Exigences de Microsoft en matière de protection des données des fournisseurs

Applicabilité

Les exigences de Microsoft en matière de protection des données des fournisseurs (« **DPR** ») s'appliquent à chaque fournisseur de Microsoft qui traite des données à caractère personnel ou des données confidentielles Microsoft en relation avec les prestations de ce fournisseur (p. ex. 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** », « **Performance** » ou « **Fourniture** »).

- En cas de conflit entre le DPR et les exigences stipulées dans les accords contractuels entre le fournisseur et Microsoft, le DPR prévaudra, à moins que le fournisseur n'identifie la disposition correcte du contrat qui remplace l'exigence applicable en matière de protection des données (dans ce cas, les termes du contrat prévaudront).
- En cas de conflit entre les exigences contenues dans le présent document et toute exigence légale ou réglementaire, les exigences légales ou réglementaires prévaudront.
- Si le fournisseur de Microsoft opère en tant que contrôleur, il se peut que ses exigences en matière de DPR soient réduites.
- Si le fournisseur de Microsoft ne traite pas les données à caractère personnel de Microsoft, mais uniquement les données confidentielles de Microsoft, le fournisseur peut avoir des exigences moindres en vertu de ce DPR.
- La section K du DPR ne s'applique qu'aux fournisseurs qui proposent à Microsoft des services impliquant des systèmes d'IA.

Transfert international des données

Sans limiter ses autres obligations, le fournisseur n'effectuera aucun transfert international de données à caractère personnel de Microsoft sans l'accord écrit préalable de Microsoft et, en tout état de cause, le fournisseur se conformera aux exigences de protection des données, notamment les clauses contractuelles types, ou, à la discrétion de Microsoft, à d'autres mécanismes appropriés de transfert international approuvés par une autorité de protection des données appropriée ou par la Commission européenne,
selon le cas, et adoptés ou acceptés par Microsoft. Les clauses contractuelles types suivantes adoptées par (i) la Commission européenne ou adoptées par le Contrôleur européen de la protection des données et approuvées par la Commission européenne, (ii) le Royaume-Uni en vertu du UK General Federal Data Protection Act (Loi fédérale britannique relative à la protection des données), (iii) la Suisse en vertu du Swiss Federal Data Protection Act (fédérale suisse relative à la protection des données), ou (iv) les clauses régissant le transfert international de données à caractère personnel officiellement adoptées par un gouvernement dans une juridiction autre que la Suisse, le Royaume-Uni et les juridictions composant l'Union européenne / l'Espace économique européen, seront incorporées et contraignantes pour le fournisseur à compter de la date de leur adoption. Le fournisseur veillera également à ce que tous les sous-traitants (tels que définis dans les Clauses contractuelles types) s'y conforment également.

Définitions essentielles

Les termes suivants utilisés dans le présent DPR ont la signification suivante. La liste d'exemples qui suit « notamment », « tel que », « p. ex. », « par exemple » ou autres termes similaires utilisés dans le présent DPR est interprétée comme incluant « sans limitation » ou « mais non limité à », à moins d'être qualifiée par des termes comme « seulement » ou « uniquement ». Pour de plus amples définitions, veuillez consulter le glossaire que vous trouverez à la fin du présent document.

Le terme « **Systèmes d'IA** » signifie un système technique qui applique un modèle optimisé afin que le système puisse, pour un ensemble donné d'objectifs définis par l'humain, effectuer des prédictions*, des recommandations ou des décisions qui influencent les environnements avec lesquels il interagit. Un tel système peut fonctionner avec différents niveaux d'automatisation. *Les prédictions peuvent faire référence à divers types d'analyse ou de production de données (y compris la traduction de texte, la création d'images synthétiques ou le diagnostic d'une panne d'électricité antérieure).

« Contrôleur » désigne l'entité qui détermine les finalités et les moyens du traitement des données à caractère personnel. Le terme « Contrôleur » inclut une entreprise, un contrôleur (tel que ce terme est défini dans le RGPD) et des termes équivalents dans les lois relatives à la protection des données, selon le contexte.

Les **« Cookies »** sont de petits fichiers texte stockés sur des appareils par des sites Web et/ou des applications qui contiennent des informations utilisées pour reconnaître une personne concernée ou un appareil.

« **Incident de données** » désigne (1) une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé aux données à caractère personnel ou aux données confidentielles de Microsoft transmises, stockées ou traitées de quelconque manière par le fournisseur ou ses sous-traitants, ou (2) une faille de sécurité liée au traitement par le fournisseur des
données à caractère personnel ou des données confidentielles de Microsoft ou un incident de confidentialité tel que défini par le projet de loi 64 (2021, chapitre 25).

« **Personne concernée** » désigne une personne physique identifiable qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne physique.

« **Droit de la personne concernée** » désigne le droit de la personne concernée d'accéder, supprimer, modifier, exporter, restreindre ou s'opposer au traitement des
Les données à caractère personnel Microsoft de cette personne concernée si la loi l'exige.

« **Utilisations prévues** » sont les principales raisons pour lesquelles les clients, fournisseurs ou utilisateurs finaux sont censés utiliser le système. Il peut s'agir d'une seule utilisation ou de plusieurs dans le cas de systèmes à usages multiples.

« **Loi** » désigne l'ensemble des lois, règles, statuts, décrets, décisions, ordonnances, règlements, jugements, codes, promulgations, résolutions et exigences applicables de toute autorité gouvernementale (fédérale, d'État, locale ou internationale) compétente. « **Illégal** » désigne toute violation de la Loi.

Les « **données confidentielles de Microsoft** » concernent toutes les informations qui, si elles sont compromises par des moyens de confidentialité ou d'intégrité, peuvent entraîner une perte financière ou de réputation importante pour Microsoft. Il s'agit notamment des produits matériels et logiciels de Microsoft, des applications internes des entreprises, des documents marketing avant publication, des clés de licence de produit et des documentations techniques relatives aux produits et services de Microsoft.

Les « **données à caractère personnel de Microsoft** » désigne toutes les données à caractère personnel traitées par Microsoft ou en son nom.

Les « **données à caractère personnel** » désigne toutes informations relatives à une personne concernée et toutes autres informations qui constituent des « données à caractère personnel » ou des « informations à caractère personnel » en vertu de la Loi.

Le terme « **traitement** » désigne toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel ou des données confidentielles de Microsoft, que ce soit ou non par des moyens automatisés, tels que la

collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre forme de mise à disposition, l'alignement ou la combinaison, la restriction, l'effacement ou la destruction. Les termes « en traitement » et « traité » ont la même signification.

« **Responsable du traitement** » désigne une entité qui traite des données à caractère personnel pour le compte d'une autre entité et inclut le prestataire de services, le responsable du traitement (tel que ce terme est défini dans le RGPD) et les termes équivalents dans les lois relatives à la protection des données, en fonction du contexte.

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

Le « **Red Teaming** » est une approche au cours de laquelle un groupe de testeurs sonde intentionnellement un système pour en identifier les limites, la surface de risque et les vulnérabilités. Plus d'informations sur https://aka.ms/CustomerRedTeamingGuide.

Une « **utilisation sensible** » de l'IA désigne l'utilisation ou l'abus raisonnablement prévisibles d'un système d'IA qui pourrait affecter une personne des manières suivantes :

- Conséquence importante sur la situation juridique ou les opportunités de vie.
- Risque d'atteinte à l'intégrité physique ou psychologique.
- Menace sur les droits humains.

« **Sous-traitant** » désigne un tiers auquel le fournisseur délègue ses obligations dans le cadre du contrat couvrant ses prestations, y compris un fournisseur affilié qui n'est pas en relation directe avec Microsoft.

« **Sous-traitant ultérieur** » désigne un tiers que Microsoft engage pour la prestation, lorsque celle-ci comprend le traitement des
données à caractère personnel pour lesquelles Microsoft est responsable du traitement.

