d'entreprise et le Bureau de l'IA responsable de Microsoft pour s'assurer que nos fournisseurs respectent les principes de confidentialité, de sécurité et d'intelligence artificielle responsable. Le programme d'assurance de la sécurité et de la confidentialité des fournisseurs (« SSPA » ou « Supplier Security and Privacy Assurance ») est le programme mis en place par Microsoft pour transmettre les instructions fondamentales de traitement des données de Microsoft à nos fournisseurs, sous la forme des exigences de protection des données des fournisseurs de Microsoft (« DPR »), disponibles sur Microsoft.com/Fournisseurs.

Les fournisseurs ont la possibilité de sélectionner des profils de traitement des données qui correspondent aux biens et/ou services que vous êtes chargé de fournir. Ces choix sont associés à des exigences en matière de garantie de conformité à Microsoft.

Tous les fournisseurs inscrits devront remplir chaque année une auto-attestation de respect du DPR. Votre profil de traitement des données détermine si l'intégralité du DPR ou un sous-ensemble d'exigences s'applique. Les fournisseurs qui traitent des données que Microsoft considère comme présentant un risque plus élevé peuvent également devoir satisfaire à des exigences supplémentaires, telles qu'une vérification indépendante de la conformité (voir [Évaluation indépendante](#)). Notez que les fournisseurs peuvent avoir à répondre à des exigences de niveau organisationnel supplémentaires définies et communiquées indépendamment du SSPA par le groupe de Microsoft responsable des relations avec les fournisseurs.

Important : Les activités de conformité réalisées permettent de déterminer le statut SSPA Vert (conforme) ou Rouge (non conforme) et des approbations de traitement des données (voir ci-dessous pour le Profil de traitement des données). Les outils d'achat de Microsoft valident que le statut SSPA est vert (pour chaque fournisseur concerné par le SSPA) avant d'autoriser toute transaction.

Profil de traitement des données

Les fournisseurs de Microsoft contrôlent leur profil de traitement des données SSPA. Les approbations choisies dans le profil de traitement des données aident le SSPA à évaluer le niveau de risque de votre (vos) engagement(s) auprès de Microsoft. Les exigences de conformité du SSPA varient en fonction du profil de traitement des données et des approbations associées, ce qui permet aux fournisseurs de déterminer les engagements pour lesquels ils souhaitent être éligibles. Il est important d'examiner attentivement les sélections et les activités de conformité qui doivent être menées à bien pour obtenir l'approbation.

Les groupes commerciaux Microsoft ne pourront travailler avec des fournisseurs que lorsque l'activité de traitement des données correspond aux approbations obtenues par ceux-ci.

Les fournisseurs pourront mettre à jour leur profil de traitement des données à tout moment de l'année s'il n'y a pas de tâches ouvertes. Si des modifications sont apportées, l'activité de

conformité applicable (tâches) sera émise et devra être réalisée avant que les nouvelles approbations ne soient répercutées sur votre profil de traitement des données. Les approbations existantes et achevées s'appliqueront jusqu'à satisfaction des exigences nouvellement communiquées. Si les tâches nouvellement exécutées ne sont pas terminées dans le délai de 90 jours autorisé, la situation au regard du SSPA passera au rouge (non conforme) et le compte risque d'être désactivé des systèmes de comptes fournisseurs de Microsoft.

Il existe également des combinaisons qui peuvent élever ou réduire les exigences de conformité. Elles figurent dans l'annexe A et c'est ce que vous pouvez vous attendre à signer à partir du portail de conformité des fournisseurs Microsoft lorsque vous renseignez votre profil. Vous pouvez toujours valider l'adéquation de votre scénario à ce cadre en demandant un examen par l'équipe SSPA.

Tableau du profil de traitement des données

#	Profil	Exigences :	Options d'assurance indépendantes
1	<p>Champ d'application : Personnel, confidentiel</p> <p>Lieu de traitement : Chez Microsoft ou le client</p> <p>Rôle dans le cadre du traitement des données : Sous-traitant ou Responsable du traitement</p> <p>Classe de données : Confidentielles ou Hautement confidentielles</p> <p>Cartes de paiement : Non applicable</p> <p>SaaS : Non applicable</p> <p>Utilisation de sous-traitants ultérieurs : N/A ou OUI</p> <p>Hébergement de site Web : N/A ou OUI</p> <p>Soins de santé : N/A ou OUI</p>	Auto-Attestation de conformité au DPR	
2	<p>Champ d'application : Données confidentielles</p> <p>Lieu de traitement : Chez le fournisseur</p> <p>Rôle dans le cadre du traitement des données : Non applicable</p> <p>Classe de données : Données confidentielles</p> <p>Cartes de paiement : Non applicable</p> <p>SaaS : Non applicable</p> <p>Utilisation de sous-traitants ultérieurs : Non applicable</p> <p>Hébergement de site Web : Non applicable</p> <p>Soins de santé : Non applicable</p>	Auto-Attestation de conformité au DPR	

