Exigences en matière de protection des données applicables aux fournisseurs de Microsoft

Applicabilité

Les exigences en matière de protection des données des fournisseurs de Microsoft (« **EPD** ») s'appliquent à tout fournisseur de Microsoft qui traite des Données personnelles ou confidentielles de Microsoft en lien avec la prestation dudit fournisseur (p. ex., la prestation de services, les licences de logiciel ou les services cloud) en vertu des dispositions de son contrat avec Microsoft (p. ex., conditions des bons de commande, contrat-cadre) (ci-après la « **Prestation** »).

- En cas de conflit entre les exigences EPD et celles spécifiées dans les accords contractuels passés entre le fournisseur et Microsoft, ce sont les EPD qui prévaudront, sauf si le fournisseur concerné identifie la disposition correcte du contrat qui supplante l'exigence applicable en matière de protection des données (auquel cas, ce sont les termes du contrat qui prévaudront).
- En cas de conflit entre les exigences stipulées dans le présent document et toute exigence légale ou statutaire, cette dernière prévaudra.
- Si le fournisseur de Microsoft fait office de Responsable du traitement des données, les exigences EPD applicables à ce fournisseur peuvent être réduites.
- Si le fournisseur de Microsoft ne traite pas de Données personnelles de Microsoft, mais uniquement des Données confidentielles de Microsoft, les exigences dudit fournisseur eu égard à cet EPD peuvent être réduites.

Transfert international de données

Sans limitation de ses autres obligations, le fournisseur n'effectuera aucun transfert international de Données personnelles de Microsoft en l'absence d'accord écrit préalable de Microsoft, et quoi qu'il en soit, le fournisseur doit respecter les Exigences en matière de protection des données, notamment les Clauses contractuelles type, ou à la discrétion de Microsoft, d'autres mécanismes de transfert transfrontaliers approuvés par une autorité appropriée chargée de la protection des données ou par la Commission européenne, le cas échéant, et adoptés ou acceptés par Microsoft. Les Clauses contractuelles type ultérieures adoptées par (i) la Commission européenne ou adoptées par le Contrôleur européen de la protection des données (CEPD) et approuvées par la Commission européenne, (ii) le Royaume-Uni en vertu de la loi UK General Federal Data Protection Act, (iii) la Suisse en vertu de la loi fédérale suisse sur la protection des données, ou (iv) les clauses régissant le transfert international de données adoptées officiellement par un gouvernement dans un territoire de compétence autre que la Suisse, le Royaume-Uni, et les juridictions constituant l'Union européenne / l'Espace économique européen, doivent être intégrées et lient le Fournisseur à compter du jour de leur adoption. Le Fournisseur doit également s'assurer que tous les sous-traitants éventuels (tels que définis dans les Clauses contractuelles types) les respectent également.

Principales définitions

Les termes ci-après sont utilisés dans les présentes EPD et sont définis comme suit. Les termes « y compris », « comme », « p. ex. », « par exemple », ou termes similaires utilisés dans les présentes EPD incluent implicitement les tournures « sans limitation » ou « mais sans s'y limiter », sauf s'ils s'accompagnent des termes « uniquement » ou « exclusivement ». Des définitions supplémentaires peuvent être consultées dans le glossaire à la fin de ce document.

Le « **Responsable du traitement »** est tout organisme qui détermine les finalités et les moyens du Traitement des Données personnelles. Le « Responsable du traitement » peut être une Entreprise, un Responsable du traitement des données (tel que ce terme est défini dans le RGPD), et les termes équivalents figurant dans les Lois sur la protection des données, conformément aux exigences du contexte.

Les « **Cookies** » sont de petits fichiers de texte conservés sur les appareils par les sites Web et / ou les applications qui contiennent des informations servant à reconnaître une Personne concernée ou un appareil.

La « **Violation des données** » est (1) une atteinte à la sécurité qui entraîne accidentellement ou illicitement l'accès à ou la destruction, la perte, l'altération, la divulgation non autorisée de Données personnelles ou confidentielles Microsoft transmises, stockées ou traitées par le Fournisseur ou ses Sous-traitants, ou (2) une vulnérabilité en matière de sécurité liée au traitement de Données personnelles de Microsoft ou de Données confidentielles de Microsoft par le Fournisseur.

Une « **Personne concernée** » désigne une personne physique identifiable susceptible d'être identifiée, directement ou indirectement, en particulier en se référant à des données d'identification comme un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs facteurs propres à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de ladite personne physique.

Les « **Droits des Personnes concernées** » sont les droits d'une Personne concernée à accéder aux Données personnelles de Microsoft de ladite Personne concernée, de les supprimer, les modifier, les exporter, ainsi que de limiter leur traitement et de s'y opposer, en cas d'exigence légale.

La « **Loi** » constitue l'ensemble des lois, règles, statuts, décrets, décisions, ordonnances, réglementations, jugements, codes, promulgations, résolutions et exigences applicables de tout organisme gouvernemental (fédéral, étatique, local ou international) compétent. L'adjectif « **illicite** » fait référence à toute violation de la Loi.

Les « **Données confidentielles de Microsoft** » sont toutes les informations qui, lorsque leur confidentialité ou intégrité est compromise, peuvent nuire gravement à la réputation de Microsoft ou entraîner une perte financière significative pour Microsoft. Il s'agit entre autres des produits matériels et logiciels de Microsoft, des applications cœur de métier internes, des supports marketing préalables au lancement, des clés de licence des produits, ainsi que des documents techniques liés aux produits et services de Microsoft.

Les « **Données personnelles de Microsoft** » sont toutes les données personnelles traitées par ou au nom de Microsoft.