Réponse des fournisseurs

Les fournisseurs confirment chaque année leur conformité à ces exigences par le biais d'un service en ligne administré par Microsoft. Veuillez consulter le guide du programme SSPA pour comprendre la manière dont la conformité est gérée.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section A : Gestion	
1	Chaque accord applicable entre Microsoft et le fournisseur (p. ex. contrat-cadre, cahier des charges, bons de commande et autres commandes) comporte des dispositions relatives à la protection de la vie privée et de la sécurité des données en ce qui concerne les données confidentielles et les données à caractère personnel de Microsoft, selon le cas, y compris des interdictions concernant la vente de données à caractère personnel de Microsoft et le traitement des données à caractère personnel de Microsoft en marge de la relation d'affaires directe entre Microsoft et le fournisseur. Pour les entreprises opérant en tant que Responsable du traitement ou sous-traitants ultérieurs dans le cadre de la prestation, en ce qui concerne les données à caractère personnel de Microsoft, l'accord doit inclure l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel de Microsoft et les catégories de personnes concernées, ainsi que les obligations et les droits de Microsoft.	Le fournisseur doit présenter le contrat applicable entre Microsoft et le fournisseur. Pour les responsables du traitement et les sous-traitants ultérieurs, les descriptions du traitement sont contenues dans l'accord applicable (*p. ex.* le cahier des charges, les bons de commande). Si Microsoft confirme que vos engagements impliquent le traitement d'IMP, le fournisseur devra disposer d'un accord d'association commerciale et/ou d'un autre accord avec Microsoft. Remarque : Les entreprises ayant des bons de commande en cours peuvent ajouter la description nécessaire des activités de traitement à un stade ultérieur du processus d'achat.
2	Si Microsoft confirme que vos engagements remplissent un rôle de sous-traitant ultérieur, le fournisseur devra avoir mis en place des accords de protection des données avec Microsoft. Remarque : Microsoft ajoutera ces désignations à votre profil lorsqu'elles s'appliqueront.	Clauses contractuelles types, addenda relatif aux données des clients en ligne, addenda relatif au traitement des données des services professionnels des fournisseurs et partenaires et/ou accord d'association commerciale.
3	Attribuer à une personne ou à un groupe désigné dans l'entreprise la responsabilité et l'obligation de rendre compte du respect du DPR.	Nommer le rôle de la personne ou du groupe chargés de veiller au respect du DPR du fournisseur de Microsoft. Document décrivant l'autorité et la responsabilité de cette personne ou de ce groupe qui joue un rôle dans le domaine de la protection de la vie privée et/ou de la sécurité.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section A : Gestion (suite)	
4	Mettre en place, maintenir et assurer une formation annuelle à la protection de la vie privée et à la sécurité pour toutes les personnes (administrateurs système, personnel d'exploitation, direction, tiers, etc.) ayant accès aux données à caractère personnel ou confidentielles de Microsoft. Si votre entreprise n'a pas de contenu préparé, vous pouvez utiliser ce script de storyboard et l'adapter à votre entreprise. Remarque : Le personnel du fournisseur peut être tenu de suivre des formations supplémentaires dispensées par les divisions de Microsoft.	Des registres annuels de présence sont disponibles et peuvent être fournis à Microsoft sur demande. Le contenu de la formation est régulièrement mis à jour et comprend des principes de protection de la vie privée et de sécurité tels que la sensibilisation à la prévention des incidents, notamment la protection des mots de passe, la surveillance des connexions, les risques associés au téléchargement de logiciels malveillants et d'autres rappels pertinents en matière de sécurité. La documentation relative au respect des exigences en matière de formation comprendra la preuve de la formation relative aux exigences réglementaires en matière de protection de la vie privée, aux obligations en matière de sécurité et au respect des exigences et obligations contractuelles applicables. La formation à la réponse aux incidents, événements simulés et mécanismes automatisés aux fins de faciliter une réponse efficace aux situations de crise. Si les données à caractère personnel Microsoft traitées par le fournisseur comprennent des IMP, le contenu de la formation devra inclure une formation HIPAA, notamment les utilisations et divulgations autorisées par le fournisseur en vertu de l'accord d'association commerciale.
5	Appliquer des sanctions appropriées aux employés qui ne respectent pas les politiques du fournisseur en matière de protection de la vie privée et de sécurité.	Documentation des politiques en matière de protection de la vie privée et de sécurité qui décrivent les sanctions en cas de non-respect (p. ex. jusqu'au licenciement).
6	Traiter les données à caractère personnel de Microsoft uniquement conformément aux instructions documentées de Microsoft, notamment les scénarios relatifs aux transferts de données à caractère personnel de Microsoft vers un pays tiers ou une organisation internationale, sauf si la loi l'exige ; dans ce cas, le responsable du traitement ou le sous-traitant ultérieur (fournisseur) devra informer le contrôleur (Microsoft) de cette exigence légale avant le traitement, à moins que la loi n'interdise cette information pour des raisons importantes d'intérêt public.	Le fournisseur compile et conserve toutes les instructions documentées de Microsoft (p. ex. les accords, le cahier des charges ou les documents de commande) et ses politiques et procédures de confidentialité et de sécurité par voie électronique, dans un endroit facilement accessible aux employés du fournisseur et aux sous-traitants participant à la prestation.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section B : Avis	
7	Le fournisseur doit utiliser la déclaration de confidentialité de Microsoft lorsqu'il collecte des données à caractère personnel pour le compte de Microsoft. L'avis de confidentialité doit être visible et disponible pour les personnes concernées afin de les aider à décider de soumettre ou non leurs données à caractère personnel au fournisseur. Remarque : Si votre entreprise est le contrôleur de l'activité de traitement, vous devrez publier votre propre avis de confidentialité.	Le fournisseur utilise un lien fwdlink vers la déclaration de confidentialité actuelle publiée par Microsoft. La déclaration de confidentialité est publiée dans tous les contextes où les données à caractère personnel d'un utilisateur sont collectées. Le cas échéant, une version hors ligne est disponible et mise à disposition avant la collecte des données. Toute déclaration de confidentialité hors ligne utilisée est la dernière version publiée qui est correctement datée. Pour les services aux employés de Microsoft, l'avis de confidentialité des données de Microsoft est utilisé.
8	Lorsqu'ils collectent des données à caractère personnel Microsoft par le biais d'un appel vocal en direct ou enregistré, les fournisseurs doivent être prêts à discuter avec les personnes concernées des pratiques applicables en matière de collecte, de traitement, d'utilisation et de conservation des données.	Un script destiné aux enregistrements vocaux indique comment les données à caractère personnel de Microsoft sont traitées et comprend : • collecte, • utilisation, et • conservation.
	Section C : Choix et consentement	
9	Le cas échéant, le fournisseur doit obtenir et enregistrer le consentement d'une personne concernée pour toutes ses activités de traitement (y compris toute activité de traitement nouvelle ou mise à jour) avant de collecter les données à caractère personnel de cette personne. Le fournisseur contrôle l'efficacité de la gestion des préférences afin de s'assurer que le délai pour honorer un changement de préférence correspond à l'exigence légale locale la plus restrictive qui s'applique.	Le fournisseur peut démontrer la manière dont une personne concernée donne son consentement à une activité de traitement et que le consentement concerne toutes les activités de traitement du fournisseur en lien avec les données à caractère personnel de la personne concernée. Le fournisseur peut démontrer la façon dont une personne concernée retire son consentement pour une activité de traitement. Le fournisseur peut démontrer la mesure dans laquelle les préférences sont vérifiées avant le lancement d'une nouvelle activité de traitement. Remarque : Les preuves peuvent être des captures d'écran de l'interaction avec l'utilisateur, l'expérimentation du service ou la possibilité de consulter la documentation technique.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section C : Choix et consentement (suite)	
10	Les fournisseurs qui créent et gèrent des sites Web et/ou des applications Microsoft ou des sites portant la marque Microsoft doivent fournir aux personnes concernées un avis et un choix transparents concernant l'utilisation de cookies, conformément aux engagements de la déclaration de confidentialité de Microsoft et aux exigences légales locales. Sauf demande expresse de l'unité opérationnelle contractante, les fournisseurs doivent utiliser la bannière standard produite par 1ES pour gérer les contrôles des choix. Cette exigence s'applique lorsque les sites ciblent des utilisateurs de l'Union européenne ou de l'Espace économique européen et d'autres régions disposant de lois sur la protection de la vie privée et partout où la déclaration de confidentialité de Microsoft est utilisée. Remarque : Les sponsors commerciaux de Microsoft sont tenus d'enregistrer les sites Web de Microsoft dans le portail interne de conformité Web (http://aka.ms/wcp) afin que l'inventaire des cookies soit catalogué et géré.	La finalité de chaque cookie doit être documentée et doit permettre de déterminer le type de cookie utilisé. • Les cookies persistants ne doivent pas être utilisés lorsque des cookies de session suffisent. • Si des cookies persistants sont utilisés, leur date d'expiration ne doit pas dépasser 13 mois après la visite de l'utilisateur sur le site. Valider la conformité avec les lois de l'UE, le cas échéant, comme : • l'utilisation de la convention d'étiquetage « Confidentialité et cookies » pour la déclaration de confidentialité, • obtenir le consentement explicite de l'utilisateur avant d'utiliser des cookies « non essentiels » à des fins telles que la publicité, et • le consentement doit expirer ou être à nouveau obtenu au maximum tous les 6 mois.
	Section D : Collecte	
11	Le fournisseur doit contrôler la collecte des données à caractère personnel et/ou confidentielles de Microsoft afin de s'assurer que les seules données collectées sont celles nécessaires à la prestation.	Le fournisseur peut remettre une documentation démontrant que les données à caractère personnel et/ou confidentielles de Microsoft collectées sont nécessaires à la prestation. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.
12	Avant de collecter des données auprès d'enfants (tels que définis par la juridiction applicable), le fournisseur devra obtenir le consentement, conformément aux lois locales sur la protection de la vie privée.	Le fournisseur peut remettre un document attestant du consentement des parents ou des tuteurs. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.

