Fournisseurs Microsoft

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

Version 9

Octobre 2023

Table des matières

Introduction

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 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.

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 SSPA sur Microsoft.com/Fournisseurs. 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.

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.

Vue d'ensemble du programme SSPA

Le SSPA est un partenariat entre les services des achats, des affaires juridiques et externes, et de la sécurité de Microsoft pour s'assurer que les fournisseurs respectent les principes de Microsoft en matière de respect de la vie privée et de la sécurité.

Le SSPA est un programme mondial qui couvre tous les fournisseurs du monde entier qui traitent des données personnelles ou des données confidentielles Microsoft en relation avec leurs prestations (par exemple des services, des licences de logiciel, des services en nuage) dans le cadre des modalités de leur contrat avec Microsoft (par exemple les conditions des ordres d'achat, les contrats-cadres) (« **Prestation** » ou « **Fourniture** »).

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). Les fournisseurs figurant sur une liste publiée de sous-traitants ultérieurs de Microsoft seront également invités à fournir une vérification indépendante de la conformité.

Important : 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

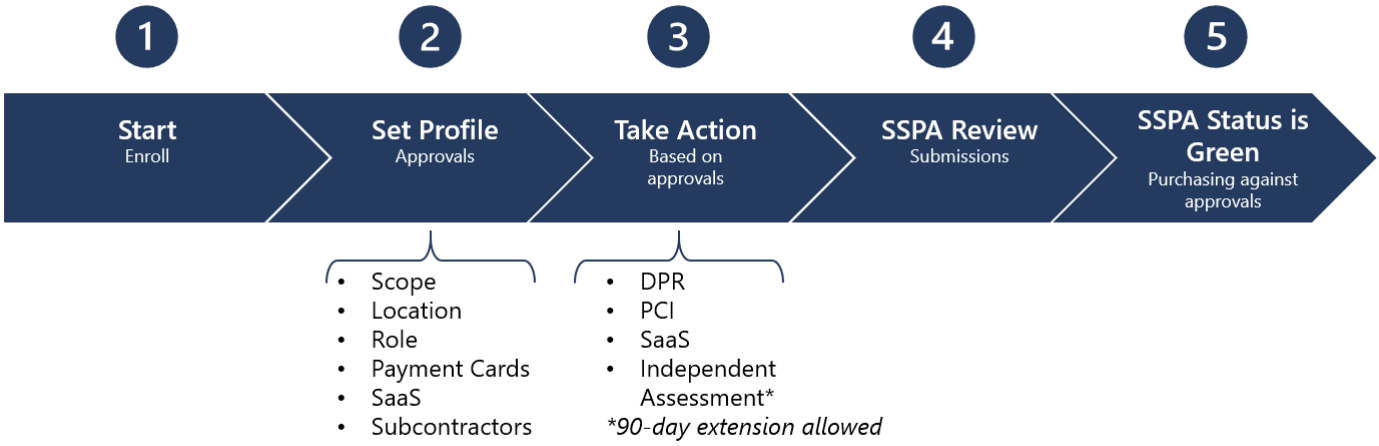
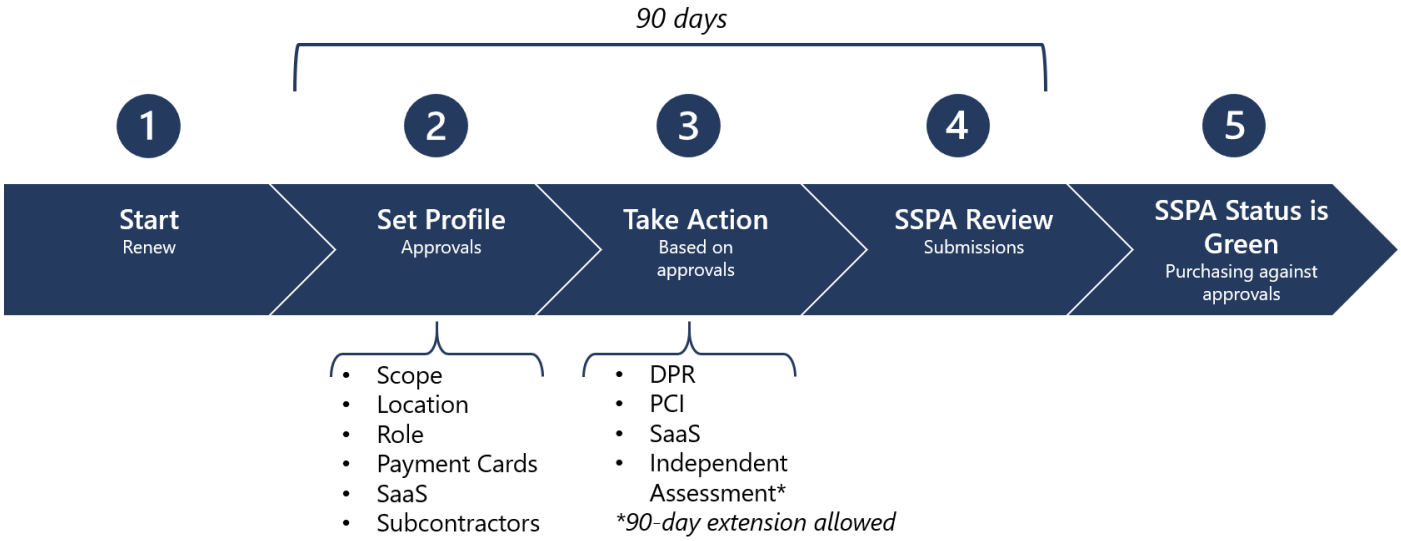


