Microsoft Procurement

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

Version 7

Novembre 2020

Présentation

Chez Microsoft, nous croyons que la confidentialité est un droit fondamental. Dans notre mission d'aider les individus et les organisations du monde entier à obtenir de meilleurs résultats, nous œuvrons chaque jour pour gagner et conserver la confiance de nos clients.

De solides pratiques en matière de confidentialité et de sécurité sont essentielles pour remplir notre mission et renforcer la confiance des clients, mais elles sont aussi imposées par la loi dans plusieurs juridictions. Les dispositions figurant dans les politiques de confidentialité et de sécurité de Microsoft reflètent nos valeurs d'entreprise et s'étendent à nos fournisseurs (comme votre entreprise) qui traitent les données de Microsoft en notre nom.

Le programme d'assurance de sécurité et de confidentialité des fournisseurs Microsoft (« **SSPA** ») a été mis en place par Microsoft pour communiquer à nos fournisseurs les instructions de traitement de nos données de référence, sous la forme des Exigences en matière de protection des données destinées aux fournisseurs de Microsoft (« **EPD** ») disponibles dans la rubrique SSPA sur Microsoft.com/Procurement. Remarque : les fournisseurs devront peut-être respecter des exigences supplémentaires au niveau organisationnel, qui sont déterminées et communiquées en dehors du programme SSPA, par le groupe Microsoft responsable des relations avec le fournisseur.

Les principaux termes SSPA sont définis dans les EPD. Pour en savoir plus sur le programme, lisez nos Forums Aux Questions (FAQ) et contactez notre équipe mondiale en écrivant à l'adresse : SSPAHelp@microsoft.com.

Vue d'ensemble du programme SSPA

Le programme SSPA est un partenariat entre Microsoft Procurement, le département Corporate External and Legal Affairs et le département Corporate Security pour s'assurer que les principes de confidentialité et de sécurité sont suivis par nos fournisseurs.

Sa portée couvre tout fournisseur dans le monde qui traite des Données personnelles ou confidentielles de Microsoft en lien avec la prestation dudit fournisseur (p. ex., la fourniture de services, les licences logicielles ou les services cloud) en vertu du contrat qu'il a signé avec Microsoft (p. ex., bons de commande, contrat cadre) (ci-après la « **Prestation** »).

Le SSPA permet au fournisseur d'effectuer des sélections de profils de traitement de données qui correspondent aux biens et/ou services pour lesquels vous avez signé un contrat de Prestation. Ces sélections déclenchent les exigences correspondantes pour fournir des garanties de conformité à Microsoft.

Tous les fournisseurs inscrits devront remplir chaque année une auto-attestation de conformité aux EPD. Votre profil de traitement des données détermine si les EPD entières sont établies ou si un sous-ensemble d'exigences s'applique. Les fournisseurs qui traitent des données considérées par Microsoft comme présentant un risque plus élevé peuvent également devoir répondre à des exigences supplémentaires, comme fournir une vérification de la conformité indépendante.

Important : les interactions avec l'activité de vérification de la conformité déterminent le statut SSPA vert (conforme) ou rouge (non conforme). Les outils d'achat de Microsoft vérifient que le statut SSPA est vert (pour chaque fournisseur concerné par le SSPA) avant de permettre la poursuite d'un engagement.

