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** » 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.

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.

« 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 non autorisée ou un accès accidentel ou illégal aux données à caractère personnel ou aux données confidentielles de Microsoft transmises, stockées ou

autrement traitées 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 d'une personne concernée d'accéder, de supprimer, de modifier, d'exporter, de restreindre ou de s'opposer au traitement des données de la Personne concernée.
Les données à caractère personnel Microsoft de cette personne concernée si la loi l'exige.

« 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.

« Données confidentielles de Microsoft » désigne toutes les informations qui, si elles sont compromises par des moyens de confidentialité ou d'intégrité, peuvent entraîner une perte financière ou atteinte à la 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.

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

« 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.

« Traitement » désigne toute opération ou tout ensemble d'opérations effectuées sur des données à caractère personnel ou sur 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, la récupération, 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 « 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).

« 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). 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. 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 : 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 dispenser une formation annuelle en matière de protection de la vie privée et de la sécurité aux employés qui auront accès aux données à caractère personnel traitées par le fournisseur dans le cadre de la prestation ou aux données 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 comprend les principes de confidentialité et de sécurité. 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. 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.
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 fwdlink vers la déclaration de confidentialité actuelle et publiée de 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 (notamment toute nouvelle activité de traitement 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 qu'une Personne concernée donne son consentement à une activité de traitement et que la portée du consentement couvre toutes les activités de traitement du fournisseur en ce qui concerne les données à caractère personnel de la Personne concernée. Le fournisseur peut démontrer la mesure dans laquelle une Personne concernée retire son consentement à 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, ainsi que doit 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 « Vie privée 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. Si la destruction des données à caractère personnel ou confidentielles de Microsoft est nécessaire, le fournisseur devra brûler, pulvériser ou déchiqueter les supports matériels contenant des données à caractère personnel et/ou confidentielles de Microsoft de 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, de les supprimer, de les modifier, de les exporter, de les restreindre et de s'opposer à leur traitement (« Droits des personnes concernées »). Si une personne concernée cherche à exercer les droits que lui confère la loi en ce qui concerne ses données à caractère personnel Microsoft, le fournisseur devra permettre à Microsoft de prendre les mesures suivantes ou de 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 devra orienter toutes les Personnes concernées qui le contactent directement vers Microsoft aux fins qu'elles puissent exercer leurs droits en tant que Personnes concernées.	Le fournisseur devra conserver les preuves des processus et procédures documentés pour faciliter l'exécution 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	S'il répond directement à la Personne concernée ou s'il propose un mécanisme en ligne en libre-service, le fournisseur devra disposer de processus et de procédures permettant d'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 des données personnelles de Microsoft concernant une Personne concernée qui ne sont pas disponibles par le biais d'un mécanisme en ligne en libre-service, le fournisseur devra faire un effort raisonnable pour localiser les données demandées et conserver suffisamment d'informations pour 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 sans le cadre des Droits des personnes concernées. 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 devra communiquer à la Personne concernée les mesures qu'elle devra prendre pour accéder à ses données à caractère personnel 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 des Personnes concernées et les mesures prises par le fournisseur en réponse à ces demandes. Si sa demande est rejetée, fournir, sur instruction de Microsoft, une explication écrite à la Personne concernée . Remettre à Microsoft, sur demande, le registre 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 permettre à Microsoft d'obtenir, ou obtenir lui-même, une copie des données à caractère personnel Microsoft demandées pour la Personne concernée authentifiée dans un format imprimé, électronique ou oral approprié.	Le fournisseur remet les données à caractère personnel de Microsoft à la Personne concernée dans un 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 prendre des précautions raisonnables pour s'assurer que les données à caractère personnel Microsoft communiquées à Microsoft ou à une Personne concernée authentifiée ne peuvent pas être utilisées pour identifier une autre personne.	Le fournisseur devra conserver des preuves documentées des procédures relatives aux précautions prises pour éviter l'identification de la Personne concernée contrairement aux termes 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 Microsoft ne sont pas complètes et exactes, le fournisseur devra transmettre le problème à Microsoft et coopérer avec cette dernière, le cas échéant, pour résoudre le problème.	Le fournisseur documente les cas de désaccord et transmet le problème à Microsoft. Le fournisseur devra remettre des preuves documentaires à 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 :	
24	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.
25	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.
26	Si Microsoft est le contrôleur 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 la mesure dans laquelle les sous-traitants utilisent les préférences de Microsoft relatives aux 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.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section G : Sous-traitants (suite)	
27	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.
28	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.
29	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.
30	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.
31	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	
32	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	
33	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. 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.
34	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. Le fournisseur devra remettre des preuves documentaires à Microsoft sur demande.