13	Si le fournisseur reçoit de Microsoft un jeu de données dont l'identification est réduite, notamment les pseudonymes, les données non identifiantes (DNI), les pseudonymes non liés, les données agrégées, les données anonymes ou tout autre terme lié à l'une de ces classifications (tel que « dépersonnalisées »), le fournisseur devra conserver les données dans l'état dans lequel il les a reçues.	Le fournisseur ne devra pas augmenter l'identification des jeux de données (c.-à-d. qu'il ne devra pas réidentifier les individus qui font partie d'un jeu de données en les associant à d'autres jeux de données, etc.) Le fournisseur dispose d'une politique/procédure de désidentification/anonymisation des données.
#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section E : Conservation	
14	Veiller à ce que les données à caractère personnel et confidentielles de Microsoft soient conservées pendant une durée n'excédant pas celle nécessaire à la prestation, à moins que la loi n'exige de prolonger la conservation des données à caractère personnel et/ou confidentielles de Microsoft.	Le fournisseur se conforme aux politiques de conservation documentées ou aux exigences de conservation spécifiées par Microsoft dans le contrat (p. ex. le cahier des charges, le bon de commande). Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.
15	Veiller à ce que, à la seule discrétion de Microsoft, les données à caractère personnel et confidentielles de Microsoft en possession ou sous le contrôle du fournisseur soient restituées à Microsoft ou détruites à l'issue de la prestation ou à la demande de Microsoft. Dans les applications, des processus doivent être mis en place pour garantir que lorsque les données sont supprimées de l'application, soit explicitement par les utilisateurs, soit sur la base d'autres déclencheurs tels que l'âge des données, elles sont supprimées en toute sécurité. Lorsqu'il est nécessaire de détruire des données à caractère personnel ou confidentielles de Microsoft, le fournisseur doit brûler, pulvériser ou déchiqueter tout bien matériel contenant des données à caractère personnel et/ou confidentielles de Microsoft, de telle manière à ce que les informations ne puissent pas être lues ou reconstituées.	Tenir un registre de l'élimination des données personnelles et confidentielles de Microsoft (ce qui peut inclure le renvoi à Microsoft pour destruction). Si la destruction est requise ou demandée par Microsoft, fournir un certificat de destruction signé par un responsable du fournisseur.
	Section F : Personnes concernées	

	Les personnes concernées disposent de certains droits en vertu de la loi, notamment le droit d'accéder à leurs données à caractère personnel, les supprimer, les modifier, les exporter, les restreindre et de s'opposer à leur traitement (« droits des personnes concernées »). Lorsqu'une personne concernée cherche à exercer les droits que lui confère la loi en matière des données à caractère personnel de Microsoft, le fournisseur doit permettre à Microsoft de prendre les mesures suivantes ou doit les exécuter pour le compte de Microsoft :	
16	aider Microsoft, par le biais de mesures techniques et organisationnelles appropriées, dans la mesure du possible, à s'acquitter de ses obligations de répondre aux demandes des personnes concernées cherchant à exercer leurs droits sans retard injustifié. Sauf indication contraire de Microsoft, le fournisseur orientera directement vers Microsoft toutes les personnes concernées qui le contactent afin qu'elles exercent leurs droits en tant que personnes concernées.	Le fournisseur conservera les preuves des procédures et processus documentés pour soutenir l'application des droits des personnes concernées. Le fournisseur devra conserver les preuves documentées des essais. Ces preuves devront être disponibles sur demande de Microsoft.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section F : Personnes concernées (suite)	
17	Lorsqu'il répond directement à la personne concernée ou qu'il propose un mécanisme de libre-service en ligne, le fournisseur dispose de procédures et de processus établis pour identifier la personne concernée à l'origine de la demande.	Le fournisseur a documenté la méthode utilisée pour identifier les personnes concernées de Microsoft. Le fournisseur devra remettre des preuves documentées à Microsoft sur demande.

18	Si Microsoft lui demande de localiser à propos d'une personne concernée des données à caractère personnel qui ne sont pas disponibles par le biais d'un mécanisme de libre-service en ligne, le fournisseur fera un effort raisonnable pour localiser les données demandées et conservera des registres suffisants permettant de démontrer qu'une recherche raisonnable a été effectuée.	Le fournisseur devra conserver des preuves documentées des procédures mises en place pour déterminer si des données personnelles de Microsoft sont détenues et remettre la documentation à Microsoft sur demande. Le fournisseur tient un registre démontrant les mesures prises pour répondre aux demandes de la personne concernée concernant ses droits. La documentation comprend : • la date et l'heure de la demande, • les mesures prises pour répondre à la demande et la date à laquelle Microsoft a été informé. Le fournisseur devra remettre la preuve de la tenue des registres à Microsoft sur demande.
19	Le fournisseur communiquera à la personne concernée les mesures qu'elle doit prendre pour accéder à ses données à caractère personnel de Microsoft, ou pour exercer ses droits de toute autre manière.	Le fournisseur devra conserver des preuves documentées des communications et des procédures d'accès aux données personnelles de Microsoft. Le fournisseur devra conserver des preuves documentées et les remettre à Microsoft sur demande.
20	Enregistrer la date et l'heure des demandes de droits de la personne concernée et des mesures prises par le fournisseur en réponse à ces demandes. Si la demande est rejetée, fournir à la personne concernée une explication écrite sur instruction de Microsoft. Sur demande, fournir à Microsoft des relevés des demandes des personnes concernées.	Le fournisseur tient un registre des demandes d'accès/de suppression et documente les modifications apportées aux données à caractère personnel de Microsoft. Documenter les cas où les demandes sont refusées et conserver les preuves de l'examen et de l'approbation de Microsoft. Le fournisseur devra remettre la preuve de l'enregistrement des demandes et des refus d'accès aux données à caractère personnel de Microsoft.
21	Le fournisseur doit autoriser Microsoft ou obtenir une copie des données à caractère personnel de Microsoft demandées pour la personne concernée authentifiée en format imprimé, électronique ou oral approprié.	Le fournisseur fournit les données à caractère personnel de Microsoft à la personne concernée en format compréhensible et sous une forme qui convient à la personne concernée et au fournisseur.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
Section F : Personnes concernées (suite)		