3	<p>Champ d'application : Données confidentielles</p> <p>Lieu de traitement : Chez le fournisseur</p> <p>Rôle dans le cadre du traitement des données : Non applicable</p> <p>Classe de données : Hautement confidentielles</p> <p>Cartes de paiement : Non applicable</p> <p>SaaS : Non applicable</p> <p>Utilisation de sous-traitants ultérieurs : Non applicable</p> <p>Hébergement de site Web : Non applicable</p> <p>Soins de santé : Non applicable</p>	<p>Auto-attestation de conformité au DPR</p> <p>et</p> <p>Assurance indépendante de la conformité</p>	<p>Options d'assurance indépendantes :</p> <ol style="list-style-type: none"> 1. Effectuer une évaluation indépendante par rapport au DPR, <p>ou</p> <ol style="list-style-type: none"> 2. Soumettre ISO 27001
4	<p>Champ d'application : Personnel, confidentiel</p> <p>Lieu de traitement : Chez le fournisseur</p> <p>Rôle dans le cadre du traitement des données : Sous-traitant de données</p> <p>Classe de données : Hautement confidentielles</p> <p>Cartes de paiement : Non applicable</p> <p>SaaS : Non applicable</p> <p>Utilisation de sous-traitants ultérieurs : Non applicable</p> <p>Hébergement de site Web : Non applicable</p> <p>Soins de santé : Non applicable</p>	<p>Auto-attestation de conformité au DPR</p> <p>et</p> <p>Assurance indépendante de la conformité</p>	<p>Options d'assurance indépendantes :</p> <ol style="list-style-type: none"> 1. Effectuer une évaluation indépendante par rapport au DPR, <p>ou</p> <ol style="list-style-type: none"> 2. Évaluation indépendante par rapport aux sections A-I du DPR et ISO 27001, <p>ou</p> <ol style="list-style-type: none"> 3. Soumettre ISO 27701 et ISO 27001
5	<p>Champ d'application : Personnel, confidentiel</p> <p>Lieu de traitement : Chez le fournisseur</p> <p>Rôle dans le cadre du traitement des données : Sous-traitant de données</p> <p>Classe de données : Données confidentielles</p> <p>Cartes de paiement : Non applicable</p> <p>SaaS : Non applicable</p> <p>Utilisation de sous-traitants ultérieurs : Non applicable</p> <p>Hébergement de site Web : Non applicable</p> <p>Soins de santé : Non applicable</p>	<p>Auto-attestation de conformité au DPR</p>	
6	<p>Champ d'application : Personnel, confidentiel</p> <p>Lieu de traitement : Chez le fournisseur</p>	<p>Auto-attestation de conformité au DPR</p>	

	<p>Rôle dans le cadre du traitement des données : Responsable du traitement des données</p> <p>Classe de données : Hautement confidentielles ou Confidentielles</p> <p>Cartes de paiement : Non applicable</p> <p>SaaS : Non applicable</p> <p>Utilisation de sous-traitants ultérieurs : N/A ou OUI</p> <p>Hébergement de site Web : Non applicable</p> <p>Soins de santé : N/A ou OUI</p>		
7	<p>Champ d'application : Personnel, confidentiel</p> <p>Lieu de traitement : N'importe lequel</p> <p>Rôle dans le cadre du traitement des données : Sous-traitant ultérieur (ce rôle est déterminé par Microsoft – le profil indiquera « Approbation de sous-traitant ultérieur » : Oui)</p> <p>Classe de données : Hautement confidentielles ou Confidentielles</p> <p>Cartes de paiement : Non applicable</p> <p>SaaS : Non applicable</p> <p>Utilisation de sous-traitants ultérieurs : Non applicable</p> <p>Hébergement de site Web : Non applicable</p> <p>Soins de santé : Non applicable</p>	<p>Auto-attestation de conformité au DPR</p> <p>et</p> <p>Assurance indépendante de la conformité</p>	<p>Options d'assurance indépendantes :</p> <ol style="list-style-type: none"> 1. Effectuer une évaluation indépendante par rapport au DPR, <p>ou</p> <ol style="list-style-type: none"> 2. Évaluation indépendante par rapport aux sections A-I du DPR et ISO 27001, <p>ou</p> <ol style="list-style-type: none"> 3. Soumettre ISO 27701 et ISO 27001
8	<p>Champ d'application : Personnel, confidentiel</p> <p>Lieu de traitement : Chez le fournisseur</p> <p>Rôle dans le cadre du traitement des données : Sous-traitant de données</p> <p>Classe de données : Hautement confidentielles ou Confidentielles</p> <p>Cartes de paiement : Non applicable</p> <p>Sous-traitants ultérieurs : OUI ou</p> <p>SaaS : OUI ou</p> <p>Hébergement de site Web : OUI ou</p> <p>Soins de santé : OUI</p>	<p>Auto-attestation de conformité au DPR</p> <p>et</p> <p>Assurance indépendante de la conformité</p>	<p>Options d'assurance indépendantes :</p> <ol style="list-style-type: none"> 1. Effectuer une évaluation indépendante par rapport au DPR, <p>ou</p> <ol style="list-style-type: none"> 2. Évaluation indépendante par rapport aux sections A-I du DPR et ISO 27001, <p>ou</p> <ol style="list-style-type: none"> 3. Soumettre ISO 27701 et ISO 27001 <p>or</p> <ol style="list-style-type: none"> 4. Rapport HITRUST (uniquement pour