Diagramme du processus SSPA – Reconduction annuelle du fournisseur



Champ d'application du SSPA

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) • 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 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

Données confidentielles de Microsoft

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

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 Microsoft peut exiger la participation pour des données ne figurant pas sur cette liste.

Profil de traitement des données

Les fournisseurs de Microsoft contrôlent leur profil de traitement des données SSPA.

Cela permet aux fournisseurs de décider quelles opérations ils souhaitent pouvoir effectuer. Portez une attention particulière aux sélections et considérez l'activité de conformité qui doit être effectuée pour obtenir l'approbation. **Voir la section « Exigences en matière d'assurance » ci-dessous et l'annexe A.**.

Les groupes commerciaux Microsoft pourront travailler avec des fournisseurs uniquement si l'activité de traitement des données correspond aux approbations obtenues par le fournisseur.

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. Lorsqu'un changement est effectué, l'activité correspondante sera émise et devra être effectuée avant l'obtention des approbations. 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 autorisé de 90 jours, la situation au regard du SSPA passera au rouge (non conforme) et le compte risquera d'être désactivé des systèmes de comptes fournisseurs de Microsoft.

Approbations du traitement des données	
1	Champ d'application du traitement des données ▪ Confidentielles ▪ À caractère personnel, confidentielles
2	Lieu du traitement des données ▪ Chez Microsoft ou le client ▪ Chez le fournisseur
3	Rôle dans le cadre du traitement des données ▪ Contrôleur ▪ Responsable du traitement des données ▪ Sous-traitant ultérieur (désigné par Microsoft)
4	Traitement des cartes de paiement ▪ Oui ▪ Sans objet
5	Logiciel à la demande ▪ Oui ▪ Sans objet
6	Utilisation de sous-traitants ultérieurs ▪ Oui

	▪ Sans objet

Considérations relatives à l'approbation et au profil

Champ d'application du traitement des 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 à caractère personnel.

À caractère personnel, confidentielles

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

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 Contrôleur du traitement des données (voir DPR).

Si vous sélectionnez cette approbation, vous ne serez pas éligible au traitement des données à caractère personnel avec la désignation de rôle « Responsable du traitement ». 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 Responsable du traitement des données 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).

Traitement des 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.

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.

Hébergement de sites Web

Sélectionnez cette option de profil si le fournisseur héberge des sites Web pour le compte de Microsoft (voir le DPR pour la définition).

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).

Cela inclut également les Travailleurs indépendants (voir le DPR).

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).