Les « **Données personnelles** » sont toutes les informations relatives à une Personne concernée et toutes les autres informations constituant des « données personnelles » ou des « informations personnelles » au regard de la loi.

Le « **Traitement** » désigne toute opération ou série d'opérations (automatisée ou manuelle) réalisée sur des Données personnelles ou confidentielles de Microsoft, comme la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou l'altération, la récupération, la consultation, l'utilisation, la divulgation par transmission, dissémination ou autre, l'alignement ou la combinaison, la restriction, la suppression ou la destruction. Les termes « traiter » et « traité(e)(s) » auront des significations correspondantes.

Une « **Entité traitant les informations** » est une personne physique ou juridique qui traite des Données personnelles au nom d'une autre entité. Il peut s'agir d'un Prestataire de services, d'un Sous-traitant (tel que ce terme est défini dans le RGPD), et des termes équivalents dans le domaine de la législation sur la protection des données, selon les exigences du contexte.

Le « **Sous-traitant** » désigne une tierce partie à qui un fournisseur délègue ses obligations dans le cadre du contrat couvrant sa Prestation, y compris un fournisseur affilié ne traitant pas directement avec Microsoft.

Le « **Sous-traitant ultérieur** » désigne une tierce partie que Microsoft engage pour une réaliser une prestation, lorsque

cette Prestation inclut le Traitement de Données personnelles de Microsoft dont Microsoft est un Responsable du traitement des données.

Réponse du fournisseur

Les fournisseurs confirment chaque année le respect des présentes exigences à l'aide d'un service en ligne administré par Microsoft. Veuillez consulter le Guide du programme SSPA pour comprendre les modalités d'administration de la conformité.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section A : Gestion	
1	Tout contrat applicable entre Microsoft et le fournisseur (p. ex., contrat-cadre, cahier des charges, bons de commande et autres commandes) spécifie les conditions en matière de protection des données confidentielles et sécurisées s'agissant des Données personnelles et confidentielles de Microsoft, le cas échéant, notamment l'interdiction de la vente des Données personnelles de Microsoft et du Traitement des Données personnelles de Microsoft en dehors de la relation commerciale directe entre Microsoft et le fournisseur. Pour les entreprises qui traitent les données ou les Sous-traitants intervenant dans les Prestations concernant les Données personnelles de Microsoft, le contrat doit inclure le champ d'application et la durée du Traitement, la nature et l'objectif dudit Traitement, le type de Données personnelles de Microsoft et les catégories de Personnes concernées, ainsi que les droits et obligations de Microsoft.	Le fournisseur doit présenter le contrat applicable conclu entre Microsoft et lui-même. Pour les Sous-traitants et les Sous-traitants ultérieurs, les descriptions du Traitement sont indiquées dans le contrat applicable (*p. ex.*, cahier des charges, bons de commande). Remarque : les entreprises possédant des bons de commande en cours peuvent ajouter la description nécessaire des activités de Traitement lors d'une étape ultérieure du processus d'achat.
2	Lorsque Microsoft confirme que vos engagements correspondent à un rôle de Sous-traitant ultérieur, le Fournisseur doit avoir conclu des accords de protection des données applicables avec Microsoft. Remarque : Microsoft publiera cette désignation sur votre profil en cas d'applicabilité.	Clauses contractuelles types, addendum sur les données client en ligne et/ou addendum sur le traitement des données des services professionnels des fournisseurs et partenaires.

3	Confier la responsabilité relative au respect des EPD à une personne ou un groupe désigné(e) au sein de la société.	Indiquer le rôle de la personne ou du groupe chargé(e) de garantir la conformité aux EPD applicables aux fournisseurs de Microsoft. Un document décrivant l'autorité et la responsabilité de ladite personne ou dudit groupe et démontrant un rôle en matière de confidentialité et/ou de sécurité.
4	Organiser, administrer et réaliser chaque année des formations sur la confidentialité et la sécurité destinées aux employés ayant accès aux Données personnelles traitées par le fournisseur lié à la Prestation ou aux Données confidentielles de Microsoft. Si votre société ne dispose pas de contenu préparé, vous pouvez utiliser ce modèle de document et l'adapter à votre situation. Remarque : le personnel du fournisseur peut être appelé à suivre des formations supplémentaires dispensées par des divisions de Microsoft.	Des registres de participation annuels sont disponibles et peuvent être fournis à Microsoft sur demande. Le contenu de la formation inclut les principes de la confidentialité et de la sécurité. Les documents de conformité aux exigences de formation incluront la preuve que des formations dans les domaines suivants ont été dispensées : exigences réglementaires de confidentialité, obligations de sécurité et conformité aux exigences et obligations contractuelles applicables.
#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section A : Gestion (suite)	
5	Traiter les Données personnelles de Microsoft conformément aux instructions fournies en matière de transferts de Données personnelles de Microsoft, y compris des scénarios portant sur le transfert de Données personnelles de Microsoft vers un pays tiers ou une organisation internationale, à moins d'y être contraint par la Loi ; dans ce cas, l'Entité traitant les informations ou le Sous-traitant ultérieur (fournisseur) doit signaler cette exigence légale au responsable du traitement des données (Microsoft) avant de procéder au Traitement, sauf si la Loi interdit lesdites informations pour des motifs d'intérêt public importants.	Le fournisseur compile et administre toutes les instructions de Microsoft documentées (p. ex., contrat, cahier des charges ou documents de commande) par voie électronique, dans un emplacement facilement accessible aux employés et sous-traitants du fournisseur intervenant dans la Prestation.
	Section B : Notification	