Diagramme de processus SSPA – Inscription de nouveau fournisseur

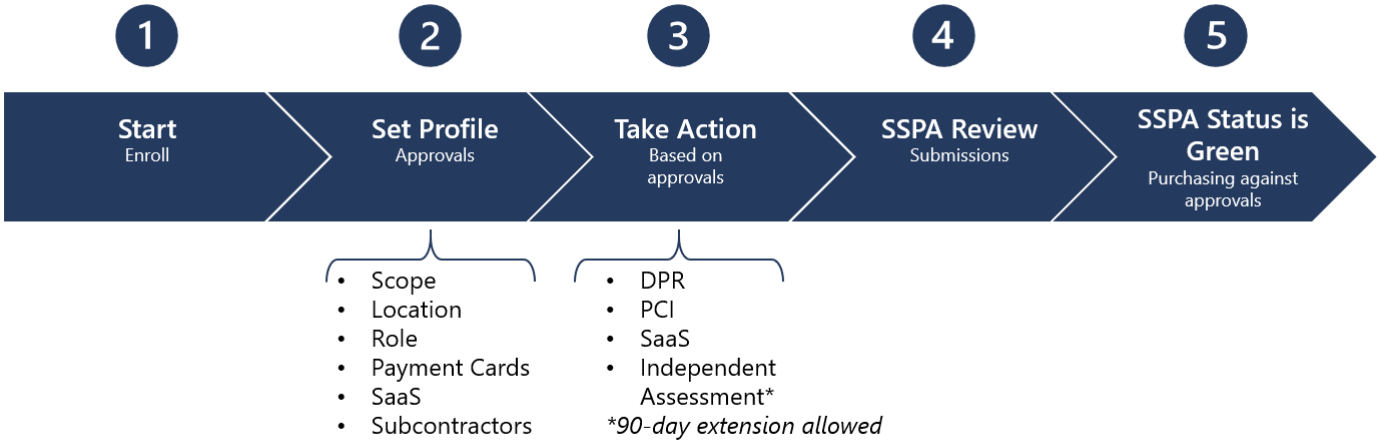
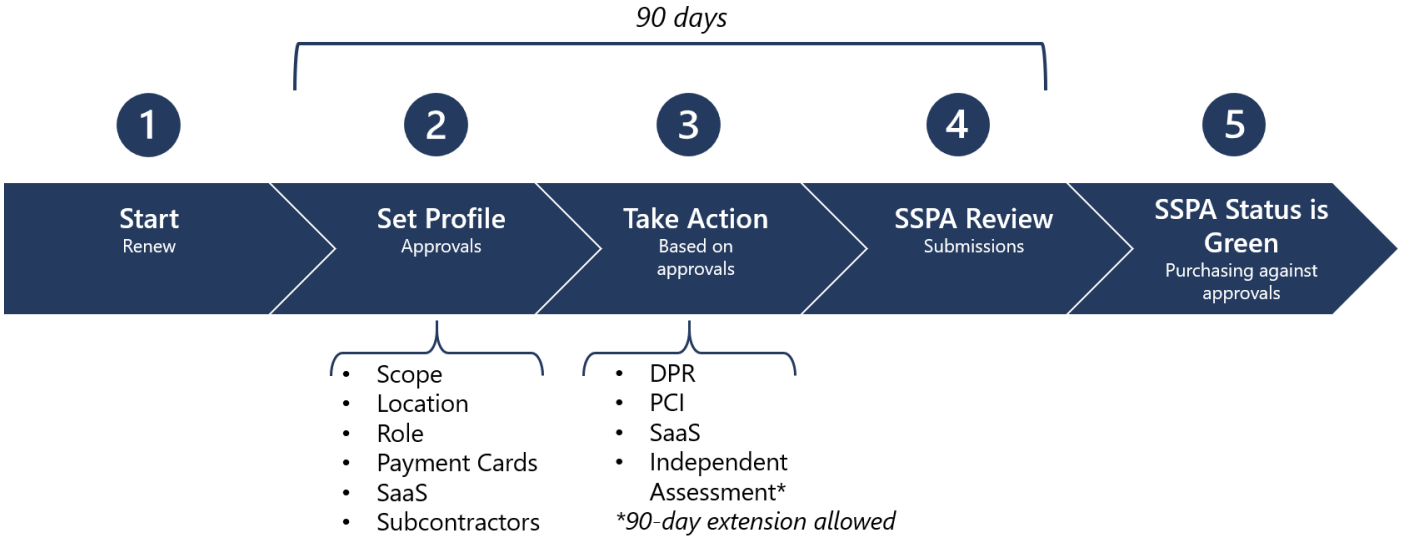


Diagramme de processus SSPA – Renouvellement annuel de fournisseur



Portée du programme SSPA

Pour vous aider à déterminer si vous (le fournisseur) traitez des Données personnelles et/ou confidentielles de Microsoft, consultez la liste d'exemples dans les tableaux ci-dessous. Notez qu'il ne s'agit que d'exemples et non d'une liste exhaustive.
Remarque : un chef d'entreprise Microsoft peut demander une inscription hors de cette liste s'il a des préoccupations quant à la nature confidentielle des données traitées.