22	Le fournisseur doit adopter des précautions raisonnables pour assurer que les données à caractère personnel de Microsoft communiquées à Microsoft ou à une personne concernée authentifiée ne peuvent pas être utilisées pour identifier une autre personne.	Le fournisseur conservera des preuves documentées concernant les procédures relatives aux précautions prises pour éviter l'identification de la personne concernée de façon contraire aux conditions de l'accord. Le fournisseur devra remettre des preuves à Microsoft sur demande.
23	Si une personne concernée estime que ses données à caractère personnel de Microsoft ne sont pas complètes et exactes, le fournisseur doit faire remonter le problème à Microsoft et coopérer pour résoudre le problème, le cas échéant.	Le fournisseur documente les cas de désaccord et transmet le problème à Microsoft. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.
24	En ce qui concerne les demandes d'accès des personnes concernées, le fournisseur doit tenir un registre de tous les destinataires avec lesquels il a partagé ou partagera des données à caractère personnel de Microsoft.	Le fournisseur peut fournir une liste de tous les destinataires actuels et des destinataires tiers éventuels des données à caractère personnel de Microsoft, sur demande.
Section G : Sous-traitants		
	Si le fournisseur a l'intention de faire appel à un sous-traitant pour traiter les données à caractère personnel ou confidentielles de Microsoft, il devra :	
25	Informer Microsoft avant de sous-traiter des services ou d'apporter des modifications concernant l'ajout ou le remplacement de sous-traitants. Remarque : Indiquez que vous acceptez cette obligation, même si vous n'engagez pas de sous-traitants actuellement, mais que vous pourriez le faire à l'avenir.	Valider que les données à caractère personnel et/ou confidentielles de Microsoft sont uniquement traitées par des sociétés connues de Microsoft, comme l'exige le contrat applicable (p. ex. le cahier des charges, l'addendum, le bon de commande) ou saisi 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.
26	Documenter la nature et l'étendue des données à caractère personnel et confidentielles de Microsoft sous-traitées par les sous-traitants, en veillant à ce que les informations collectées soient nécessaires à la prestation.	Le fournisseur conserve la documentation relative aux données à caractère personnel et confidentielles de Microsoft divulguées ou transférées aux sous-traitants. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section G : Sous-traitants (suite)	
27	Lorsque Microsoft est le responsable du traitement des données à caractère personnel de Microsoft, s'assurer que le sous-traitant utilise les données à caractère personnel de Microsoft conformément aux préférences de contact indiquées par la personne concernée.	Démontrer comment les sous-traitants utilisent les préférences Microsoft des personnes concernées. Fournir des documents justificatifs (p. ex. capture d'écran, accord de niveau de service, cahier des charges, etc.) indiquant le délai dans lequel un sous-traitant doit honorer un changement de préférence.
28	Limiter le traitement par le sous-traitant des données personnelles ou confidentielles de Microsoft aux fins nécessaires à l'exécution du contrat du fournisseur avec Microsoft. Si les données à caractère personnel de Microsoft sont des IMP, conclure également avec le sous-traitant un accord d'association commerciale qui limite le traitement des données à caractère personnel de Microsoft par le sous-traitant et protège la confidentialité et la sécurité des données à caractère personnel de Microsoft de la même manière que l'accord d'association commerciale conclu entre Microsoft et le fournisseur.	Le fournisseur peut remettre une documentation démontrant que les données à caractère personnel et/ou confidentielles de Microsoft fournies à un sous-traitant sont nécessaires à la prestation. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande, y compris un accord d'association commerciale, le cas échéant.
29	Examiner les réclamations afin de déceler des indices d'un traitement non autorisé ou illégal des données à caractère personnel de Microsoft.	Le fournisseur peut démontrer que des systèmes et processus sont en place pour traiter les réclamations concernant l'utilisation ou la divulgation non autorisée des données à caractère personnel de Microsoft par un sous-traitant. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.
30	Notifier Microsoft sans délai dès qu'il apprend qu'un sous-traitant a traité des données à caractère personnel ou confidentielles de Microsoft à des fins autres que celles liées à la prestation.	Le fournisseur a remis les instructions et les moyens permettant à un sous-traitant de signaler l'utilisation abusive des données de Microsoft. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.
31	Si le fournisseur collecte des données à caractère personnel auprès de tiers pour le compte de Microsoft, le fournisseur devra s'assurer que les politiques et pratiques de protection des données de ces tiers sont conformes au contrat conclu entre le fournisseur et Microsoft et au DPR.	Le fournisseur peut remettre une documentation sur la diligence raisonnable exercée en ce qui concerne les politiques et pratiques de protection des données du tiers. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.

32	Prendre rapidement des mesures aux fins d'atténuer tout préjudice réel ou potentiel causé par le traitement non autorisé ou illégal des données à caractère personnel et confidentielles de Microsoft par un sous-traitant.	Le fournisseur doit conserver les preuves documentaires du plan et de la procédure et remettre les preuves de la documentation à Microsoft sur demande.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section H : Qualité	
33	Le fournisseur doit maintenir l'intégrité de toutes les données à caractère personnel de Microsoft, en veillant à ce qu'elles demeurent exactes, complètes et pertinentes au regard des finalités déclarées pour lesquelles elles ont été traitées.	Le fournisseur peut démontrer que des procédures sont en place pour valider les données à caractère personnel de Microsoft lorsqu'elles sont collectées, créées et mises à jour. Le fournisseur peut démontrer que des procédures de suivi, d'examen des activités du système d'information et d'échantillonnage sont en place pour vérifier l'exactitude en permanence et la corriger, le cas échéant. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.
	Section I : Contrôle et application	
34	Le fournisseur dispose d'un plan d'intervention en cas d'incident qui l'oblige à informer Microsoft, conformément aux exigences contractuelles ou dans les meilleurs délais, selon ce qui se produit le plus tôt, dès qu'il a connaissance d'un incident de données. Le fournisseur doit, à la demande ou sur instruction de Microsoft, coopérer avec ce dernier dans le cadre de l'enquête, de l'atténuation ou de la remédiation à l'incident, notamment en fournissant à Microsoft les données, les informations, l'accès au personnel du fournisseur ou le matériel nécessaire à la réalisation d'un examen judiciaire. Il se peut qu'un accès au personnel ou au matériel du fournisseur soit nécessaire afin de réaliser un examen d'analyse. Remarque : Veuillez consulter le guide du programme SSPA pour savoir comment notifier un incident à Microsoft.	Le fournisseur dispose d'un plan de réponse aux incidents qui comprend une étape de notification aux clients (Microsoft), comme décrit dans cette section. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.