6	Le fournisseur doit utiliser la Déclaration de confidentialité de Microsoft lorsqu'il collecte des Données personnelles au nom de Microsoft. L'avis de confidentialité doit être clair et mis à la disposition des Personnes concernées pour les aider à décider si elles souhaitent confier leurs Données personnelles au fournisseur. Remarque : si votre entreprise est le Responsable de l'activité de Traitement, publiez votre propre avis de confidentialité.	Le fournisseur utilise un lien fwdlink vers la dernière Déclaration de confidentialité publiée par Microsoft. La Déclaration de confidentialité est publiée lors de la collecte des Données personnelles d'un utilisateur. Le cas échéant, une version hors connexion est disponible et est fournie avant la collecte des données. Toute Déclaration de confidentialité hors connexion utilisée constitue la dernière version publiée et est datée correctement. Pour les services aux employés Microsoft, la Notification de protection des données Microsoft est utilisée.
7	Lors de la collecte de Données personnelles de Microsoft via un appel téléphonique en direct ou enregistré, les fournisseurs doivent être préparés à parler des pratiques applicables en matière de collecte, de gestion, d'utilisation et de conservation des données avec les Personnes concernées.	Un script des enregistrements vocaux explique le Traitement des Données personnelles de Microsoft, ainsi que : ▪ leur collecte, ▪ leur utilisation et ▪ leur conservation.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section C : Choix et consentement	
8	Le cas échéant, le fournisseur doit obtenir et documenter le consentement de la Personne concernée pour toutes ses activités de Traitement des données (y compris toute activité de Traitement nouvelle et mise à jour) avant de collecter les Données personnelles à son sujet. Le fournisseur contrôle l'efficacité de la gestion des préférences pour garantir les délais de la mise en œuvre des modifications des préférences conformément aux exigences juridiques locales les plus restrictives.	Le fournisseur doit pouvoir expliquer comment une Personne concernée donne son consentement pour une activité de Traitement, et que la portée dudit consentement couvre l'ensemble des activités de Traitement du fournisseur relativement aux Données personnelles de la Personne concernée. Le fournisseur peut expliquer les modalités de retrait par une Personne concernée de son consentement à une activité de Traitement. Le fournisseur peut expliquer les modalités de vérification des préférences avant le lancement de toute nouvelle activité de Traitement. Remarque : la preuve peut prendre la forme de captures d'écran de l'interaction utilisateur, d'une expérimentation du service ou d'une possibilité de consulter la documentation technique.
9	Les fournisseurs qui créent et gèrent des sites Web et des applications de Microsoft doivent communiquer aux Personnes concernées des notifications claires sur l'utilisation des cookies et leur offrir un choix en la matière conformément aux engagements de la Déclaration de confidentialité de Microsoft et aux dispositions de la législation locale. Sauf instruction contraire spécifique de l'unité organisationnelle contractante, les fournisseurs doivent utiliser la Bannière standard produite par 1ES pour gérer les options de choix. Cette exigence s'applique lorsque les sites ciblent des utilisateurs dans l'Union européenne / l'Espace économique européen et d'autres régions dotées de lois applicables sur la confidentialité et à chaque fois que l'on utilise la Déclaration de confidentialité de Microsoft. Remarque : les entreprises commanditaires de Microsoft sont tenus d'enregistrer les sites Web de Microsoft sur le portail interne de conformité Web (http://aka.ms/wcp) pour que l'inventaire des cookies soit catalogué et géré.	L'objectif de chaque cookie doit être consigné, et le type de cookie mis en œuvre doit être précisé. ▪ Les cookies permanents ne doivent pas être utilisés si les cookies de session suffisent. ▪ Si des cookies permanents sont utilisés, leur date d'expiration doit être ultérieure à 13 mois après qu'un utilisateur a consulté le site. Validation de la conformité avec les Lois de l'UE, le cas échéant, notamment : ▪ l'utilisation de la convention de signalisation « Confidentialité et cookies » pour la déclaration de confidentialité, ▪ l'obtention du consentement affirmatif de l'utilisateur avant l'utilisation de cookies à des fins « non essentielles » (par exemple, la publicité). ▪ Le consentement doit expirer ou être redemandé au moins tous les six (6) mois.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section D : Collecte	
10	Le fournisseur doit contrôler la collecte des Données personnelles et/ou confidentielles de Microsoft afin de s'assurer que les seules données recueillies sont celles requises pour la Prestation.	Le fournisseur doit pouvoir fournir des documents qui montrent que les Données personnelles et/ou confidentielles de Microsoft recueillies sont nécessaires pour la Prestation. Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.
11	Avant de recueillir des Données personnelles auprès d'enfants (tel que défini par la juridiction applicable), le Fournisseur doit obtenir le consentement conformément aux dispositions des lois locales sur la confidentialité.	Le fournisseur peut fournir une documentation du consentement du parent / titulaire de l'autorité parentale. Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section E : Conservation	
12	S'assurer que les Données personnelles et confidentielles de Microsoft ne sont pas conservées plus longtemps que nécessaire à la prestation des services, sauf si une conservation continue des Données personnelles et/ou confidentielles de Microsoft est requise par la Loi.	Le fournisseur respecte les exigences ou politiques documentées en matière de conservation des données spécifiées par Microsoft dans le contrat (p. ex., le cahier des charges ou le bon de commande). Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.