Données personnelles par type

Exemples (non exhaustifs)

Données sensibles
Données relatives aux mineurs
Données génétiques, biométriques ou relatives à la santé
Origine raciale ou ethnique
Croyances, opinions et affiliations politiques, religieuses ou philosophiques
Adhésion à un syndicat
Vie sexuelle ou orientation sexuelle d'une personne physique
Statut d'immigration (visa, permis de travail, etc.)
Documents d'identité gouvernementaux (passeport, permis de conduire, visa, numéro de sécurité sociale, numéro d'identité nationale)
Données de localisation précises de l'utilisateur (à moins de 300 mètres)
Données de contenu de clients
Documents, photos, vidéos, musiques, etc.
Revues et/ou évaluations d'un produit ou service
Réponses à des enquêtes
Historique de navigation, intérêts et favoris.
Documents écrits, dactylographiés et vocaux (voix/audio et/ou chat/robot)
Données d'identification (mots de passe, indices des mots de passe, nom d'utilisateur, données biométriques utilisées pour l'identification)
Données de client associées avec un dossier de support

Données récoltées et générées
Données d'emplacement imprécises
Adresse IP
Préférences et personnalisation de l'appareil
Utilisation de service pour les sites Web, suivi des clics sur les pages Web
Données des réseaux sociaux, relations de graphe social
Données d'activité des appareils connectés, comme les moniteurs d'activité physique
Données de contact (comme le nom, l'adresse, le numéro de téléphone, l'adresse e-mail, la date de naissance, contacts dépendants et d'urgence)
Évaluation des fraudes et des risques, vérification des antécédents
Informations sur les assurances, la retraite et les prestations
Curriculum vitae de candidats, remarques/feedback d'entretiens
Données de compte
Données des moyens de paiement
Numéro de carte de crédit et date d'expiration
Numéro d'acheminement bancaire
Numéro de compte bancaire
Demandes de crédit ou ligne de crédit
Documents et identifiants fiscaux
Données relatives aux investissements ou aux dépenses
Cartes d'entreprise
Informations pseudonymisées de l'utilisateur final (EUPI) (Identificateurs créés par Microsoft pour identifier des utilisateurs de produits et de services Microsoft)
Identificateur global unique (GUID)
Identificateur de passeport de l'utilisateur ou identificateur unique (PUID)
Informations d'identification d'un utilisateur final hachées (EUII)
ID de session
ID d'appareil
Données de diagnostic
Données de journal

Données confidentielles de Microsoft par classe

Exemples (non exhaustifs)

Données hautement confidentielles
Informations relatives ou liées au développement, aux tests ou à la fabrication de produits Microsoft ou de composants de ces produits *Logiciels, services en ligne, services ou matériel Microsoft vendus dans le commerce, quel que soit le canal utilisé (le « **Produit Microsoft** »)*
Informations marketing de la version préliminaire d'appareils Microsoft
Données financières internes de Microsoft non annoncées assujetties aux règles de la SEC
Données confidentielles
Clés de licence des produits Microsoft au nom de Microsoft pour la distribution via n'importe quel canal
Informations relatives ou liées au développement ou aux tests d'applications métier (LOB) internes de Microsoft
Ressources marketing des versions préliminaires de Microsoft pour des logiciels et des services de la société, comme Office, SQL, Azure, etc.
Documents écrits, de conception, électroniques ou imprimés relatifs aux services ou produits Microsoft, comme des appareils (guides de procédures ou processus, données de configuration, etc.)

Important : un chef d'entreprise Microsoft peut étendre la portée du programme à des données non incluses dans cette liste.

Profil de traitement des données

Les fournisseurs de Microsoft ont un contrôle total sur leur profil de traitement des données SSPA.

Cela leur permet de décider des engagements de Prestations pour lesquels ils souhaitent être éligibles. Soyez particulièrement attentifs aux sélections et tenez compte de l'activité de conformité qui doit être effectuée pour obtenir l'approbation. **Reportez-vous à la section « Exigences en matière d'assurance » ci-dessous et à l'Annexe A**.