Exigences en matière d'assurance

Exigences en fonction des approbations de profil

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. Cette section explique les différentes exigences SSPA.

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 dans le 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.

Action : Recherchez votre profil d'approbation dans l'annexe A et étudiez les exigences d'assurance correspondantes et les options d'assurance indépendante, le cas échéant.

Important : si votre profil comprend le logiciel à la demande (SaaS), des sous-traitants, un hébergement de sites Web ou des cartes de paiement, une assurance supplémentaire sera requise.

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 pourra 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 devront 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 sont uniquement acceptés si des références à l'appui sont fournies et si 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 son nom à un formulaire SSPA, cette personne certifie qu'elle a lu et compris le DPR. 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.

Remarque : 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.

Exigence d'évaluation indépendante

Veuillez 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.

L'annexe A 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 27001 (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), 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. Dans le cas d'un fournisseur nouvellement inscrit, l'évaluateur testera la conception des contrôles de processus. Dans tous les autres cas, l'évaluateur testera l'efficacité des contrôles.

5. La portée de la mission d'évaluation est limitée aux données à caractère personnel et/ou aux données confidentielles de Microsoft en rapport avec les prestations du fournisseur en question.
6. 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.**
7. 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.

L'équipe SSPA a mis à disposition une liste d'évaluateurs préférentiels. Ces entreprises sont habituées à mener 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.

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.

Exigences applicables aux logiciels à la demande

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.

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

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

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 à caractère personnel et/ou confidentielles de Microsoft doivent les déclarer. En outre, le fournisseur doit également déclarer les pays dans lesquels ces données à caractère personnel seront traitées par chaque sous-traitant ultérieur.

Incidents de 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 par le biais de SupplierWeb ou envoyez un e-mail à SuppIR@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.

Annexe A

Exigences en fonction des approbations de profil

#	Profil	Exigences en matière d'assurance	Options d'assurance indépendantes
1	**Champ d'application** : À caractère personnel, confidentielles **Lieu du traitement :** Chez Microsoft ou le client **Rôle du traitement :** Sous-traitant ou Responsable du traitement **Classe des données :** Confidentielles ou Hautement confidentielles **Cartes de paiement :** S/O **SaaS :** S/O **Utilisation de sous-traitants ultérieurs :** S/O **Hébergement de sites Web :** S/O **Soins de santé :** S/O	Auto-attestation de conformité au DPR	
2	**Champ d'application :** Confidentielles **Lieu du traitement :** Chez le fournisseur **Rôle du traitement :** S/O **Classe des données :** Confidentielles **Cartes de paiement :** S/O **SaaS :** S/O **Utilisation de sous-traitants ultérieurs :** S/O **Hébergement de sites Web :** S/O **Soins de santé :** S/O	Auto-attestation de conformité au DPR	
3	**Champ d'application** : Confidentielles **Lieu du traitement :** Chez le fournisseur **Rôle du traitement :** S/O **Classe des données :** Hautement confidentielles **Cartes de paiement :** S/O **SaaS :** S/O	Auto-attestation de conformité au DPR **et** Assurance indépendante de la conformité	Options d'assurance indépendantes : 1. Effectuer une évaluation indépendante par rapport au DPR, **ou** 2. Soumettre ISO 27001

	Utilisation de sous-traitants ultérieurs : S/O **Hébergement de sites Web :** S/O **Soins de santé :** S/O		
#	Profil	Exigences en matière d'assurance	Options d'assurance indépendantes
4	**Champ d'application :** À caractère personnel, confidentielles **Lieu du traitement :** Chez le fournisseur **Rôle du traitement :** Responsable du traitement des données **Classe des données :** Hautement confidentielles **Cartes de paiement :** S/O **SaaS :** S/O **Utilisation de sous-traitants ultérieurs :** S/O **Hébergement de sites Web :** S/O **Soins de santé :** S/O	Auto-attestation de conformité au DPR **et** Assurance indépendante de la conformité	Options d'assurance indépendantes : 1. Effectuer une évaluation indépendante par rapport au DPR, 2. Évaluation indépendante par rapport aux sections A-I du DPR et ISO 27001, **ou** 3. Soumettre ISO 27701 **et** ISO 27001
5	**Champ d'application :** À caractère personnel, confidentielles **Lieu du traitement :** Chez le fournisseur **Rôle du traitement :** Responsable du traitement des données **Classe des données :** Confidentielles **Cartes de paiement :** S/O **SaaS :** S/O **Utilisation de sous-traitants ultérieurs :** S/O **Hébergement de sites Web :** S/O **Soins de santé :** S/O	Auto-attestation de conformité au DPR	
6	**Champ d'application :** À caractère personnel, confidentielles **Lieu du traitement :** Chez le fournisseur **Rôle du traitement :** Contrôleur **Classe des données :** Hautement confidentielles ou Confidentielles **Cartes de paiement :** S/O	Auto-attestation de conformité au DPR	