			une entité couverte ou un prestataire de services de santé aux États-Unis)
	Tout profil parmi ceux qui figurent ci-dessus et cartes de paiement	Exigences applicables ci-dessus et assurance PCI	Soumettre la certification PCI
	Tout profil parmi ceux qui figurent ci-dessus et logiciel à la demande (SaaS)	Exigences applicables ci-dessus et soumettre sa certification ISO 27001 exigée par le contrat couvrant les services fonctionnels.	Soumettre une certification ISO 27001 avec une couverture fonctionnelle des services fournis.
	Tout profil parmi ceux qui figurent ci-dessus et Systemes d'intelligence artificielle (IA)	Auto-attestation de conformité au DPR, y compris la partie sur l'IA et Assurance indépendante de la conformité	Options d'assurance indépendantes : 1. Effectuer une évaluation indépendante par rapport au DPR, y compris la partie sur l'IA, ou 2. Évaluation indépendante par rapport aux sections A-I du DPR et ISO 27001, ou 3. Évaluation indépendante par rapport aux sections A-I du DPR et ISO 27701 et ISO 27001, ou

			<p>4. Soumettre ISO 27701, ISO 27001, et ISO 42001</p> <p>(*ISO 42001 requise pour la prestation de services impliquant des systèmes d'IA à usage sensible)</p>
--	--	--	---

Champ d'application :

Données confidentielles

Sélectionnez cette approbation si les Prestations du fournisseur font intervenir le traitement de données confidentielles Microsoft uniquement.

Si vous sélectionnez cette approbation, vous ne serez pas éligible aux missions de traitement des données personnelles.

Personnel, confidentiel

Sélectionnez cette approbation si les performances du fournisseur font intervenir le traitement de données personnelles et confidentielles de Microsoft.

Pour vous aider à déterminer si vous (le fournisseur) traitez des données personnelles et/ou des données confidentielles de Microsoft, consultez la liste d'exemples dans les tableaux ci-dessous. Veuillez noter qu'il ne s'agit que d'exemples et non d'une liste exhaustive.

Remarque : Un responsable Microsoft peut demander une inscription même si le fournisseur ne figure pas sur cette liste en raison de la nature confidentielle des données traitées.

Données personnelles par type

On peut citer à titre d'exemple, sans toutefois s'y limiter :

Données sensibles
Données relatives à des enfants
Données génétiques, biométriques, ou relatives à la santé
Origine raciale ou ethnique
Croyances, convictions et affiliations politiques, religieuses ou philosophiques
Adhésion à un syndicat
Vie ou orientation sexuelle d'une personne physique
Situation au regard de l'immigration (visa, autorisation de travail, etc.)

Identifiants gouvernementaux (passeport, permis de conduire, visa, numéros de sécurité sociale, numéros d'identité nationale)
Données de localisation précise de l'utilisateur (dans un rayon de 300 mètres)
Numéros de compte bancaire personnel
Numéro et date d'expiration des cartes de crédit ; ou code de sécurité ou d'accès ou mot de passe / informations d'authentification permettant d'accéder à un compte
Informations pseudonymisées de l'utilisateur final (EUPI) (Identifiants générés par Microsoft pour identifier les utilisateurs de produits et services de Microsoft) <ul style="list-style-type: none"> • Identificateur global unique (GUID) • Identifiant d'utilisateur de passeport ou Identifiant unique (PUID) • Informations d'identification d'utilisateur final hachées (EUII) • Identifiants de session • Identifiants d'appareil • Données de diagnostic • Données d'enregistrement • Données des clients associées à un dossier d'assistance
Données relatives au contenu des clients
Documents, photos, vidéos, musique, etc.
Avis et / ou notations publiées pour un produit ou service
Réponses à des enquêtes
Historique de navigation, intérêts et liste des favoris
Signatures, texte saisi et paroles prononcées (voix/audio et/ou chat/bot)
Données d'autorisation (mots de passe, indications en vue de la récupération des mots de passe, nom d'utilisateur, données biométriques utilisées à des fins d'identification)
Données des clients associées à un dossier d'assistance
Données capturées et générées
Données de localisation imprécises
Adresse IP
Préférences et personnalisation des appareils

Utilisation du service pour les sites Web, pistage des clics sur les pages Web
Données relatives aux réseaux sociaux, graphe des relations sociales
Données d'activité des appareils connectés tels que des moniteurs d'activité physique
Coordonnées telles que le nom, l'adresse, le numéro de téléphone, l'adresse de courrier électronique, la date de naissance, les contacts des personnes à charge et en cas d'urgence
Évaluation des fraudes et risques, vérification des antécédents
Assurance, retraite, détails des prestations sociales
CV de candidats, notes d'entretien/feed-back
Métadonnées et télémétrie
Données relatives aux comptes
Données des instruments de paiement
Numéro et date d'expiration de cartes de crédit
Coordonnées d'acheminement des virements interbancaires
Numéro de compte bancaire
Demandes ou lignes de crédit
Documents et identifiants fiscaux
Données relatives aux investissements ou dépenses
Cartes d'entreprise
Données des clients en ligne
Client de Microsoft online enterprise (locataire Azure, locataire M365, etc.)
Client de Microsoft consumer (Xbox Live, OneDrive Consumer)
Client de Microsoft entreprise (client sur site)
Données d'assistance (le client émet un ticket)
Données relatives aux comptes (données de facturation, e-commerce)
Enquête /inscription à un événement / une formation
Informations médicales protégées
Numéros d'identification nationaux (y compris les numéros tribaux et les numéros d'identification des informations médicales)