Les groupes d'entreprises Microsoft ne pourront créer des engagements qu'avec des fournisseurs chez lesquels 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 **si aucune tâche n'est en cours**. Lorsqu'une modification est apportée, l'activité correspondante est émise et doit être terminée avant de pouvoir obtenir les approbations. Les approbations existantes et terminées s'appliqueront jusqu'à ce que les nouvelles exigences émises soient complétées.

Si les tâches nouvellement exécutées ne sont pas terminées dans le délai de 90 jours autorisé, le statut SSPA devient ROUGE, et le compte risque d'être désactivé des systèmes des comptes fournisseurs de Microsoft.

Avertissement : si vous commencez une mise à jour de profil avant le renouvellement annuel, mais que vous décidez de ne pas apporter de modifications, le système continue d'exécuter les exigences correspondantes qui doivent être à nouveau remplies.

Approbations de traitement des données	
1	Portée du traitement des données ▪ Données confidentielles ▪ Données personnelles et confidentielles
2	Emplacement du traitement des données ▪ Chez Microsoft ou chez le client ▪ Chez le fournisseur
3	Rôle de traitement des données ▪ Contrôleur (indépendant ou commun) ▪ Entité traitant les informations (entité traitant les informations ou sous-traitant ultérieur)
4	Traitement de cartes de paiement ▪ Oui ▪ S. O.
5	Logiciel en tant que service ▪ Oui ▪ S. O.
6	Recours à des sous-traitants ▪ Oui ▪ S. O.

Considérations relatives à l'approbation

Portée du traitement des données

Données confidentielles

Sélectionnez cette approbation si la Prestation du fournisseur implique le Traitement de Données confidentielles de Microsoft. Consultez les définitions dans les EPD.

Si vous sélectionnez cette approbation, vous ne serez pas éligible pour des engagements de traitement de Données personnelles.

Données personnelles et confidentielles

Sélectionnez cette approbation si la Prestation du fournisseur implique le Traitement de Données personnelles et de Données confidentielles de Microsoft. Consultez les définitions dans les EPD.

_____

Emplacement du traitement

Chez Microsoft ou chez le client

Sélectionnez cette approbation si la Prestation du fournisseur implique le Traitement, par le fournisseur, de données dans l'environnement réseau de Microsoft, dans lequel le personnel utilise des informations d'identification d'accès *@microsoft.com* ou dans l'environnement d'un client de Microsoft.

Ne sélectionnez pas cette option dans les circonstances suivantes :

- Le fournisseur gère une installation offshore désignée par Microsoft.
- Le fournisseur fournit des ressources à Microsoft, et ces ressources travaillent parfois sur le réseau Microsoft ou en dehors de celui-ci. L'emplacement du traitement pour le travail hors réseau compte comme du travail « chez le fournisseur ».

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

_____

Rôle de traitement des données

Contrôleur (recouvre les contrôleurs indépendants et communs)

Sélectionnez cette approbation si **tous** les aspects de la Prestation par le fournisseur répondent à la définition du rôle de traitement de données du Contrôleur (voir les EPD).

Si vous sélectionnez cette approbation, vous ne serez pas éligible au traitement des Données personnelles avec la désignation de rôle « Entité traitant les informations ». Si le fournisseur est une Entité traitant les informations et un Contrôleur de Microsoft, ne sélectionnez pas « Contrôleur », mais plutôt « Entité traitant les informations ».

Entité traitant les informations (recouvre les entités traitant les informations et les sous-traitants ultérieurs)

Il s'agit du rôle de traitement le plus courant lorsque les fournisseurs traitent des données au nom de Microsoft. Consultez les définitions des termes Entité traitant les informations et Sous-traitant ultérieur dans les EPD.

_____

Traitement de cartes de paiement

Sélectionnez cette approbation si les données traitées par le fournisseur incluent des données à l'appui du traitement des cartes de crédit ou autres cartes de paiement au nom de Microsoft.

Cette approbation permet à un fournisseur de se charger d'engagements de traitement de cartes de paiement.