13	S'assurer que, à l'entière discrétion de Microsoft, les Données personnelles ou confidentielles de Microsoft que le fournisseur détient ou contrôle sont restituées à Microsoft ou détruites à l'issue de la Prestation ou à la demande de Microsoft. Des processus doivent être mis en place au sein des applications pour s'assurer que les données sont bien effacées lorsqu'elles sont supprimées de l'application par l'utilisateur ou par un mécanisme basé par exemple sur leur ancienneté. Lorsque la destruction de Données personnelles ou confidentielles de Microsoft est nécessaire, le fournisseur doit brûler, pulvériser ou détruire les documents physiques contenant des Données personnelles et/ou confidentielles de Microsoft de sorte que celles-ci ne puissent pas être lues ou reconstituées.	Tenir un registre documentant la suppression des Données personnelles et confidentielles de Microsoft (il peut s'agir d'un renvoi à Microsoft pour destruction). Si une destruction est exigée ou demandée par Microsoft, le fournisseur doit fournir un certificat de destruction signé par l'un de ses agents.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section F : Personnes concernées	
	Les Personnes concernées ont certains droits en vertu de la Loi, notamment le droit d'accéder à leurs Données personnelles, de les supprimer, les modifier et les exporter, ainsi que de limiter leur Traitement et de s'y opposer (« **Droits des Personnes concernées** »). Lorsqu'une Personne concernée souhaite exercer les droits que lui confère la Loi en vigueur pour ses Données personnelles de Microsoft, le fournisseur doit autoriser Microsoft à effectuer les actions suivantes ou s'en charger au nom de Microsoft :	
14	Aider Microsoft, par les mesures techniques et organisationnelles appropriées, dans la mesure du possible, à respecter ses obligations de réponse aux demandes des Personnes concernées souhaitant exercer leurs droits sans retard injustifié. Sauf indication contraire de Microsoft, le fournisseur renvoie toutes les Personnes concernées qui le contactent directement vers Microsoft pour faire valoir leurs Droits.	Le fournisseur conserve la preuve des processus et procédures documentés pour attester du respect des droits des Personnes concernées. Le fournisseur conserve la preuve documentée des tests. La preuve doit être mise à la disposition de Microsoft sur demande.
15	Lorsqu'il répond directement à la Personne concernée ou lorsqu'il offre un mécanisme de libre-service en ligne, le fournisseur met en place des processus et des procédures pour identifier la Personne concernée à l'origine de la demande.	Le fournisseur consigne la méthode employée pour identifier les Personnes concernées de Microsoft. Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.
16	Si Microsoft lui demande de retracer des Données personnelles de Microsoft relatives à une Personne concernée qui ne sont pas disponibles via un mécanisme de libre-service en ligne, le fournisseur doit déployer les efforts raisonnables pour localiser les données demandées et conserver des enregistrements suffisants pour montrer qu'une recherche raisonnable a été effectuée.	Le fournisseur conserve la preuve écrite des procédures mises en place pour déterminer s'il détient des Données personnelles de Microsoft et fournit ladite preuve à Microsoft sur demande. Le fournisseur tient un registre expliquant les étapes suivies pour répondre aux demandes relatives aux Droits des Personnes concernées. La documentation inclut : ▪ la date et l'heure de la demande, ▪ les actions entreprises pour répondre à cette demande, et le moment où Microsoft en a eu connaissance. Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section F : Personnes concernées (suite)	
17	Le fournisseur communique à la Personne concernée les étapes à suivre afin de consulter ou faire valoir ses droits eu égard à ses Données personnelles de Microsoft.	Le fournisseur conserve la preuve écrite des communications et procédures relatives à l'accès aux Données personnelles de Microsoft. Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.
18	Consigner la date et l'heure des demandes relatives aux Droits des Personnes concernées et les opérations effectuées par le fournisseur en réponse à ces demandes. En cas de rejet de la demande et à la discrétion de Microsoft, fournir à la Personne concernée une explication écrite. Fournir les enregistrements des demandes des Personnes concernées à la demande de Microsoft.	Le fournisseur conserve les demandes d'accès / de suppression dans ses archives et consigne les modifications apportées aux Données personnelles de Microsoft. Consigner les rejets de demandes et archiver des preuves du processus d'examen et d'approbation de Microsoft. Le fournisseur doit fournir la preuve qu'il consigne les demandes et dénis d'accès aux Données personnelles de Microsoft.
19	Le fournisseur doit obtenir (ou autoriser Microsoft à obtenir) une copie des Données personnelles de Microsoft demandées et relatives à la Personne concernée authentifiée sous forme imprimée, électronique ou orale, selon le cas.	Le fournisseur transmet les Données personnelles de Microsoft à la Personne concernée dans un format compréhensible et pratique pour la Personne concernée et le fournisseur.
20	Le fournisseur doit prendre des précautions raisonnables pour s'assurer que les Données personnelles de Microsoft communiquées à Microsoft ou une Personne concernée authentifiée ne peuvent pas être utilisées pour identifier une autre personne.	Le fournisseur conserve la preuve documentée des procédures relatives aux précautions prises pour éviter l'identification de la Personne concernée contraire aux dispositions de l'Accord. Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.
21	Si une Personne concernée estime que ses Données personnelles de Microsoft ne sont pas exhaustives ni correctes, le fournisseur doit signaler le problème à Microsoft et collaborer comme il se doit avec Microsoft pour le résoudre.	Le fournisseur consigne les désaccords et en informe Microsoft. Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section G : Sous-traitants	
	Si le fournisseur souhaite recourir à un sous-traitant pour traiter les Données personnelles ou confidentielles de Microsoft, il doit :	
22	Informer Microsoft avant d'engager des services de sous-traitance ou d'apporter des modifications liées à l'ajout ou au remplacement de sous-traitants. Remarque : indiquez que vous acceptez cette obligation, même si vous n'employez pas actuellement de sous-traitants, mais si vous pourriez le faire à l'avenir.	Vérifier que les Données personnelles de Microsoft sont uniquement traitées par des sociétés connues de Microsoft, ainsi que l'exige le contrat applicable (p. ex. un cahier des charges, un addendum, un bon de commande) ou figurent dans la base de données SSPA. Le fournisseur peut publier sa liste de sous-traitants en ligne et inclure un lien vers la page de la base de données SSPA.