Données démographiques utilisées dans un contexte d'informations médicales protégées (IMP) :

- Date de naissance
- Sexe
- Appartenance ethnique
- Données biométriques
- Photos du visage
- Adresse (complète ou partielle)
- Coordonnées
- Coordonnées en cas d'urgence

Usage sensible (systèmes d'IA)

Incidence sur la situation juridique ou les possibilités de vie, y compris :

- Systèmes d'évaluation et de notation des risques du système de justice pénale
- Système d'admission dans l'enseignement supérieur
- Systèmes d'évaluation et de demande de crédit

Risque de blessure physique ou psychologique, y compris :

- Systèmes de diagnostic ou de traitement médical
- Systèmes de santé mentale et de bien-être
- Systèmes de contrôle des équipements et de maintenance prédictive

Menace pour les droits de l'homme, y compris :

- Systèmes médiatiques synthétiques susceptibles de générer de la désinformation ou de la propagande politique afin d'influencer les élections
- Système d'alerte fondé sur des expressions religieuses, politiques ou sociales
- Système de crédit social

Données confidentielles de Microsoft

On peut citer à titre d'exemple, sans toutefois s'y limiter les données suivantes :

Hautement confidentielles

Informations relatives ou liées au développement, au test ou à la fabrication de produits ou de composants de produits Microsoft

Les logiciels, les services en ligne ou le matériel Microsoft vendus dans le commerce par tout canal sont considérés comme des « Produits Microsoft »

Remarque : Pour le développement d'un produit de jeu, le responsable Microsoft peut indiquer si le produit de travail doit comporter une classification de données hautement confidentielles ou confidentielles.

Informations relatives au marketing des appareils Microsoft préalables à la mise sur le marché
Données financières d'entreprise Microsoft non annoncées soumises aux règles de la SEC

Confidentielles
Clés de licence de produit Microsoft au nom de Microsoft pour distribution par une méthode quelconque
Informations concernant ou liées au développement ou au test des applications internes d'une activité (LOB)
Informations relatives au marketing des logiciels et services Microsoft tels que Office, SQL, Azure, etc., préalables à la mise sur le marché
Documentation écrite, de conception, électronique ou imprimée pour tous les services ou produits Microsoft, tels que les appareils (guides de processus ou de procédure, données de configuration, etc.)

Important : Un responsable de Microsoft peut exiger la participation pour des données ne figurant pas sur cette liste.

Lieu du traitement

Chez Microsoft ou le client

Sélectionnez cette approbation si les Prestations du fournisseur font intervenir le traitement des données dans l'environnement réseau Microsoft où le personnel utilise les identifiants d'accès @microsoft.com ou dans l'environnement d'un client Microsoft.

Ne choisissez pas cette option dans les circonstances suivantes :

- Le fournisseur gère une installation extraterritoriale (OF) désignée par Microsoft.
- Le fournisseur fournit des ressources à Microsoft, et il travaille parfois sur et hors du réseau Microsoft. Le lieu de traitement pour le travail hors réseau est considéré comme « chez le fournisseur ».

Chez le fournisseur

Si la condition « chez Microsoft ou le client » (telle que décrite ci-dessus) ne s'applique pas, sélectionnez cette option.

Rôle dans le cadre du traitement des données

Contrôleur

Sélectionnez cette approbation si tous les aspects des Prestations du fournisseur répondent à la définition du rôle du Responsable du traitement des données (voir DPR).

Si vous sélectionnez cette approbation, vous ne serez pas éligible au traitement des données personnelles avec la désignation de rôle « Sous-traitant ». Si le fournisseur est à la fois un Responsable du traitement et un Contrôleur des données de Microsoft, ne sélectionnez pas « Contrôleur » et sélectionnez plutôt Responsable du traitement des données.

Responsable du traitement des données

Il s'agit du rôle de traitement le plus courant lorsque les fournisseurs traitent les données pour le compte de Microsoft. Veuillez consulter la définition de sous-traitant dans le DPR.

Sous-traitant ultérieur de données

Les fournisseurs ne peuvent pas s'auto-identifier en tant que sous-traitants ultérieurs chez Microsoft, car cela nécessite une approbation préalable par les équipes internes chargées du respect de la vie privée. Veuillez consulter la définition de Sous-traitant ultérieur de données dans le DPR. Les sous-traitants ultérieurs sont soumis à des exigences contractuelles et de conformité supplémentaires, notamment un addendum sur la protection des données et une [évaluation indépendante](#) (voir ci-dessous). Les fournisseurs figurant sur une liste publiée de sous-traitants ultérieurs de Microsoft seront également invités à fournir une vérification indépendante de la conformité.

Traitement de cartes de paiement

Sélectionnez cette approbation si une partie des données traitées par le fournisseur comprend des données destinées à faciliter le traitement des cartes de crédit ou d'autres cartes de paiement au nom de Microsoft.

Cette approbation permet à un fournisseur de se livrer à des activités de traitement de cartes de paiement.