Logiciel en tant que service

Sélectionnez cette approbation si la Prestation du fournisseur implique la fourniture d'un service à Microsoft à l'aide d'une technologie basée sur Internet, couvrant l'accès et l'utilisation de serveurs, de réseaux de stockage et de centres de données. Le fournisseur traite les données en dehors du site ou de l'environnement de Microsoft. Exemples de services cloud : logiciels en tant que service (« SaaS »), plateformes en tant que service (« PaaS ») et infrastructures en tant que service (« IaaS »).

Microsoft définit les logiciels en tant que service, ou SaaS, comme la fourniture de fonctions logicielles via un mécanisme basé sur Internet, sur un code commun, utilisé dans un modèle un à plusieurs, sur le paiement à l'utilisation ou sous forme d'abonnement basé sur des mesures d'utilisation.

Recours à des Sous-traitants

Sélectionnez cette approbation si le fournisseur fait appel à des Sous-traitants pour effectuer la Prestation. Consultez les définitions dans les EPD.

Exigences en matière d'assurance

Exigences basées sur les approbations du profil

Les approbations sélectionnées par le fournisseur dans son profil de traitement des données permettent à l'équipe SSPA d'évaluer le niveau de risque du ou des engagements de Microsoft avec le fournisseur du point de vue du traitement des données. Les exigences de conformité SSPA applicables aux fournisseurs diffèrent en fonction des approbations dans les profils des fournisseurs. Cette section explique les différentes exigences SSPA.

Certaines combinaisons peuvent élever ou réduire les exigences de conformité. Ces combinaisons sont indiquées dans l'Annexe A. Elles illustrent ce que vous pouvez vous attendre à devoir réaliser depuis le portail Microsoft Supplier Compliance lorsque vous complétez votre profil. Vous pouvez toujours valider la façon dont votre scénario s'inscrit dans ce cadre en demandant un examen par une équipe SSPA.

Action : recherchez votre profil d'approbation dans l'Annexe A et passez en revue les exigences en matière d'assurance et les options d'assurance indépendante applicables.

Important : si vous sélectionnez les options « SaaS », « Sous-traitants », « Hébergement de site Web » ou « Cartes de paiement » dans votre profil, une assurance supplémentaire est requise.

Auto-attestation de conformité aux EPD

Tous les fournisseurs inscrits au programme SSPA doivent remplir une auto-attestation de conformité aux EPD dans les 90 jours qui suivent la réception de la demande. Cette demande sera fournie sur une base annuelle, mais pourrait être plus fréquente si le profil de traitement des données est mis à jour au cours de l'année. Les comptes fournisseurs passeront au statut SSPA ROUGE (non conforme) si la période de 90 jours est dépassée. Aucun nouveau bon de commande concerné ne sera traité tant que votre statut SSPA ne sera pas VERT (conforme).

Les fournisseurs nouvellement inscrits doivent remplir les exigences, en fonction des sélections d'approbation, pour obtenir le statut SSPA vert (conforme) avant le début des engagements.

Comme mentionné, le profil de traitement des données détermine si les EPD entières sont établies ou si seul un sous-ensemble s'applique. Ces approbations peuvent être modifiées tout au long de l'année, mais chaque fois qu'une modification est apportée, les exigences associées doivent être remplies pour que la modification entre en vigueur.

Important : l'équipe SSPA n'est pas autorisée à fournir des prolongations pour cette tâche.

Les représentants autorisés qui rempliront l'auto-attestation doivent s'assurer qu'ils disposent de suffisamment d'information de la part d'experts en la matière pour répondre à chaque exigence avec confiance. En outre, en ajoutant leur nom à un formulaire SSPA, ils certifient avoir lu et compris les EPD. Les fournisseurs peuvent toujours ajouter d'autres contacts à l'outil en ligne pour les aider à remplir les exigences.

Le Représentant agréé (voir définition) doit :

1. déterminer les exigences qui s'appliquent ;
2. publier une réponse à chaque exigence applicable ;
3. signer et soumettre l'attestation sur le portail Microsoft Supplier Compliance.

Applicabilité

Les fournisseurs doivent répondre à toutes les exigences applicables des EPD établies selon le profil de traitement des données. Parmi les exigences établies, certaines ne s'appliquent pas nécessairement aux biens ou services qu'une entreprise fournit à Microsoft. Celles-ci peuvent être marquées comme « ne s'applique pas » avec un commentaire détaillé à l'intention des examinateurs SSPA qui les valideront.