23	Documenter la nature et la portée des Données personnelles et confidentielles de Microsoft déléguées à des sous-traitants, en s'assurant que les informations collectées sont nécessaires à la Prestation.	Le fournisseur conserve dans ses archives une documentation relative aux Données personnelles et confidentielles de Microsoft communiquées ou transférées à des sous-traitants. Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.
24	Lorsque Microsoft est le Responsable du traitement des Données personnelles de Microsoft, s'assurer que le sous- traitant utilise lesdites Données personnelles de Microsoft conformément aux préférences de contact stipulées par la Personne concernée.	Montrer les modalités d'utilisation des préférences de la Personne concernée de Microsoft par les sous- traitants. Fournir des documents justificatifs (p. ex. capture d'écran, ANS, champ d'application des travaux, etc.) comprenant le délai imparti à un sous-traitant pour honorer une modification de préférence.
25	Limiter le traitement des Données personnelles ou confidentielles de Microsoft par le sous-traitant aux fins lui permettant de remplir ses obligations stipulées dans le contrat passé avec Microsoft.	Le fournisseur peut transmettre des documents qui montrent que les Données personnelles de Microsoft communiquées à un sous-traitant sont nécessaires pour la Prestation. Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section G : Sous-traitants (suite)	
26	Vérifier les plaintes afin d'y rechercher des indications de traitement non autorisé ou illicite des Données personnelles de Microsoft.	Le fournisseur peut prouver que des systèmes et des processus sont en place pour gérer les réclamations concernant une utilisation ou une communication non autorisée de Données personnelles de Microsoft par un sous-traitant. Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.
27	Notifier rapidement Microsoft lorsqu'il est établi qu'un sous-traitant a traité des Données personnelles ou confidentielles de Microsoft à des fins autres que celles liées à la Prestation.	Le fournisseur a fourni aux sous-traitants les instructions et les moyens nécessaires pour signaler toute utilisation abusive des données de Microsoft. Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.
28	Si le fournisseur recueille des Données personnelles auprès de tiers pour le compte de Microsoft, il doit vérifier que les politiques et pratiques de protection des données des tiers sont conformes au contrat du fournisseur avec Microsoft et aux EPD.	Le fournisseur peut fournir une documentation de la diligence raisonnable effectuée concernant les politiques et pratiques de protection des données du tiers. Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.
29	Prendre rapidement des mesures afin d'atténuer tout préjudice réel ou potentiel provoqué par le traitement non autorisé ou illicite des Données personnelles et confidentielles de Microsoft par un sous-traitant.	Le fournisseur doit conserver une preuve écrite du plan et de la procédure, et la fournir à Microsoft sur demande.
	Section H : Qualité	
30	Le fournisseur doit assurer l'intégrité de toutes les Données personnelles de Microsoft, en vérifiant qu'elles sont exactes, complètes et pertinentes aux fins de Traitement stipulées.	Le fournisseur peut prouver que des procédures sont en place pour valider les Données personnelles de Microsoft lorsqu'elles sont collectées, créées et mises à jour. Le fournisseur peut prouver que des procédures de surveillance et d'échantillonnage sont en place pour vérifier continuellement l'exactitude des informations si nécessaire. Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section I : Contrôle et application	
31	Le fournisseur dispose d'un plan de réponse aux incidents qui l'oblige à informer Microsoft conformément aux exigences contractuelles ou sans retard injustifié, selon l'option qui intervient la première, dès qu'il a connaissance d'une Violation des données. Le fournisseur doit, à la demande ou sur instruction de Microsoft, coopérer avec Microsoft à toute enquête, atténuation ou réparation de l'Incident, notamment en fournissant à Microsoft des données, des informations, un accès au personnel ou au matériel du Fournisseur nécessaire pour procéder à une expertise judiciaire. Remarque : Veuillez vous reporter au Guide du programme SSPA pour en savoir plus sur les modalités de notification d'un incident à Microsoft.	Le fournisseur dispose d'un plan de réponse aux incidents qui comprend une étape d'information des clients (Microsoft), comme décrit dans la présente section. Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.
32	Mettre en œuvre un plan d'intervention et contrôler la résolution de chaque incident de Violation des données afin de s'assurer que des mesures correctives appropriées sont prises en temps opportun.	Le fournisseur a consigné les procédures à suivre pour remédier à une Violation des données jusqu'à la résolution du problème. Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.
33	Lorsque Microsoft est un Responsable du traitement des Données personnelles de Microsoft, mettre en place un processus de réclamation officiel afin de répondre à toutes les plaintes relatives à la protection des données faisant intervenir des Données personnelles de Microsoft.	Le fournisseur dispose d'un moyen de recevoir des plaintes faisant intervenir des Données personnelles de Microsoft et d'une procédure documentée de traitement des plaintes. Le fournisseur doit fournir à Microsoft une preuve écrite sur demande.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section J : Sécurité	
	Le fournisseur doit mettre en place, mettre en œuvre et gérer un programme de sécurité des informations qui comprend des règles et des procédures destinées à la protection des Données personnelles et confidentielles de Microsoft conformément aux bonnes pratiques du secteur et à la Loi. Le programme de sécurité du fournisseur doit respecter les normes indiquées ci-dessous, exigences 34-50.	Une certification ISO 27001 ou SOC 2 valable est un substitut acceptable aux dispositions de la section J. Contacter SSPA à cet effet. Remarque : vous devez fournir la certification.
34	Réaliser des évaluations de la sécurité du réseau annuelles, notamment : ▪ examiner les principales modifications apportées à l'environnement, par exemple, nouveau composant système, modification de la topologie du réseau ou des règles du pare-feu ; ▪ réaliser des analyses de vulnérabilité ; et ▪ archiver les journaux des modifications.	Le fournisseur consigne les évaluations du réseau, les journaux des modifications et les résultats des analyses. Les journaux des modifications requis doivent suivre les modifications, fournir des informations sur le motif de la modification, et inclure le nom et le titre de l'approbateur désigné.