Exigence de certification de conformité aux normes de sécurité de l'industrie des cartes de paiement (PCI DSS)

Le Payment Card Industry Data Security Standard (PCI DSS) est un cadre en vue de la mise en place de mesures de sécurité robustes applicables aux données des cartes de paiement qui prévoit la prévention, la détection et la réaction appropriée aux incidents de sécurité. Ce cadre a été développé par le Conseil des normes de sécurité PCI, une organisation sectorielle d'autoréglementation. L'objectif des exigences PCI DSS est d'identifier les vulnérabilités de la technologie et des processus qui présentent des risques pour la sécurité des données des titulaires des cartes qui sont traitées.

Microsoft est tenu de respecter ces normes. Si un fournisseur gère les informations de carte de paiement au nom de Microsoft, nous exigeons une preuve de respect de ces normes. Consultez le [Conseil des normes de sécurité PCI](#) pour comprendre les exigences définies par l'organisation PCI.

Selon le volume de transactions traitées, un fournisseur devra soit faire certifier la conformité par un évaluateur de sécurité qualifié, soit remplir un questionnaire [d'auto-évaluation](#).

Les marques de cartes de paiement définissent les seuils pour le type d'évaluation, généralement :

- Niveau 1 : fourniture d'un certificat d'attestation de conformité d'évaluateur PCI tiers
- Niveau 2 ou 3 : fourniture d'un questionnaire d'auto-évaluation PCI DSS (SAQ) signé par l'agent du fournisseur.

Présenter la certification applicable qui répond aux exigences PCI. Les fournisseurs qui traitent ou stockent les données de paiement des clients de Microsoft doivent posséder une certification PCI Tier 1 à jour en tant que fournisseur de services.

Logiciel à la demande (SaaS)

Le logiciel à la demande (SaaS) permet aux utilisateurs de se connecter et d'utiliser des applications basées sur le cloud via Internet. À des fins de conformité au SSPA, on entend SaaS au sens large pour inclure également la plateforme à la demande (PaaS) et l'infrastructure à la demande (IaaS). (Pour en savoir plus sur le SaaS, veuillez consulter cette [explication](#).)

Microsoft définit le **logiciel à la demande (SaaS)** comme un logiciel basé sur un code commun utilisé dans un modèle à origine unique et destinations multiples, et sur une base de paiement à l'utilisation ou comme un abonnement basé sur des mesures de l'utilisation. Le fournisseur de services cloud développe et gère des logiciels basés sur le cloud, fournit des mises à jour logicielles automatiques et met des logiciels à la disposition de ses clients via Internet sur une base à origine unique et destinations multiples, avec paiement à l'utilisation. Cette méthode de livraison de logiciels et de licences permet d'accéder aux logiciels en ligne via un abonnement au lieu de les acheter et de les installer sur chaque ordinateur individuel.

Remarque : la plupart des fournisseurs SaaS devront ajouter l'approbation du sous-traitant dans le portail dédié à la conformité des fournisseurs Microsoft si les données à caractère personnel ou confidentielles Microsoft sont hébergées sur une plateforme tierce ou chez un fournisseur d'infrastructure cloud.

Les fournisseurs qui répondent à la définition SaaS qui figure dans le profil de traitement des données peuvent être tenus de fournir une certification ISO 27001 valable si cela est requis dans le contrat de services Microsoft Cloud. Veuillez ne pas soumettre de certification de centre de données. Nous entendons que l'on nous présente la certification ISO 27001 qui s'applique au(x) service(s) logiciel(s) indiqué(s) dans votre contrat avec Microsoft.

Utilisation de sous-traitants ultérieurs

Sélectionnez cette approbation si le fournisseur a recours à des sous-traitants pour offrir les prestations (voir le DPR pour les définitions). « **Sous-traitant** » désigne un tiers auquel le

fournisseur délègue ses obligations dans le cadre du contrat couvrant ses prestations, y compris un fournisseur affilié qui n'est pas en relation directe avec Microsoft.

Cela inclut également les consultants (voir le DPR).

Microsoft considère le recours à des sous-traitants ultérieurs comme un facteur à haut risque. Les fournisseurs qui utilisent des sous-traitants ultérieurs qui traiteront des données personnelles et/ou confidentielles de Microsoft doivent les divulguer. En outre, le fournisseur doit également divulguer les pays dans lesquels ces données personnelles seront traitées par chaque sous-traitant ultérieur.

Hébergement de sites Web

Sélectionnez cette option de profil si le fournisseur héberge des sites Web, fournit des portails Web, des services en ligne et/ou des applications mobiles pour le compte de Microsoft.

« Hébergement de sites Web » désigne un service d'hébergement de sites Web en ligne qui crée et/ou entretient des sites Web pour le compte de Microsoft sous le domaine Microsoft, c.-à-d. que le fournisseur fournit tous les équipements et services nécessaires pour créer et entretenir un site et le rendre accessible sur Internet. Le « fournisseur de services d'hébergement Web » ou « hébergeur Web » est le fournisseur qui pourvoit les outils et services nécessaires pour que le site ou la page Web soit visualisé(e) sur Internet, tels que les cookies ou les balises Web pour la publicité.