Les soumissions d'EPD sont examinées par l'équipe SSPA pour toute sélection de « ne s'applique pas », « conflit juridique local » ou « conflit relatif au contrat » par rapport aux exigences émises. Les examinateurs vérifient l'activité d'engagement associée à un compte fournisseur pour valider la sélection de « ne s'applique pas ». L'équipe SSPA peut demander des éclaircissements sur une ou plusieurs sélections. Les conflits juridiques locaux et les conflits relatifs au contrat ne sont acceptés que si des références justificatives sont fournies et que le conflit est clair.

Exigence d'évaluation indépendante

Reportez-vous à la section Exigences par approbations de l'Annexe A pour consulter les approbations de traitement des données qui déclenchent cette exigence.

Les fournisseurs peuvent modifier les approbations en mettant à jour leur profil de traitement des données.

Pour obtenir les approbations qui exigent une vérification indépendante de la conformité, les fournisseurs devront choisir un évaluateur indépendant pour valider la conformité par rapport aux EPD. L'évaluateur doit préparer une lettre d'avis afin de fournir des garanties de conformité à Microsoft. Cette lettre doit être sans réserve, et tous les problèmes de non-conformité doivent être résolus et corrigés avant que la lettre de confirmation ne soit soumise au portail Microsoft Supplier Compliance Portal pour être examinée par l'équipe SSPA. Les évaluateurs peuvent nous envoyer un e-mail à l'adresse SSPAHelp@Microsoft.com pour obtenir un modèle de lettre d'avis approuvé.

L'Annexe A inclut les alternatives de certification acceptables si vous choisissez de ne pas faire appel à un évaluateur indépendant pour contrôler la conformité aux EPD (si applicable, comme pour les fournisseurs SaaS, les fournisseurs de services d'hébergement de sites Web ou les fournisseurs faisant appel à des Sous-traitants). Les normes ISO 27701 (confidentialité) et ISO 27001 (sécurité) peuvent être considérées comme fournissant un mappage étroit avec les Exigences en matière de protection des données (EPD).

Important : les rapports SOC 2 (avec couverture de sécurité) ne seront plus acceptés après **décembre 2021**.

L'équipe SSPA peut effectuer une évaluation indépendante manuellement si les circonstances au-delà des déclencheurs standard justifient une vérification diligente supplémentaire. Il peut s'agir d'une demande de la division de la protection de la vie privée ou de la sécurité, de la validation des mesures correctives en cas d'incident lié aux données ou de l'obligation d'exécuter automatiquement les droits des personnes concernées.

Conseils relatifs à cette exigence :

1. L'engagement doit être réalisé par un évaluateur disposant d'une formation technique et de connaissances suffisantes pour évaluer adéquatement la conformité.
2. Les évaluateurs doivent être affiliés à l'International Federation of Accountants (IFAC) ou à l'American Institute of Certified Public Accountants (AICPA), ou doivent disposer de certifications d'autres organismes liés à la confidentialité et à la sécurité, notamment l'International Association of Privacy Professionals (IAPP) ou l'Information Systems Audit and Control Association (ISACA).
3. L'évaluateur doit utiliser les EPD les plus récentes, ce qui inclut les preuves requises pour répondre à chaque exigence. **Les fournisseurs devront fournir les réponses de leur attestation EPD approuvée la plus récente à l'évaluateur.**

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 vérifiera l'efficacité des contrôles.
5. La portée de l'engagement d'évaluation se limite aux Données personnelles ou confidentielles de Microsoft en lien avec la Prestation dudit fournisseur.
6. La portée de l'engagement est limitée à toutes les activités de traitement de données du champ d'application effectuées par rapport au numéro de compte fournisseur qui a reçu la demande. Si le fournisseur choisit d'évaluer un certain nombre de comptes fournisseurs en même temps, la **lettre d'attestation doit inclure la liste des comptes fournisseurs compris dans l'évaluation et les adresses associées**.
7. La lettre soumise à l'équipe SSPA ne doit pas inclure de déclarations dans lesquelles le fournisseur ne peut pas satisfaire aux Exigences en matière de protection des données telles qu'elles sont rédigées. Ces problèmes doivent être corrigés avant que la lettre ne soit soumise.