35	Le fournisseur doit définir, communiquer et mettre en œuvre une politique pour les appareils mobiles afin de sécuriser et de limiter l'accès aux Données personnelles ou confidentielles de Microsoft et leur utilisation sur un appareil mobile.	Le fournisseur doit prouver qu'il applique une politique de conformité pour les appareils mobiles lorsque le traitement des Données personnelles ou confidentielles de Microsoft nécessite l'utilisation d'un appareil mobile.
36	Toutes les ressources utilisées dans le cadre de la Prestation doivent être prises en compte et avoir un propriétaire identifié. Le fournisseur est responsable d'en tenir un inventaire ; d'établir une utilisation acceptable et autorisée pour ces ressources ; et de leur assurer un niveau de sécurité adéquat tout au long de leur cycle de vie.	Inventaire des ressources en appareils utilisées dans le cadre de la Prestation. L'inventaire de ces ressources doit comprendre : ▪ l'emplacement de l'appareil ; ▪ la classification des données sur la ressource ; ▪ la documentation de la récupération des ressources lors de la résiliation d'un contrat de travail ou d'un accord commercial ; et ▪ la documentation de la destruction du support de stockage des données lorsqu'elles ne sont plus nécessaires.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section J : Sécurité (suite)	
37	Établir et administrer des procédures de gestion des droits d'accès pour empêcher tout accès non autorisé aux Données personnelles ou confidentielles de Microsoft détenues par le fournisseur.	Le fournisseur prouve qu'il a mis en œuvre un plan de gestion des droits d'accès comprenant : ▪ des procédures de contrôle d'accès, ▪ des procédures d'identification, ▪ des procédures de blocage après plusieurs tentatives, ▪ des paramètres robustes pour la sélection d'informations d'authentification, ▪ la désactivation des comptes utilisateur dans les quarante-huit (48) heures qui suivent la résiliation d'un contrat de travail, ▪ des contrôles de mots de passe comportant des exigences de longueur et de complexité des mots de passe pour éviter leur réutilisation Le fournisseur prouve qu'il a établi un processus pour vérifier l'accès des utilisateurs aux Données personnelles et confidentielles de Microsoft, en appliquant le principe du privilège minimum. Ce processus doit inclure : ▪ des rôles utilisateur clairement définis, ▪ des procédures permettant de contrôler et de justifier l'approbation de l'accès aux rôles, et ▪ la confirmation du fait que les utilisateurs dont les rôles donnent accès aux données de Microsoft disposent d'un justificatif de l'exercice de ce rôle/l'appartenance à ce groupe.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section J : Sécurité (suite)	
38	Définir et mettre en œuvre des procédures de gestion des correctifs qui priorisent les correctifs de sécurité destinés aux systèmes utilisés pour traiter les Données personnelles ou confidentielles de Microsoft. Ces procédures incluent : ▪ une approche des risques définie pour donner la priorité aux correctifs de sécurité ▪ la possibilité de gérer et de mettre en œuvre des correctifs d'urgence ▪ l'applicabilité au système d'exploitation et aux logiciels serveur comme le serveur d'applications et le logiciel de base de données ▪ une documentation du risque atténué par le correctif et le suivi des exceptions, et ▪ des exigences en matière de logiciel dont la prise en charge par l'entreprise de création a pris fin.	Le fournisseur peut prouver qu'une procédure de gestion des correctifs a été mise en œuvre et répond à cette exigence en couvrant, au minimum, les éléments suivants : ▪ Une affectation de la gravité pour informer la définition de priorités. (Les définitions de gravité sont documentées.) ▪ Une procédure documentée pour mettre en œuvre des correctifs d'urgence. ▪ Une validation du fait que les systèmes d'exploitation qui ne sont plus pris en charge par l'entreprise de création ne sont plus utilisés. ▪ Des dossiers de gestion des correctifs qui suivent les approbations et les exceptions.
39	Installer des logiciels antivirus et de protection contre les programmes malveillants sur le matériel connecté au réseau utilisé pour traiter les Données personnelles et confidentielles de Microsoft, y compris sur les serveurs et les ordinateurs de production et de formation afin d'empêcher toute intrusion de virus et de programmes malveillants. Mettre à jour les définitions des programmes malveillants de manière quotidienne ou sur recommandation du fournisseur du logiciel antivirus ou de protection contre les programmes malveillants. Remarque : cette disposition s'applique à tous les systèmes d'exploitation, dont Linux.	Des dossiers prouvent l'utilisation de logiciels anti- virus et anti-malware. Remarque : cette exigence s'applique à tous les systèmes d'exploitation.
40	Les fournisseurs développant des logiciels pour Microsoft doivent intégrer des principes de sécurité dès la conception dans le processus de génération.	Les documents de spécifications techniques des fournisseurs incluent des points de contrôle pour la validation de la sécurité dans leurs cycles de développement.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section J : Sécurité (suite)	
41	Utiliser un programme de prévention des pertes de données (« **DLP** ») pour prévenir les intrusions, les pertes et autres activités non autorisées. Les données doivent être correctement classifiées, étiquetées et protégées, et le fournisseur doit surveiller les systèmes d'informations utilisés lors du traitement des Données personnelles ou confidentielles de Microsoft pour détecter les intrusions, les pertes et les activités non autorisées. Le programme DLP, au minimum : ▪ requiert l'utilisation d'un hôte standard, d'un réseau et de systèmes de détection des intrusions (« **IDS** ») cloud si vous conservez des Données personnelles ou confidentielles de Microsoft, ▪ requiert l'implémentation de systèmes avancés de protection contre les intrusions (« **IPS** ») configurés pour surveiller et empêcher activement la perte de données, ▪ en cas de violation du système, requiert l'analyse de ce dernier pour résoudre tous les problèmes de vulnérabilité restants, ▪ requiert une description des procédures de surveillance du système avec les outils de détection ; ▪ établit la mise en place d'un processus de gestion et de réponse aux incidents à suivre lorsqu'un événement de Violation des données est détecté, et ▪ exige des communications (à tous les employés du fournisseur et à tous les sous-traitants n'intervenant plus dans les Prestations du fournisseur) concernant le téléchargement et l'utilisation non autorisés des Données personnelles ou confidentielles de Microsoft.	Programme DLP documenté déployé avec des procédures en place pour prévenir les intrusions, les pertes et autres activités non autorisées (et au minimum, tous les éléments spécifiés dans cette section).