	SaaS : S/O **Utilisation de sous-traitants ultérieurs :** S/O **Hébergement de sites Web :** S/O **Soins de santé :** S/O		

#	Profil	Exigences en matière d'assurance	Options d'assurance indépendantes
7	**Champ d'application :** À caractère personnel, confidentielles **Lieu du traitement :** N'importe lequel **Rôle du traitement :** Sous-traitant ultérieur (ce rôle est déterminé par Microsoft – le profil indiquera « Approbation de sous-traitant ultérieur : Oui ») **Classe des données :** Hautement confidentielles ou Confidentielles **Cartes de paiement :** S/O **SaaS :** S/O **Utilisation de sous-traitants ultérieurs :** S/O **Hébergement de sites Web :** S/O **Soins de santé :** S/O	Auto-attestation de conformité au DPR **et** Assurance indépendante de la conformité	Options d'assurance indépendantes : 1. Effectuer une évaluation indépendante par rapport au DPR, 2. Évaluation indépendante par rapport aux sections A-I du DPR et ISO 27001, **ou** 3. Soumettre ISO 27701 **et** ISO 27001
Impact de l'ajout de SaaS, sous-traitants ultérieurs, hébergement de sites Web, Soins de santé			
8	**Champ d'application :** À caractère personnel, confidentielles **Lieu du traitement :** Chez le fournisseur **Rôle du traitement :** Responsable du traitement des données **Classe des données :** Hautement confidentielles ou Confidentielles **Cartes de paiement :** S/O **Sous-traitants ultérieurs :** OUI ou **SaaS :** OUI ou **Hébergement de sites Web :** OUI ou **Soins de santé :** OUI	Auto-attestation de conformité au DPR **et** Assurance indépendante de la conformité	Options d'assurance indépendantes : 1. Effectuer une évaluation indépendante par rapport au DPR, 2. Évaluation indépendante par rapport aux sections A-I du DPR et ISO 27001, **ou** 3. Soumettre ISO 27701 **et** ISO 27001 **ou** 4. Rapport HITRUST (**uniquement** pour une entité couverte ou un prestataire de

			services de santé aux États-Unis)

#	Profil	Exigences en matière d'assurance	Options d'assurance indépendantes
9	**Champ d'application :** À caractère personnel, confidentielles **Lieu du traitement :** Chez le fournisseur **Rôle du traitement :** Contrôleur **Classe des données :** Hautement confidentielles ou Confidentielles **Cartes de paiement :** S/O **Sous-traitants ultérieurs :** OUI ou **SaaS :** OUI ou **Hébergement de sites Web :** OUI ou **Soins de santé :** OUI	Auto-attestation de conformité au DPR	
Assurance supplémentaire pour les cartes de paiement et SaaS			
10	Tout profil parmi ceux qui figurent ci-dessus et **cartes de paiement**	Exigences applicables ci-dessus et assurance PCI	Soumettre la certification PCI DSS
11	Tout profil parmi ceux qui figurent ci-dessus et **logiciel à la demande (SaaS)**	Exigences applicables ci-dessus **et** soumettre votre certification ISO 27001 exigée par le contrat couvrant les services fonctionnels.	Soumettre une certification ISO 27001 avec une couverture fonctionnelle des services fournis.