Soins de santé

Sélectionnez cette option de profil si le fournisseur est tenu de traiter des informations médicales protégées (voir le DPR pour la définition).

« **Informations médicales protégées** » ou « **IMP** » désigne les données à caractère personnel de Microsoft qui sont protégées par la loi HIPAA (Health Information Portability and Accountability Act).

Systèmes d'intelligence artificielle (IA)

Sélectionnez cette option de profil si le fournisseur fournit à Microsoft des services impliquant des systèmes d'IA, notamment l'utilisation d'outils, de systèmes ou de plateformes dotés d'une technologie d'IA destinés à former et construire des systèmes intelligents afin de créer un contenu entièrement nouveau, tel que des images, des sons, des vidéos, des idées, des analyses et/ou du texte.

L'approbation des systèmes d'IA du SSPA inclura une documentation sur le traitement des données personnelles et/ou confidentielles de Microsoft, les répercussions sur les personnes, les organisations et la société, et l'acceptation des certifications appropriées des fournisseurs. Le

fournisseur doit remplir la partie sur l'IA responsable des exigences de Microsoft en matière de protection des données des fournisseurs et signer les accords requis et/ou effectuer les vérifications internes de Microsoft avant que l'achat ne puisse être effectué. Tous les fournisseurs de systèmes d'intelligence artificielle devront fournir des options d'assurance indépendante. La norme ISO 42001 peut être proposée pour valider la conformité à la section K du DPR et est **requis** pour tous les cas sensibles en matière d'IA. Pour les fournisseurs faisant l'objet d'une évaluation indépendante au titre de la section K du DPR, l'évaluation indépendante doit être réalisée par un évaluateur privilégié (liste disponible [ici](#)).

Cette approbation ne sera accordée que si l'évaluation indépendante est acceptée par le SSPA.

Vue d'ensemble du processus SSPA

Qu'est-ce que le SSPA ?

Chez Microsoft, nous pensons que le respect de la vie privée est un droit fondamental. Notre mission est de donner à chaque personne et chaque organisation de la planète la possibilité d'accomplir plus de choses, et nous nous efforçons de gagner et de conserver chaque jour la confiance de nos clients.

Des pratiques solides en matière de confidentialité et de sécurité sont essentielles à notre mission, essentielles à la confiance des clients. Il s'agit parfois même d'une obligation légale. Les normes de respect de la vie privée et de sécurité adoptées par Microsoft témoignent de nos valeurs en tant qu'entreprise et s'appliquent également à nos fournisseurs qui traitent les données Microsoft en notre nom.

Les termes clés du SSPA sont définis dans le [DPR](#). Pour en savoir plus sur le programme, lisez notre rubrique [Questions](#) (FAQ) et communiquez avec notre équipe internationale en écrivant à SSPAHelp@microsoft.com.

Le DPR est une obligation annuelle. Les activités de conformité permettent de déterminer le statut SSPA Vert (conforme) ou Rouge (non conforme). Les outils d'achat de Microsoft valident que le statut SSPA est vert (pour chaque fournisseur concerné par le SSPA) avant d'autoriser toute transaction.

Diagramme du processus SSPA – Inscription des nouveaux fournisseurs

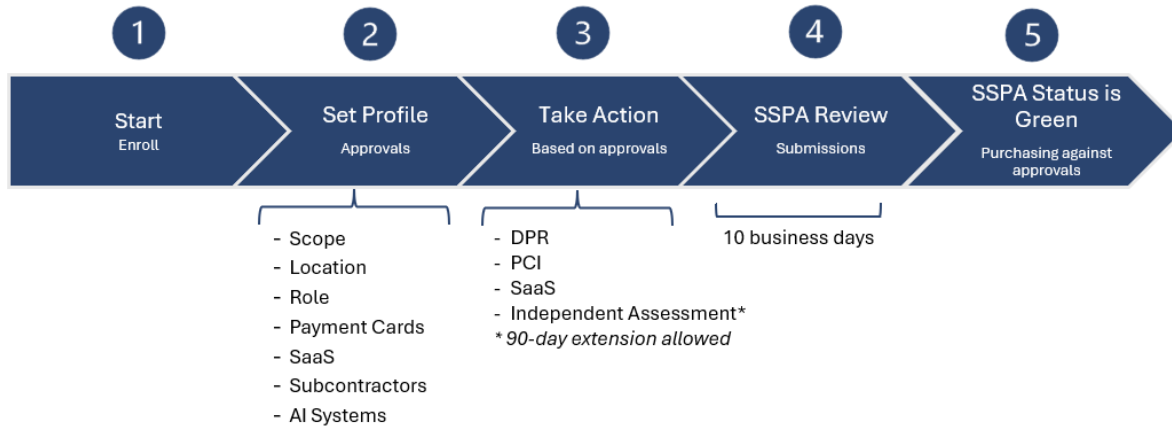
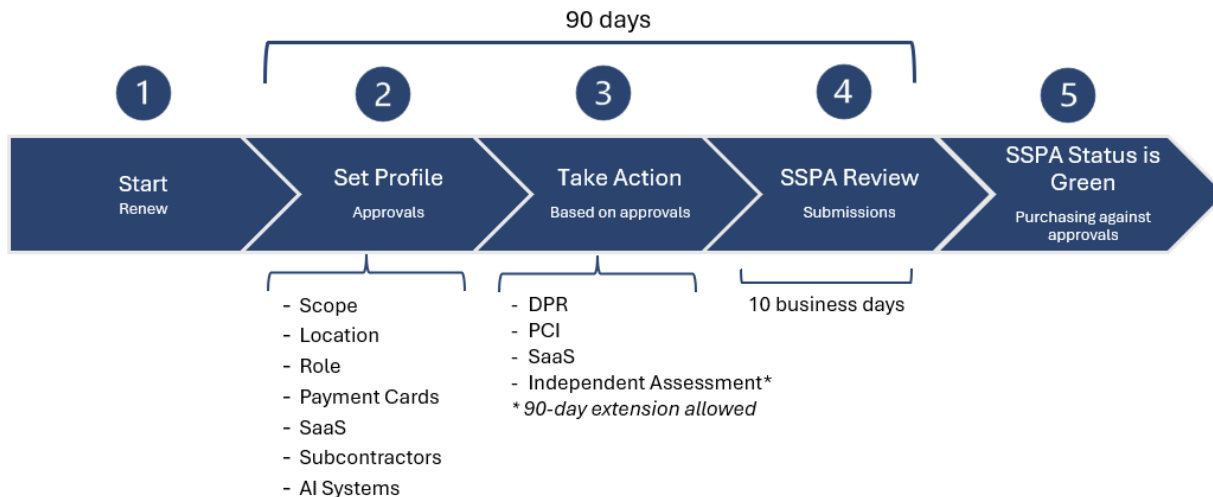