42	Communiquer rapidement à la direction et à Microsoft les résultats de l'enquête en réponse à l'incident.	Des systèmes et des processus doivent être en place pour communiquer à Microsoft les résultats de l'enquête en réponse à l'incident.
43	Les administrateurs système, le personnel des opérations, la direction et les tiers doivent suivre une formation à la sécurité annuelle.	Mettre en place un programme de formation en matière de sécurité qui comprend les éléments suivants : ▪ Formation annuelle en matière de réponse aux incidents, et ▪ Simulation d'événements et de mécanismes automatisés pour améliorer l'efficacité des réponses en cas de crise. ▪ Sensibilisation à la prévention des incidents, notamment en matière de risques associés au téléchargement de logiciels malveillants.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section J : Sécurité (suite)	
44	Le fournisseur doit s'assurer que des processus de planification de sauvegarde protègent les Données personnelles et confidentielles de Microsoft contre les utilisations, accès, divulgations, modifications et destructions non autorisés.	Le fournisseur peut prouver qu'il documente les procédures de réponse et de récupération détaillant la manière dont l'organisation gérera un événement perturbateur et assurera un certain niveau (prédéfini) de sécurité pour ses informations en fonction des objectifs de continuité de la sécurité des informations approuvés par la direction. Le fournisseur peut prouver qu'il a défini et mis en œuvre des procédures pour sauvegarder périodiquement, stocker de manière sécuritaire et récupérer efficacement les données critiques.
45	Mettre en place et tester des plans de continuité des activités et de rétablissement après catastrophe.	Un plan de rétablissement après catastrophe doit inclure les éléments suivants : ▪ Définition de critères pour déterminer si un système est critique pour les activités du fournisseur. ▪ Établissement d'une liste des systèmes critiques (en fonction des critères définis) à rétablir en priorité en cas d'urgence. ▪ Définition d'une procédure de rétablissement après catastrophe pour chaque système critique afin que les ingénieurs qui ne connaissent pas le système puissent rétablir le fonctionnement de l'application en moins de soixante-douze (72) heures. ▪ Test et examen des plans de rétablissement après catastrophe annuels (ou plus fréquents) pour s'assurer que les objectifs de rétablissement sont réalisables.
46	Authentifier l'identité d'une personne avant de lui permettre d'accéder aux Données personnelles et confidentielles de Microsoft et s'assurer que l'accès est limité au domaine d'activité de la personne en question permis dans le cadre de la Prestation.	Vérifier que tous les identifiants des utilisateurs sont uniques et qu'ils utilisent une méthode d'authentification standard du secteur comme Azure Active Directory. Un accès de haut niveau (privilèges d'administration ou autres types de privilèges avancés) nécessite un second facteur, comme un authentificateur utilisant une carte à puce ou un téléphone. Programme de sécurité des informations documenté couvrant le processus visant à s'assurer que l'accès de tous les employés et sous-traitants du fournisseur aux Données personnelles ou confidentielles de Microsoft n'est ni plus étendu ni plus prolongé que nécessaire pour intervenir sur la Prestation.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section J : Sécurité (suite)	
47	Le fournisseur doit protéger toutes les données Traitées dans le cadre de la Prestation en transit sur les réseaux au moyen d'un chiffrement reposant sur des certificats « **TLS** » (Transport Layer Security) ou « **IPsec** » (Internet Protocol Security). Ces méthodes sont décrites dans les normes NIST 800-52 et NIST 800-57 ; une norme équivalente du secteur peut également être utilisée. Le fournisseur doit refuser la remise de Données personnelles ou confidentielles de Microsoft transmises de façon non chiffrée.	Le processus de création, de déploiement et de remplacement de certificats TLS ou autres doit être défini et mis en œuvre.
48	Tous les appareils du fournisseur (ordinateurs portables, stations de travail, etc.) qui accéderont à des Données personnelles ou confidentielles de Microsoft ou les traiteront doivent utiliser le chiffrement sur disque.	Utiliser la spécification BitLocker ou une autre solution de chiffrement sur disque équivalente pour tous les appareils client utilisés dans le cadre de la gestion des Données personnelles ou confidentielles de Microsoft.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section J : Sécurité (suite)	
49	Des systèmes et des procédures (conformes aux normes actuelles du secteur comme décrit dans la norme NIST 800-111) doivent être mis en place pour chiffrer les Données personnelles et/ou confidentielles de Microsoft au repos (lorsqu'elles sont stockées), y compris les suivantes : ▪ Les données d'identification (par ex., noms d'utilisateur/mots de passe) ▪ Les données des moyens de paiement (p. ex., numéros de carte de crédit ou de compte bancaire) ▪ Les données personnelles liées à l'immigration ▪ Les données des profils médicaux (p. ex., les numéros de dossier médical ou les marqueurs et identifiants biométriques, comme l'ADN, les empreintes digitales, les rétines et iris, les empreintes vocales, la structure des visages, les mesures de la main, utilisés à des fins d'authentification) ▪ Les données d'identification émises par le gouvernement (p. ex., numéros de sécurité sociale ou de permis de conduire) ▪ Les données appartenant aux clients de Microsoft (p. ex., SharePoint, documents Office 365, clients OneDrive) ▪ La documentation liée aux produits de Microsoft non annoncés ▪ La date de naissance ▪ Les informations de profil des enfants ▪ Les données géographiques en temps réel ▪ L'adresse physique personnelle (non professionnelle) ▪ Les numéros de téléphone personnels (non professionnels) ▪ La religion ▪ Les opinions politiques ▪ L'orientation/la préférence sexuelle ▪ Les réponses aux questions de sécurité (p. ex., authentification à deux facteurs, réinitialisation du mot de passe) ▪ Le nom de jeune fille de la mère	Vérifier que les Données personnelles et confidentielles de Microsoft sont chiffrées au repos.