35	Mettre en œuvre un plan de remédiation et contrôler la résolution de chaque incident de données afin de s'assurer que les mesures correctives appropriées sont prises en temps utile.	Le fournisseur a documenté les procédures qu'il suivra pour répondre à un incident de données jusqu'à sa clôture. Cela inclut l'envoi de mises à jour ponctuelles à Microsoft jusqu'à ce que le problème soit résolu, ainsi que l'envoi d'une étude après l'incident. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.
#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section I : Contrôle et application (suite)	
36	Lorsque Microsoft est un contrôleur des données à caractère personnel de Microsoft, mettre en place une procédure de réclamation formelle pour répondre à toutes les réclamations relatives à la protection des données impliquant des données à caractère personnel de Microsoft.	Le fournisseur dispose des moyens de recevoir les réclamations concernant les données à caractère personnel de Microsoft et a mis en place une procédure de réclamation documentée pour traiter les réclamations. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.
	Section J : Sécurité	
	Le fournisseur doit établir, mettre en œuvre et maintenir un programme de sécurité des informations comprenant des politiques et procédures, afin de protéger et de maintenir en sécurité les données à caractère personnel et confidentielles de Microsoft, conformément aux bonnes pratiques de l'industrie et comme l'exige la loi. Le programme de sécurité du fournisseur doit répondre aux normes mentionnées ci-dessous, exigences 37 à 52. Si les données à caractère personnel de Microsoft sont des IMP, le fournisseur devra également procéder régulièrement à une évaluation technique et non technique en réponse aux changements environnementaux et opérationnels affectant la sécurité des IMP, et ce afin d'établir la mesure dans laquelle les politiques et procédures du fournisseur répondent aux exigences de la règle de sécurité de l'HIPAA.	Une certification ISO 27001 valide est un remplacement acceptable de la section J. Contactez le programme SSPA pour appliquer cette substitution. Sécurité. Contacter le programme SSPA afin de mettre en œuvre ce remplacement. Remarque : Vous devrez fournir la certification.

37	Effectuer des évaluations annuelles de la sécurité du réseau, notamment : • l'évaluation des risques et vulnérabilités potentiels pour la confidentialité, l'intégrité et la disponibilité des données à caractère personnel de Microsoft et la mise en œuvre de mesures visant à réduire les risques, • l'examen des changements majeurs apportés à l'environnement, tels qu'un nouveau composant du système, la topologie du réseau, les règles du pare-feu, • la tenue de registres des modifications.	Le fournisseur a documenté les évaluations du réseau, les registres des modifications et les résultats des analyses. Les registres des modifications doivent assurer le suivi des modifications, fournir des informations sur la raison de la modification et inclure le nom et le titre de l'approbateur désigné. Les registres des 90 derniers jours sont disponibles sur demande.
38	Le fournisseur doit définir, communiquer et mettre en œuvre une politique relative aux appareils mobiles qui sécurise et limite l'utilisation des données à caractère personnel ou confidentielles de Microsoft consultées ou utilisées sur un appareil mobile.	Le fournisseur démontre qu'il applique une politique conforme en matière d'appareils mobiles lorsque le traitement des données à caractère personnel ou confidentielles de Microsoft nécessite l'utilisation d'un appareil mobile.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section J : Sécurité (suite)	
39	Tous les actifs physiques et virtuels utilisés pour soutenir les prestations, la sécurité et les opérations doivent être comptabilisés et leur propriétaire doit être identifié. Le fournisseur est responsable de la tenue d'un inventaire de ces actifs d'informations, de l'établissement d'une utilisation acceptable et autorisée des actifs et de la fourniture du niveau de protection approprié pour les actifs tout au long de leur cycle de vie.	Inventaire des équipements utilisés pour soutenir les performances, la sécurité et les opérations. L'inventaire de ces actifs doit comprendre : • l'emplacement de l'appareil, • la classification des données sur l'actif, • l'enregistrement de la récupération des actifs en cas de cessation d'emploi ou d'accord commercial, et • l'enregistrement de l'élimination des supports de stockage de données lorsqu'ils ne sont plus nécessaires. • tous les dispositifs physiques et virtuels utilisés par le personnel du fournisseur avec des identifiants @microsoft.com pour accéder aux données de Microsoft doivent être entièrement gérés uniquement par Microsoft. Aucun logiciel de sécurité supplémentaire ne doit être installé au-delà de ce qui est prévu par Microsoft.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section J : Sécurité (suite)	
40	Établir et maintenir des procédures de gestion des droits d'accès afin d'empêcher tout accès non autorisé aux données à caractère personnel ou confidentielles de Microsoft sous le contrôle du fournisseur.	Le fournisseur démontre qu'il a mis en œuvre un plan de gestion des droits d'accès qui comprend : • les procédures de contrôle d'accès, • les procédures d'identification, • les procédures de verrouillage après des tentatives infructueuses, • la déconnexion automatique après inactivité • des paramètres robustes pour la sélection des informations d'authentification, et • la désactivation des comptes d'utilisateurs (notamment les comptes utilisés par les employés ou les sous-traitants) en cas d'embauche ou de cessation d'emploi dans un délai de 48 heures • des contrôles stricts des mots de passe qui imposent la longueur et la complexité des mots de passe et empêchent leur réutilisation • l'utilisation de l'authentification multifacteur (MFA) pour les identités. Le fournisseur démontre qu'il dispose d'un processus établi permettant d'examiner l'accès des utilisateurs aux données à caractère personnel et confidentielles de Microsoft, en appliquant le principe du moindre privilège. Ce processus comprend : • des rôles d'utilisateurs clairement définis, • des procédures permettant d'examiner et de justifier l'approbation de l'accès aux rôles, et • de vérifier que les utilisateurs des rôles ayant accès aux données Microsoft disposent d'une justification documentée de leur appartenance au groupe/rôle.

		• des interdictions strictes concernant les comptes ou mots de passe partagés

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section J : Sécurité (suite)	
41	Définir et mettre en œuvre des procédures de gestion des correctifs qui donnent la priorité aux correctifs de sécurité des systèmes utilisés pour traiter les données à caractère personnel ou confidentielles de Microsoft. Ces procédures comprennent : • la réalisation d'analyses de vulnérabilité sur une base mensuelle, avec un rapport de conformité de haut niveau indiquant les analyses mensuelles des 12 mois précédents • une approche des risques définie visant à établir des priorités en matière de correctifs de sécurité • la capacité à gérer et à mettre en œuvre des correctifs d'urgence, • l'applicabilité au système d'exploitation et aux logiciels de serveur, tels que les serveurs d'application et les logiciels de base de données, • la documentation indiquant l'atténuation des risques par le correctif et le suivi des exceptions, et • les exigences relatives au retrait des logiciels qui ne sont plus pris en charge par la société auteur.	Le fournisseur peut démontrer qu'il a mis en œuvre une procédure de gestion des correctifs qui répond à cette exigence et couvre au minimum les éléments suivants : • Les définitions de gravité sont documentées et attribuées aux mises à jour afin de déterminer les priorités de déploiement. • La procédure documentée de mise en œuvre des correctifs d'urgence. • Les dossiers de gestion des correctifs qui suivent les approbations et les exceptions, et qui comprennent des données sur la conformité des correctifs. Les registres des 90 derniers jours sont disponibles sur demande.
42	Installer un logiciel antivirus et un logiciel anti-malware sur l'équipement connecté au réseau utilisé pour traiter les données à caractère personnel et confidentielles de Microsoft, notamment les serveurs, les ordinateurs de production et de formation, afin de les protéger contre les virus potentiellement dangereux et les applications logicielles malveillantes. Les logiciels antivirus et anti-malware doivent être régulièrement corrigés et mis à jour. Mettre à jour les définitions anti-malware quotidiennement ou selon les instructions du fournisseur du logiciel antivirus/anti-malware. Remarque : Ceci s'applique à tous les systèmes d'exploitation, y compris Linux.	Il existe des registres montrant que l'utilisation des logiciels antivirus et anti-malware est active. Remarque : Cette exigence s'applique à tous les systèmes d'exploitation.
43	Les fournisseurs qui développent des logiciels pour Microsoft doivent intégrer les principes de sécurité dans le processus de création, et ce dès la conception.	Les documents des caractéristiques techniques des fournisseurs comprennent des points de contrôle pour la validation de la sécurité dans leurs cycles de développement. Le fournisseur utilise une forme quelconque de