Diagramme du processus SSPA – Reconduction annuelle du fournisseur



Exigence en matière d'assurance

Les approbations sélectionnées dans votre profil de traitement des données aident l'équipe SSPA à évaluer le niveau de risque de votre travail pour Microsoft. Les exigences de conformité SSPA diffèrent en fonction du profil de traitement des données et des approbations associées.

Auto-Attestation de conformité au DPR

Tous les fournisseurs inscrits au SSPA doivent remplir une auto-attestation de conformité au DPR dans les 90 jours suivant la réception de la demande. Cette demande sera fournie sur une base annuelle, mais peut être plus fréquente si le profil de traitement des données est mis à jour en milieu d'année. Les comptes fournisseurs passeront au statut SSPA Rouge (non conforme) à l'expiration de la période de 90 jours sans réponse. Les nouveaux bons de commande dans le champ d'application ne pourront pas être traités tant que le statut SSPA ne sera pas passé au vert (conforme).

Les fournisseurs nouvellement inscrits doivent satisfaire aux exigences émises pour obtenir un statut SSPA vert (conforme) avant que les missions puissent commencer.

Important : L'équipe SSPA n'est pas autorisée à accorder des délais supplémentaires pour cette tâche.

Les fournisseurs sont tenus de répondre à toutes les exigences DPR applicables imposées, conformément au profil de traitement des données. Il est prévisible que quelques exigences puissent ne pas s'appliquer aux biens ou services que le fournisseur livre à Microsoft. Ceux-ci peuvent être marqués comme « non applicable » avec un commentaire détaillé à valider par l'équipe SSPA.

Les soumissions de DPR comportant une mention « non applicable », « conflit juridique local » ou « conflit contractuel » feront l'objet d'un examen par l'équipe SSPA et d'une vérification du respect des exigences énoncées. L'équipe SSPA peut demander des éclaircissements sur un ou plusieurs choix. Les conflits juridiques et contractuels locaux ne sont acceptés que si des références à l'appui sont fournies et le conflit est résolu.

Les représentants autorisés qui remplissent l'auto-attestation doivent s'assurer qu'ils disposent de suffisamment d'informations provenant d'experts en la matière pour répondre à chaque exigence en toute confiance. De plus, en ajoutant leur nom à un formulaire SSPA, ils certifient qu'ils ont lu et compris le DPR. Un contact de sécurité distinct doit signer la section J du DPR et peut être appelé à intervenir en cas d'incident de sécurité impliquant votre entreprise. Les fournisseurs peuvent ajouter d'autres contacts à l'outil en ligne pour faciliter la réponse aux exigences.

Le représentant autorisé (voir DPR pour la définition) doit :

1. déterminer les exigences applicables.
2. indiquer une réponse à chaque exigence applicable.
3. signer et soumettre l'attestation sur le portail de conformité des fournisseurs de Microsoft.

Important : L'équipe SSPA peut demander à des collaborateurs de fournir des preuves de conformité à une exigence particulière en matière de protection des données afin d'étayer les attestations de conformité. En outre, les fournisseurs peuvent être sélectionnés pour fournir les preuves décrites dans les exigences de protection des données des fournisseurs de Microsoft en dehors du cycle de conformité annuel. Cela ne s'appliquera que pour les entreprises qui ne sont pas soumises à la tâche d'évaluation indépendante.

Exigence d'évaluation indépendante

Veillez consulter les exigences par approbation à l'annexe A pour voir les approbations de traitement de données qui donnent lieu à cette exigence.

Les fournisseurs ont la possibilité de modifier les approbations en mettant à jour leur profil de traitement des données. Toutefois, si le fournisseur a un rôle de « sous-traitant ultérieur » dans le traitement des données, il ne pourra pas modifier cette approbation et devra se soumettre à une évaluation indépendante chaque année.