#	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité
	Section J : Sécurité (suite)	

50	Rendre anonymes toutes les Données personnelles de Microsoft utilisées dans un environnement de développement ou de test.	Les Données personnelles de Microsoft ne doivent pas être utilisées dans des environnements de développement ou de test ; en l'absence d'autres solutions, elles doivent être suffisamment anonymes pour empêcher l'identification des Personnes concernées ou toute utilisation malintentionnée. Remarque : les données anonymisées sont différentes des données pseudonymisées. Les données anonymisées sont des données qui ne concernent pas une personne physique identifiée ou identifiable lorsque la personne concernée par les données à caractère personnel n'est pas ou plus identifiable.

Glossaire

Un « **Représentant autorisé** » est une personne qui a le niveau d'autorité approprié pour signer au nom de la société. Cette personne aurait les connaissances requises en matière de confidentialité et de sécurité ou aurait consulté un expert en la matière avant de soumettre sa réponse à une action du programme SSPA. Également, en ajoutant son nom à un formulaire SSPA, elle certifie avoir lu et compris les EPD.

L'« **EUDPR** » désigne le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE.

« **Travailleur indépendant** » désigne les personnes effectuant des tâches ou des services à la demande qui sont acquis via des plateformes numériques ou d'autres moyens.

Le « **RGPD** » désigne le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Les « **Exigences en matière de protection des données confidentielles** » désignent le RGPD, l'EUDPR, les législations locales de l'UE/EEE sur la protection des données, la loi californienne sur la protection de la vie privée des consommateurs, Cal. Civ. Code § 1798.100 ss (la « *CCPA* »), la loi britannique sur la protection des données de 2018 et toutes les lois, réglementations et autres exigences juridiques connexes ou ultérieures applicables au Royaume-Uni, et toutes les lois, réglementations et autres exigences juridiques applicables relatives (a) à la vie privée et à la sécurité des données ; ou (b) à l'utilisation, la collecte, la conservation, le stockage, la sécurité, la divulgation, le transfert, l'élimination et tout autre traitement de toutes les Données personnelles.

Les **« Clauses type de l'UE** » et les « **Clauses contractuelles type** » sont (i) les clauses contractuelles type en matière de protection des données pour le transfert de Données personnelles à un Sous-traitant établi dans un pays tiers qui ne garantit pas un niveau adéquat de protection des données, telles qu'elles figurent dans l'Article 46 du RGPD et sont approuvées par la décision 2021/914 (UE) de la Commission européenne du 4 juin 2021 ; (ii) toute clause contractuelle type de remplacement adoptée par (a) la Commission européenne, (b) le Contrôleur européen de la protection des données et approuvée par la Commission européenne, (c) le Royaume-Uni conformément à la loi fédérale britannique sur la protection des données, (d) la Suisse conformément à la loi fédérale suisse sur la protection des données, ou (e) par un gouvernement d'une juridiction autre que la Suisse, le Royaume-Uni et les juridictions comprenant l'Union européenne / l'Espace économique européen où les clauses régissent le transfert international de données personnelles, et seront incorporées et

exécutoires pour le Fournisseur à compter du jour de leur adoption.

« **Hébergement de site Web** » Un service d'hébergement de site Web est un service en ligne qui crée et/ou gère des sites Web pour le compte de Microsoft sous le domaine Microsoft, c'est-à-dire que le fournisseur fournit tous les matériaux et services nécessaires pour créer et gérer un site et le rend accessible sur l'Internet. Le « prestataire de services d'hébergement Web » ou « hébergeur Web » est le fournisseur qui fournit les outils et les services nécessaires à la consultation du site Web ou de la page Web sur Internet, tels que des cookies ou des balises Web à des fins publicitaires.