		balayage de code pour signaler les défauts évidents.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section J : Sécurité (suite)	
44	Utiliser un programme de prévention des pertes de données (« DLP ») pour empêcher les intrusions, les pertes et autres activités non autorisées au niveau de l'application, du système et de l'infrastructure. Les données doivent être correctement classées, étiquetées et protégées. Le fournisseur doit surveiller les systèmes d'informations utilisés lors du traitement des données à caractère personnel ou confidentielles de Microsoft afin de détecter toute intrusion, perte ou autre activité non autorisée. Le programme DLP doit au minimum : • exiger l'utilisation de systèmes de détection d'intrusion (« IDS ») standards sur l'hôte, sur le réseau et dans le nuage si vous conservez des données à caractère personnel ou confidentielles de Microsoft, • nécessiter la mise en œuvre de systèmes de protection contre les intrusions (« IPS ») configurés pour surveiller et empêcher activement la perte de données, • en cas de violation d'un système, il conviendra d'analyser le système pour s'assurer que toutes les vulnérabilités résiduelles sont également prises en compte, • décrire les procédures requises pour contrôler les outils de détection de la compromission des systèmes, • établir un processus de gestion et de réponse aux incidents qui devra être mis en œuvre si un incident de données est détecté, et • exiger des communications (à tous les employés du fournisseur et aux sous-traitants qui sont retirés des opérations du fournisseur) concernant l'utilisation et le téléchargement non autorisés de données à caractère personnel ou confidentielles de Microsoft.	Programme DLP documenté déployé avec des procédures mises en place aux fins de prévenir les intrusions, les pertes et autres activités non autorisées (et, au minimum, tous les éléments spécifiés dans cette section).

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section J : Sécurité (suite)	
45	Le fournisseur doit veiller à ce que des secrets ne soient pas intégrés ou codés en dur dans le logiciel, à quelque stade que ce soit du processus de développement.	Le fournisseur dispose de procédures documentées pour garantir que les secrets tels que les noms d'utilisateur, mots de passe, clés SSH, jetons d'accès à l'API, etc., n'aient jamais été incorporés dans les fichiers sources ou de configuration, que ce soit dans des environnements de test ou de production. Le fournisseur peut démontrer : • L'utilisation d'une version prise en charge et actuelle d'un outil de prévention de l'exposition des informations d'identification tel que GitHub Advanced Security (GHAS) ou d'un service ou outil similaire. • L'assurance que, si des fichiers sources ou de configuration aient intégré par erreur des secrets, ces derniers sont documentés comme étant révoqués dès leur découverte. • L'assurance que toute information d'identification de remplacement ou secondaire n'a pas été réinsérée dans le code. • La documentation de tous les faux positifs et des mesures correctives adoptées.
46	Le fournisseur doit veiller à ce que les processus de planification de la sauvegarde protègent les données à caractère personnel et confidentielles de Microsoft contre l'utilisation, l'accès, la divulgation, l'altération et la destruction non autorisés.	Le fournisseur peut démontrer qu'il dispose de procédures documentées de réponse et de récupération détaillant la manière dont l'entreprise gérera un événement perturbateur et devra maintenir la sécurité des informations à un niveau prédéterminé sur la base d'objectifs de continuité de la sécurité des informations approuvés par la direction. Le fournisseur peut démontrer qu'il a défini et mis en œuvre des procédures visant à sauvegarder régulièrement, stocker en toute sécurité et récupérer efficacement les données critiques.

47	Établir et tester des plans de continuité des activités et de reprise après sinistre.	Un plan de reprise après sinistre doit comprendre les éléments suivants : • Critères définis pour déterminer si un système est essentiel au fonctionnement de l'entreprise du fournisseur. • Dresser la liste des systèmes critiques, sur la base des critères définis, qui doivent faire l'objet d'une récupération en cas de sinistre. • La procédure de reprise après sinistre définie pour chaque système essentiel, garantissant qu'un ingénieur ne connaissant pas le système puisse récupérer l'application en moins de 72 heures. • Des tests et examens annuels (ou plus fréquents) des plans de reprise après sinistre aux fins de s'assurer que les objectifs de reprise peuvent être atteints.
#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section J : Sécurité (suite)	
48	Authentifier l'identité d'une personne avant de lui accorder un accès aux données à caractère personnel ou confidentielles de Microsoft, et veiller à ce que l'accès soit limité au champ d'activité de la personne en question, autorisée à soutenir les performances.	S'assurer que tous les identifiants des utilisateurs sont uniques et que chacun d'entre eux dispose d'une méthode d'authentification standard, telle que Azure Active Directory. Doit exiger l'utilisation d'une authentification multifacteur (MFA), telle qu'une carte à puce ou un authentificateur sur un téléphone. Programme de sécurité des informations documenté, couvrant le processus permettant de garantir que l'accès de tous les employés et sous-traitants du fournisseur aux données à caractère personnel ou confidentielles de Microsoft ne dépasse pas la durée nécessaire pour soutenir la prestation.

49	Le fournisseur doit protéger toutes les données traitées dans le cadre de ses prestations en les faisant transiter par des réseaux au moyen d'un chiffrement utilisant Transport Layer Sécurité (« **TLS** ») ou Internet Protocol Security (« **IPsec** »). Ces méthodes sont décrites dans les documents NIST 800-52 et NIST 800-57 ; il est également possible d'utiliser une norme industrielle équivalente. Le fournisseur doit refuser la livraison de toute donnée à caractère personnel ou confidentielle de Microsoft transmise par des moyens non chiffrés.	Le processus de création, de déploiement et de remplacement des certificats TLS ou autres doit être défini et appliqué.
50	Tous les appareils du fournisseur (ordinateurs portables, postes de travail, etc.) qui accèderont aux données à caractère personnel ou confidentielles de Microsoft, ou qui les traiteront, devront utiliser un système de chiffrement sur disque.	Il convient de chiffrer tous les appareils aux fins de répondre à la norme BitLocker ou à une autre solution de chiffrement sur disque équivalente dans l'industrie pour tous les appareils clients utilisés pour traiter les données à caractère personnel ou confidentielles de Microsoft.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section J : Sécurité (suite)	
51	Des systèmes et procédures (utilisant les normes actuelles de l'industrie telles que celles décrites dans la norme **NIST 800-111**) doivent être mis en place afin de chiffrer au repos (lorsqu'elles sont stockées) **toutes les** données à caractère personnel et/ou confidentielles de Microsoft. On peut citer à titre d'exemple, sans toutefois s'y limiter : • les données d'identification (p. ex. nom d'utilisateur / mot de passe) • les données relatives aux instruments de paiement (p. ex. les numéros de carte de crédit et de compte bancaire) • les données à caractère personnel relatives à l'immigration • les données relatives au profil médical (p. ex. les numéros de dossier médical ou les marqueurs ou identifiants biométriques, comme l'ADN, les empreintes digitales, la rétine et l'iris, la voix, le visage et les mains, 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, les documents O365, les clients OneDrive) • la documentation relative aux produits Microsoft non annoncés • la date de naissance • les informations sur le 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	Vérifier que les données à caractère personnel et confidentielles de Microsoft sont chiffrées au repos.