L'équipe SSPA tient à disposition une liste des évaluateurs préférés. Ces entreprises sont habituées à la réalisation d'évaluations SSPA. Les fournisseurs sont tenus de payer pour cette évaluation ; les coûts varieront en fonction de l'échelle et de la portée du traitement des données.

Exigence de certification PCI DSS

La norme de sécurité des données PCI DSS (Payment Card Industry Data Security Standard) est un framework de renforcement de la sécurité pour les paiements par carte de crédit, qui comprend des mesures de prévention et de détection, ainsi que les réactions appropriées en cas d'incidents de sécurité. Ce framework a été développé par le PCI Security Standards Council, un organisme d'autoréglementation du secteur. Les exigences de la norme PCI DSS ont pour objet l'identification des vulnérabilités technologiques et des processus qui présentent des risques pour la sécurité des données des titulaires de cartes traitées.

Microsoft doit respecter ces normes. Si un fournisseur gère des informations de carte de paiement au nom de Microsoft, nous exigeons une preuve de son adhésion à ces normes. Reportez-vous au site PCI Security Standards Council pour comprendre les exigences définies par l'organisme PCI.

En fonction du volume de transactions traité, un fournisseur devra demander à un évaluateur de la sécurité qualifié de certifier la conformité ou pourra compléter un formulaire d'auto-évaluation.

Les marques de carte de paiement déterminent les seuils du type d'évaluation, généralement :

- Niveau 1 : fournir un certificat PCI DSS d'un évaluateur tiers
- Niveau 2 ou 3 : fournir un questionnaire d'auto-évaluation PCI DSS signé par un employé du fournisseur.

Le programme SSPA accepte les deux types d'évaluation. Soumettez la certification applicable, qui répond aux exigences PCI.

Exigence SaaS

Les fournisseurs qui fournissent des logiciels en tant que service à Microsoft doivent présenter une certification ISO 27001 valide assurant la couverture fonctionnelle du service logiciel géré par eux.

Remarque : l'équipe SSPA n'attend pas de certification tierce des centres de données comme par le passé. Nous exigeons la certification ISO 27001 du ou des services logiciels fournis à Microsoft et indiqués dans votre contrat avec Microsoft.

Recours à des Sous-traitants

Microsoft considère le recours à la sous-traitance comme un facteur de risque élevé.

Les EPD exigent que les fournisseurs préviennent Microsoft lorsqu'ils font appel à des tiers pour traiter des données du champ d'application. Cela peut se faire par l'intermédiaire du programme SSPA.

Incidents liés aux données

Si un fournisseur a connaissance d'un incident lié à la confidentialité ou à la sécurité des données, il doit avertir Microsoft conformément aux instructions des EPD. Voir la définition applicable dans l'Annexe B.

Envoyez un e-mail à l'adresse SSPAHelp@microsoft.com à l'aide du modèle suivant : Signaler un incident lié aux données. Veillez à inclure les éléments suivants :

- Date de l'incident lié aux données :
- Nom du fournisseur :
- Numéro du fournisseur :
- Contact(s) Microsoft informé(s) :
- PO associé, si applicable/disponible :
- Résumé de l'incident lié aux données :

Annexe A

Exigences basées sur les approbations du profil

N°	Profil	Exigences en matière d'assurance	Options d'assurance indépendante
1	**Portée** : Données personnelles et confidentielles **Emplacement du traitement :** Chez Microsoft ou chez le client **Rôle de traitement :** Entité traitant les informations ou Contrôleur **Classe des données :** Confidentielles **ou** Hautement confidentielles **Cartes de paiement :** S. O. **SaaS :** S. O. **Recours à des Sous-traitants :** S. O. **Hébergement de sites Web :** S. O.	Auto-attestation de conformité aux EPD	
2	**Portée :** Données confidentielles **Emplacement du traitement :** Chez le Fournisseur **Rôle de traitement :** Entité traitant les informations **Classe des données :** Confidentielles **Cartes de paiement :** S. O. **SaaS :** S. O. **Recours à des Sous-traitants :** S. O. **Hébergement de sites Web :** S. O.	Auto-attestation de conformité aux EPD	