35	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.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	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 36 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. Remarque : Vous devrez fournir la certification.
36	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, et ▪ 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.
37	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.

38	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.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section J : Sécurité (suite)	
39	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, ▪ 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, et ▪ des contrôles stricts des mots de passe qui imposent la longueur et la complexité des mots de passe et empêchent leur réutilisation. 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.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section J : Sécurité (suite)	
40	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.
41	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.
42	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 : ▪ L'attribution d'un niveau de gravité afin d'établir des priorités. (Les définitions de la gravité sont documentées). ▪ La procédure documentée de mise en œuvre des correctifs d'urgence. ▪ La confirmation qu'il n'existe pas d'utilisation de systèmes d'exploitation qui ne sont plus pris en charge par la société auteur. ▪ Les registres de gestion des correctifs qui suivent les approbations et les exceptions.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section J : Sécurité (suite)	
43	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 : ▪ nécessiter l'utilisation de systèmes de détection d'intrusion standard pour l'hôte, le réseau et l'informatique en nuage ▪ (« **IDS** ») 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, ▪ exiger des communications (à tous les employés du fournisseur et aux sous-traitants qui quittent, et ▪ la prestation du fournisseur) en ce qui concerne le téléchargement et l'utilisation non autorisés des 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)	
44	Communiquer rapidement à la direction et à Microsoft les résultats de l'enquête menée à la suite de la réponse à l'incident.	Des systèmes et des processus doivent être mis en place aux fins de communiquer à Microsoft les résultats de l'enquête sur la réponse à l'incident.
45	Les administrateurs du système, le personnel d'exploitation, les tiers de gestion et toute personne accédant aux données à caractère personnel ou confidentielles de Microsoft doivent suivre une formation annuelle en matière de sécurité.	Mettre en place un programme annuel de formation en matière de sécurité qui comprend : ▪ La formation à la réponse aux incidents, événements simulés et mécanismes automatisés aux fins de faciliter une réponse efficace aux situations de crise. ▪ 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. ▪ Si les données à caractère personnel Microsoft sont des IMP, le programme de sensibilisation et de formation devra comprendre des rappels de sécurité et aborder la question du contrôle des connexions et de la protection des mots de passe. ▪ Un contenu régulièrement mis à jour.
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.

#	Exigences de Microsoft en matière de protection des données des fournisseurs	Preuve de conformité
	Section J : Sécurité (suite)	
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.
48	Authentifier l'identité d'une personne avant de lui accorder l'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 spécifique, autorisée à soutenir la prestation.	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. L'accès élevé (administratif ou autres types de privilèges accrus) doit nécessiter l'utilisation d'un second facteur, tel qu'une carte à puce ou un système d'authentification téléphonique. 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 Security (« **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.

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

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. les 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 ▪ 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	Vérifier que les données à caractère personnel et confidentielles de Microsoft sont chiffrées au repos.

#	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.
53	Le fournisseur doit s'assurer que des éléments ~~les~~ secrets ne sont pas intégrés ou codés en dur dans le logiciel à aucune étape du processus de développement.	Le fournisseur a documenté des procédures pour s'assurer que des secrets tels que les noms d'utilisateur, les mots de passe, les clés SSH, les jetons d'accès API, etc., n'ont jamais été intégrés dans les fichiers source 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 identifiants tels que GitHub Advanced Security (GHAS) ou un service ou outil similaire. ▪ l'assurance que si les fichiers source ou de configuration incluaient par erreur des secrets, ces secrets ont été documentés comme révoqués dès leur découverte. ▪ l'assurance qu'aucun identifiant de remplacement ou secondaire n'a été réintroduit dans le code. ▪ la documentation de tous les faux positifs et leur correction.

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).

« 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.