	• l'orientation/la préférence sexuelle • les réponses aux questions de sécurité (p. ex. à deux facteurs, réinitialisation du mot de passe) • le nom de jeune fille de la mère	

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section J : Sécurité (suite)	
52	Anonymiser toutes les données à caractère personnel de Microsoft utilisées dans un environnement de développement ou de test.	Les données à caractère personnel de Microsoft ne doivent pas être utilisées dans des environnements de développement ou de test ; s'il n'existe pas d'autre solution, elles devront être rendues anonymes afin d'empêcher l'identification des Personnes concernées ou l'utilisation abusive des données à caractère personnel. Remarque : Les données anonymisées sont différentes des données pseudonymisées. Les données anonymisées sont des données qui ne se rapportent pas à une personne physique identifiée ou identifiable lorsque la Personne concernée par les données à caractère personnel n'est pas ou plus identifiable. Si les données à caractère personnel Microsoft sont des IMP, l'anonymisation devra répondre à la norme de dépersonnalisation HIPAA.
	Section K: Systèmes d'IA	
53	Lorsque des systèmes d'IA sont inclus dans la fourniture d'un service, le fournisseur doit avoir établi avec Microsoft les conditions applicables aux systèmes d'IA. Toute modification des utilisations prévues doit être divulguée dans les plus brefs délais et faire l'objet d'un examen d'exactitude et de conformité au moins une fois par an.	Les conditions contractuelles des systèmes d'IA figurent dans le contrat conclu entre Microsoft et le fournisseur.
54	Attribuer à une personne ou à un groupe désigné au sein de l'entreprise la responsabilité du dépannage, de la gestion, de l'exploitation, de la supervision et du contrôle du système d'IA pendant et après son déploiement.	Nommer le rôle de la personne ou du groupe chargés de veiller au respect du DPR du fournisseur de Microsoft. Un document décrivant l'autorité et la responsabilité de cette personne ou de ce groupe.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section K: Systèmes d'IA (suite)	
55	La mise en place, l'entretien et la prestation d'une formation annuelle en matière de protection de la vie privée et de sécurité par le fournisseur dans le cadre de la performance pour toutes les personnes qui auront accès aux données des systèmes d'IA ou qui les traiteront.	Des registres annuels de présence sont disponibles et peuvent être fournis à Microsoft sur demande. La documentation relative au respect des exigences en matière de formation comprendra la preuve de la formation relative aux exigences réglementaires en matière de protection de la vie privée, aux obligations en matière de sécurité et au respect des exigences et obligations contractuelles applicables pour l'utilisation continue des systèmes d'IA. Le contenu de la formation est validé chaque année.
56	Le fournisseur dispose d'un plan d'intervention en cas d'incident sur le système d'IA qui l'oblige à informer Microsoft conformément aux exigences contractuelles, à la législation applicable en matière de protection de la vie privée ou dans les meilleurs délais, selon ce qui se produit en premier, dès qu'il prend connaissance d'un incident concernant les données ou d'une défaillance constatée qui aurait un impact négatif sur l'une des utilisations prévues et l'une des utilisations sensibles répertoriées pour un système d'IA. Veuillez consulter le guide du programme SSPA pour savoir comment notifier un incident à Microsoft.	Le fournisseur dispose d'un plan d'intervention en cas d'incident sur le système d'IA qui comprend les éléments suivants pour tous les points de terminaison : • Une mesure pour notifier les clients (Microsoft), telle que décrite dans cette exigence. • Un plan de restauration du système, y compris le temps écoulé jusqu'à ce que l'ensemble du système puisse être restauré à un point antérieur. • Une aide à la désactivation des fonctionnalités, y compris le temps écoulé jusqu'à ce que la fonctionnalité puisse être désactivée. • Un processus de mise à jour et de diffusion des mises à jour pour chaque modèle, y compris le temps écoulé jusqu'à la mise à jour du système. • Un processus concernant la manière dont les clients, les partenaires et les utilisateurs finaux seront informés des modifications apportées au système, de la mise à jour des connaissances à propos des défaillances et des meilleures mesures d'atténuation. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.
57	Le fournisseur doit avoir mis en place un Red Teaming pour les systèmes d'IA. Les vulnérabilités doivent être abordées avant le déploiement du système d'IA.	Le fournisseur dispose d'une documentation sur les points suivants : • Les processus de Red Teaming sont établis. • Les vulnérabilités ont été corrigées.

58	Le fournisseur a mis en place un programme d'IA responsable afin de garantir la conformité des données par le biais de divulgations et de documentation, y compris ce qui suit :	Le fournisseur dispose d'une documentation qui décrit le programme d'IA responsable. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.
59	Le fournisseur dispose de déclarations de transparence sur les utilisations prévues.	Les déclarations de transparence sur les utilisations prévues sont fournies à Microsoft sur demande.
#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section K: Systèmes d'IA (suite)	
60	**Accord signé** : lorsqu'elles s'engagent avec des fournisseurs d'IA, les organisations doivent établir des conditions contractuelles claires dans un accord signé. Ces accords doivent aborder explicitement le traitement des données, la confidentialité, les droits de propriété intellectuelle, la responsabilité, l'intervention en cas d'incident et toute utilisation sensible applicable.	Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande, y compris un accord d'association commerciale, le cas échéant.
61	**Responsabilité :** définir clairement les responsabilités en matière de déploiement de l'IA et de gestion des risques au sein de l'organisation. Les organisations doivent identifier les parties responsables des conséquences des systèmes d'IA. Il s'agit notamment de répondre aux préoccupations éthiques, aux préjugés et à toute question susceptible de se poser au fil du temps. Un contrôle et un audit réguliers des modèles d'IA sont essentiels afin de conserver la conformité avec les lignes éthiques directrices.	Le fournisseur dispose d'un document décrivant le programme d'IA responsable, y compris l'obligation de rendre des comptes et les responsabilités de la personne ou du groupe. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.
62	**Évaluation des risques** : procéder à une évaluation des risques liés à la protection de la vie privée, à la sécurité et/ou à l'IA responsable afin de prendre en compte les préjugés potentiels, les vulnérabilités en matière de sécurité et les conséquences involontaires. Si des utilisations sensibles sont comprises, des orientations concernant les contrôles ou les mesures d'atténuation nécessaires doivent être incluses.	Le fournisseur conservera la preuve des évaluations des risques, ou bien d'une documentation ou d'un rapport similaire, y compris les tests, le suivi de l'évolution du système et la maintenance annuelle continue afin d'améliorer les erreurs connues ou découvertes, les impacts divers sur les groupes démographiques, les hallucinations et les autres mesures correctives ou contrôles techniques requis pour rester conforme en matière de sécurité et de protection de la vie privée. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.
63	Transparence et explicabilité : Les systèmes d'IA doivent être transparents et explicables. Le fournisseur doit fournir des renseignements sur la manière dont les décisions sont prises. Les informations à fournir doivent	Le fournisseur doit consigner tous les rapports de défaillance du système, de corruption, d'hallucinations ou d'utilisation abusive signalée qui nuit à l'objectif. Il doit également fournir la preuve des mesures prises