N°	Profil	Exigences en matière d'assurance	Options d'assurance indépendante
3	**Portée** : Données confidentielles **Emplacement du traitement :** Chez le Fournisseur **Rôle de traitement :** Entité traitant les informations **Classe des données :** Hautement confidentielles **Cartes de paiement :** S. O. **SaaS :** S. O. **Recours à des Sous-traitants :** S. O. **Hébergement de sites Web :** S. O.	Auto-attestation de conformité aux EPD **et** Assurance de conformité indépendante	Options d'assurance indépendante : 1. Réaliser une évaluation indépendante par rapport aux EPD, **ou** 2. Soumettre la certification ISO 27001, **ou** 3. Soumettre la certification SOC 2 avec les Security Trust Criteria (cette option sera retirée en décembre 2021)
4	**Portée :** Données personnelles et confidentielles **Emplacement du traitement :** Chez le Fournisseur **Rôle de traitement :** Entité traitant les informations **Classe des données :** Hautement confidentielles **Cartes de paiement :** S. O. **SaaS :** S. O. **Recours à des Sous-traitants :** S. O. **Hébergement de sites Web :** S. O.	Auto-attestation de conformité aux EPD **et** Assurance de conformité indépendante	Options d'assurance indépendante : 1. Réaliser une évaluation indépendante par rapport aux EPD, **ou** 2. Soumettre les certifications ISO 27701 **et** ISO 27001

N°	Profil	Exigences en matière d'assurance	Options d'assurance indépendante
5	**Portée :** Données personnelles et confidentielles **Emplacement du traitement :** Chez le Fournisseur **Rôle de traitement :** Entité traitant les informations **Classe des données :** Confidentielles **Cartes de paiement :** S. O. **SaaS :** S. O. **Recours à des Sous-traitants :** S. O. **Hébergement de sites Web :** S. O.	Auto-attestation de conformité aux EPD	
6	**Portée :** Données personnelles et confidentielles **Emplacement du traitement :** Chez le Fournisseur **Rôle de traitement :** Contrôleur **Classe des données :** Hautement confidentielles ou confidentielles **Cartes de paiement :** S. O. **SaaS :** S. O. **Recours à des Sous-traitants :** S. O. **Hébergement de sites Web :** S. O.	Auto-attestation de conformité aux EPD	

N°	Profil	Exigences en matière d'assurance	Options d'assurance indépendante
Impact de l'ajout des options « SaaS », « Sous-traitants » « Hébergement de site Web »			
7	**Portée :** Données personnelles et confidentielles **Emplacement du traitement :** Chez le Fournisseur **Rôle de traitement :** Entité traitant les informations **Classe des données :** Hautement confidentielles ou confidentielles **Cartes de paiement :** S. O. **Sous-traitants :** OUI ou **SaaS :** OUI ou **Hébergement de site Web :** OUI	Auto-attestation de conformité aux EPD **et** Assurance de conformité indépendante	Options d'assurance indépendante : 1. Réaliser une évaluation indépendante par rapport aux EPD, **ou** 2. Soumettre les certifications ISO 27701 **et** ISO 27001
8	**Portée :** Données personnelles et confidentielles **Emplacement du traitement :** Chez le Fournisseur **Rôle de traitement :** Contrôleur **Classe des données :** Hautement confidentielles **ou** confidentielles **Cartes de paiement :** S. O. **Sous-traitants :** OUI ou **SaaS :** OUI ou **Hébergement de site Web :** OUI	Auto-attestation de conformité aux EPD	

N°	Profil	Exigences en matière d'assurance	Options d'assurance indépendante
Assurance supplémentaire pour les options Cartes de paiement et SaaS			
9	L'un des profils ci-dessus et l'option **Cartes de paiement**	Les exigences ci-dessus qui s'appliquent **et** l'assurance PCI	Soumettre la certification PCI DSS
10	L'un des profils ci-dessus et l'option **SaaS**	Les exigences ci-dessus qui s'appliquent **et** soumettre votre certification ISO 27001 contractuellement requise, qui couvre les services fonctionnels.	Soumettre une certification ISO 27001 avec couverture fonctionnelle des services fournis.