Pour obtenir les approbations qui nécessitent une vérification indépendante de la conformité, les fournisseurs doivent sélectionner un évaluateur indépendant chargé de valider la conformité au DPR. L'évaluateur doit préparer une lettre d'avis certifiant la conformité à l'intention de Microsoft. Cette lettre doit être sans réserve et il doit avoir été remédiée à tous les défauts de conformité avant que la lettre de confirmation ne soit soumise sur le portail de conformité des fournisseurs Microsoft pour examen par l'équipe SSPA. **Les évaluateurs peuvent télécharger un modèle de lettre d'avis approuvé, qui est joint au PDF « Évaluateurs préférentiels » disponible [ici](#).**

Le [tableau des profils de traitement des données du SSPA](#) présente des alternatives de certification acceptables si vous choisissez de ne pas faire appel à un évaluateur indépendant pour vérifier la conformité au DPR (le cas échéant, comme pour les fournisseurs SaaS, les fournisseurs d'hébergement de sites Web ou les fournisseurs avec des sous-traitants ultérieurs). Les normes ISO 27701 (confidentialité) et ISO 42001 (sécurité) sont considérées comme correspondant étroitement au DPR.

Si le fournisseur est une entité couverte ou un prestataire de services de santé aux États-Unis, nous acceptons un rapport HITRUST pour la protection de la confidentialité et de la sécurité.

Si des circonstances dépassant les déclencheurs standard justifient une diligence raisonnable supplémentaire, l'équipe SSPA peut exiger une évaluation indépendante, quel que soit le profil de traitement des données. Il peut s'agir par exemple d'une demande des services confidentialité ou sécurité de la division, de la validation de la résolution des incidents de données, ou de l'exigence de respect des droits des personnes concernées par le traitement automatisé des données.

Conseils pour l'approche de cette exigence :

1. L'examen doit être effectué par un évaluateur ayant une formation technique et une connaissance du sujet suffisantes pour évaluer de manière adéquate la conformité.
2. Les évaluateurs doivent être affiliés à la Fédération internationale des comptables ([IFAC](#)) ou à l'American Institute of Certified Public Accountants ([AICPA](#)) ; un auditeur ISO certifié, qualifié pour les normes ISO 27001, ISO 27701 et ISO 42001, le cas échéant ; ou doivent posséder des certifications d'autres organisations compétentes en matière de confidentialité et de sécurité, telles que l'International Association of Privacy Professionals ([IAPP](#)) ou l'Information Systems Audit and Control Association ([ISACA](#)).

3. L'évaluateur doit utiliser le DPR le plus récent dans lequel figurent les preuves requises pour appuyer chaque exigence. **Les fournisseurs devront fournir à l'évaluateur leurs réponses d'attestation DPR les plus récemment approuvées.**
4. La portée de l'évaluation est limitée à toutes les activités de traitement de données dans le champ d'application exécutées sur le numéro de compte du fournisseur qui a reçu la demande. Si le fournisseur choisit plus d'un compte fournisseur à la fois, **la lettre d'attestation devra comporter la liste des comptes fournisseurs inclus dans l'évaluation et les adresses associées.**
5. La lettre soumise à l'équipe SSPA ne doit comprendre aucune déclaration indiquant que le fournisseur ne peut pas respecter les exigences de protection des données telles qu'elles sont écrites. Ces problèmes doivent être corrigés avant que la lettre ne soit présentée.

Le SSPA a [mis à disposition](#) une liste d'évaluateurs préférentiels. Ces entreprises sont habituées à conduire des évaluations SSPA. Les fournisseurs doivent payer pour cette évaluation ; les coûts varient en fonction de l'ampleur et du champ d'application du traitement des données.

Profils nécessitant une assurance indépendante supplémentaire :

Logiciel à la demande (SaaS)

Les fournisseurs qui répondent à la définition SaaS qui figure dans le profil de traitement des données peuvent être tenus de fournir une certification ISO 27001 valable si cela est requis dans le contrat de services Microsoft Cloud. Veuillez ne pas soumettre de certification de centre de données. Nous entendons que l'on nous présente la certification ISO 27001 qui s'applique au(x) service(s) logiciel(s) indiqué(s) dans votre contrat avec Microsoft.

Les examinateurs de l'équipe SSPA valideront que votre soumission est conforme à l'obligation contractuelle.

Systemes d'IA

Si la prestation de services comprend un [usage sensible](#), une certification ISO 42001 sera exigée. De plus, la norme ISO 42001 peut être proposée pour la section K de la tâche d'évaluation indépendante.

Incidents relatifs aux données

Si un fournisseur a connaissance d'un incident lié à la confidentialité ou à la sécurité des données, il devra en informer Microsoft comme le prévoit et le précise le DPR.

Signalez un incident relatif aux données à l'aide de [SupplierWeb](#) ou envoyez un e-mail à SupplR@microsoft.com.

Veillez à bien indiquer :

- La date de l'incident de données
- Le nom du fournisseur

- Le numéro du fournisseur
- Les interlocuteurs notifiés chez Microsoft
- L'ordre d'achat correspondant, si applicable/disponible
- Un résumé de l'incident de données.