	encourager la transparence dans l'architecture des modèles, les données de formation et les processus de prise de décision.	pour résoudre les problèmes. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.
64	**Surveillance et adaptation** : Le fournisseur doit démontrer qu'il surveille en permanence les systèmes d'IA et qu'il les adapte et les met à jour lorsque de nouveaux risques apparaissent.	Le fournisseur doit consigner tous les rapports de défaillance du système, de corruption, d'hallucinations ou d'utilisation abusive signalée qui nuit à l'objectif. Il doit également fournir la preuve des mesures prises pour résoudre les problèmes. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section K: Systèmes d'IA (suite)	
65	Le fournisseur doit remettre les informations requises, les rapports ou toute autre documentation similaire avec tous les types d'erreurs, définitions des mesures de performance, indicateurs de performance, de sécurité et de fiabilité des données demandés pour chaque utilisation prévue.	• Définir et fournir des fourchettes d'erreurs acceptables pour chaque facteur opérationnel susceptible d'avoir une incidence sur chacune des utilisations prévues, ainsi que tout facteur opérationnel supplémentaire susceptible de réduire les fourchettes acceptables ou de réduire les taux d'erreurs acceptables (y compris les taux d'erreurs faussement positives et négatives) susceptibles d'impacter ces utilisations prévues. • Identifier les facteurs opérationnels et/ou les utilisations prévues, y compris la qualité des données d'entrée du système, d'utilisation et de contexte opérationnel essentiels pour gérer l'utilisation fiable et sûre du système dans son contexte de déploiement. • Divulguer et documenter les cas d'utilisation sensible. • Documenter la mise en œuvre de contrôles efficaces dans la conception du système afin de décourager les préjugés d'automatisation (la tendance éventuelle à se fier de manière excessive aux résultats produits par le système). • Documenter toutes les limites du système, les limites du modèle de données d'entrée ou de sortie, ou les défaillances prévisibles, y compris les utilisations pour lesquelles le système n'a pas été conçu ou évalué et qui peuvent avoir une incidence sur les utilisations prévues. • Documenter les mesures d'atténuation et les contrôles mis en œuvre pour les risques notoires liés à l'IA, tels que la manipulation de l'inférence (« jailbreaks »), la manipulation du modèle (p. ex., empoisonnement des données) et la divulgation d'informations inférentielles (p. ex., extraction d'invite). • Des preuves de la précision et des performances du système, ainsi que du degré auquel ces résultats sont généralisables à d'autres cas d'utilisation.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section K: Systèmes d'IA (suite)	
66	Le fournisseur mettra à jour les divulgations de transparence, y compris l'utilisation sensible et les utilisations prévues, et informera Microsoft dans les cas suivants : • l'ajout de nouvelles utilisations, • les changements de fonctionnalité, • le passage du produit à l'étape de la nouvelle version, • la découverte ou l'application de nouvelles informations sur des performances fiables et sûres ayant une incidence sur l'utilisation prévue, • la disponibilité de nouvelles informations à propos de la précision et de la performance du système.	Le fournisseur dispose d'un plan lors de la mise à jour des informations de transparence qui comprend une étape de notification aux clients (Microsoft), comme décrit dans cette section.
67	Dans le cadre des divulgations de transparence, le fournisseur doit documenter une procédure opérationnelle standard et un plan d'action de surveillance de la santé du système pour chaque système d'IA ou modèle de données, qui comprend les éléments suivants : • les processus permettant de reproduire les défaillances du système pour faciliter le dépannage et la prévention de futures défaillances, • les événements qui seront surveillés, • la manière dont les événements seront examinés en priorité, • la fréquence attendue de ces examens, • la manière dont les événements seront priorisés pour la réponse et le délai de résolution, • les composants d'IA tiers, dont les logiciels libres, sont tenus à jour.	Le fournisseur a documenté les politiques et procédures de contrôle de la santé des systèmes qu'il surveillera pour chaque système d'IA, tel que décrit dans la présente section. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.
68	Établir et documenter un inventaire détaillé des méthodes de surveillance de la santé des systèmes à utiliser, notamment : • les données et les informations générées par les référentiels de données, les analyses du système et les alertes associées, • les processus par lesquels les clients peuvent communiquer des informations sur les défaillances	Le fournisseur a documenté les méthodes de surveillance de la santé du système décrites dans la présente section. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.

	et les préoccupations, et • les processus par lesquels le grand public peut faire part de ses commentaires.	

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section K: Systèmes d'IA (suite)	
69	S'il s'avère que le système d'IA n'est pas adapté aux utilisations prévues à un moment quelconque avant ou pendant l'utilisation du système, le fournisseur s'engage à : • retirer l'utilisation prévue des documents destinés aux clients et informer les clients actuels du problème, prendre des mesures pour combler les lacunes identifiées ou arrêter le système, • réviser la documentation relative à l'utilisation prévue, et • publier la documentation révisée à l'intention des clients.	Le fournisseur a documenté les politiques et procédures qu'il mettra en œuvre en cas de défaillance d'utilisation prévue, telle que décrite dans cette section.
70	Le fournisseur doit identifier et divulguer tous les groupes démographiques connus, y compris les groupes marginalisés, qui risquent de subir une dégradation ou une détérioration de la qualité du service en fonction de l'utilisation prévue du système d'IA, des zones géographiques où le système d'IA sera déployé ou des préjugés inhérents au système d'IA. Les groupes démographiques comprennent : • les groupes définis par un facteur unique, et • les groupes définis par une association de facteurs.	Le fournisseur doit identifier et documenter tous les facteurs justifiables, dont les facteurs circonstanciels et d'autres facteurs opérationnels (par exemple, le « bruit de fond » pour les systèmes de reconnaissance vocale), qui expliquent : • toute incapacité à atteindre un niveau de performance minimum pour un groupe démographique identifié, • les différences de performance qui subsistent entre les groupes démographiques identifiés. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.

Glossaire

« Représentant autorisé » désigne une personne qui dispose du niveau d'autorité approprié pour signer au nom de l'entreprise. Cette personne doit avoir les connaissances requises en matière de protection de la vie privée et de sécurité ou avoir consulté un expert en la matière avant de soumettre sa réponse à une action du programme SSPA. De plus, en ajoutant son nom à un formulaire SSPA, cette personne certifie qu'elle a lu et compris le DPR.

« 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 qui effectuent des tâches ou des services à la demande, par l'intermédiaire de plateformes numériques ou d'autres moyens.

« 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).

« Surveillance humaine » désigne la catégorie de surveillance humaine délimitée par le fournisseur et le niveau d'intervention disponible en cas de détection de défaillances dans le système d'IA pour les utilisations prévues :

- Humain dans la boucle (capacité d'intervention humaine dans chaque cycle de prise de décision du système)
- Humain sur la boucle (capacité d'intervention humaine pendant le cycle de conception du système et surveillance du fonctionnement du système)
- Humain aux commandes (capacité à surveiller l'activité globale du système d'IA et à décider quand et comment utiliser le système d'IA dans une situation donnée)

« Exigences en matière de protection des données à caractère personnel » désigne le RGPD, l'EUDPR, les lois locales de l'UE/EEE relatives à la protection des données, la loi californienne relative à la protection de la vie privée des consommateurs (California Consumer Privacy Act), Cal. Civ. Code § 1798.100 et seq. (*« CCPA »*), le UK Data Protection Act 2018 (Loi britannique de 2018 relative à la protection des données) et toute loi, réglementation et autre exigence légale connexe ou ultérieure applicable au Royaume-Uni, ainsi que toute loi, réglementation et autre exigence légale applicable concernant (a) la vie privée et la sécurité des données ; ou (b) l'utilisation, la collecte, la conservation, le stockage, la sécurité, la divulgation, le transfert, l'élimination et tout autre traitement de toute donnée à caractère personnel.

« Clauses types de l'UE » et « Clauses contractuelles types » désigne (i) les clauses types de protection des données pour le transfert de données à caractère personnel à des sous-traitants établis dans des pays tiers qui n'assurent pas un niveau adéquat de protection des données, telles que décrites à l'Article 46 du RGPD et approuvées par la décision (UE) 2021/914 de la Commission européenne du 4 juin 2021 ;
(ii) toute clause contractuelle type qui lui succède adoptée par (a) la Commission européenne, (b) le Contrôleur européen de la protection des données et approuvé par la Commission européenne, (c) le Royaume-Uni en vertu de la loi fédérale générale relative à la protection des données (General Federal Data Protection Act), (d) la Suisse en vertu de la loi fédérale suisse relative à la protection des données, ou (e) par un gouvernement dans une juridiction autre que la Suisse, le Royaume-Uni et les juridictions composant l'Union européenne / l'Espace économique européen où les clauses régissent le transfert international de données à caractère personnel, sera incorporée et contraignante pour le fournisseur à compter du jour de son adoption.

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