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

Applicabilité

Les exigences en matière de protection des données destinées aux fournisseurs de Microsoft (ci-après les « **EPD** ») s'appliquent à tout fournisseur Microsoft qui traite les Données personnelles ou confidentielles Microsoft en lien avec la prestation dudit fournisseur (p. ex., la fourniture de services, les licences logicielles ou les services cloud) en vertu du contrat qu'il a signé avec Microsoft (p. ex., bons de commande, contrat cadre) (ci-après la « **Prestation** »).

- En cas de conflit entre les exigences stipulées dans le présent document et celles spécifiées dans les accords contractuels passés entre le fournisseur et Microsoft, les EPD prévaudront, sauf si le fournisseur concerné identifie dans le formulaire d'attestation EPD la disposition correspondante du contrat en conflit avec la section applicable des EPD (auquel cas, les termes du contrat prévaudront).
- En cas de conflit entre les exigences stipulées dans le présent document et une exigence légale ou statutaire, cette dernière prévaudra.
- Si le fournisseur Microsoft fait office de Contrôleur, seules les exigences des sections J Sécurité et A Gestion des présentes EPD s'appliquent relativement aux activités de Traitement dudit fournisseur.
- Si le fournisseur Microsoft ne traite pas de Données personnelles Microsoft, mais uniquement des Données confidentielles Microsoft, seules les exigences des sections A Gestion, E Conservation et J Sécurité des présentes EPD s'appliquent relativement au Traitement des Données confidentielles Microsoft par ledit fournisseur.

Transfert international de données

Sans limitation de ses autres obligations, le fournisseur n'effectue aucun transfert international des Données personnelles Microsoft, sauf accord écrit préalable de Microsoft, et quoi qu'il en soit, le fournisseur doit respecter les exigences en matière de protection des données définies dans toute clause contractuelle type, les règles professionnelles contraignantes ou tout autre modèle approuvé par une autorité chargée de la protection des données, le Contrôleur européen de la protection des données ou la Commission européenne, et adopté ou accepté par Microsoft, y compris les frameworks UE-États-Unis et Suisse-États-Unis du Privacy Shield et la réglementation européenne générale sur la protection des données. Le fournisseur accepte de prévenir Microsoft s'il s'aperçoit qu'il ne peut plus respecter ses obligations et fournir le niveau de protection requis par les principes du Privacy Shield. Le fournisseur doit également s'assurer de la conformité de tous les sous-traitants (tels que définis dans la Clause 1(d) des Clauses contractuelles types de 2010 publiées en annexe de la décision C(2010)593 de la Commission européenne).

Principales définitions

Les termes ci-après sont utilisés dans les présentes EPD et sont définis comme suit. Les exemples qui suivent les termes « y compris », « comme », « p. ex. », « par exemple », ou termes similaires utilisés dans les présentes EPD incluent implicitement les tournures « sans limitation » ou « mais sans s'y limiter », sauf s'ils s'accompagnent des termes « uniquement » ou « exclusivement ».

Le « **Contrôleur** » est la personne physique ou juridique, l'autorité publique, l'agence ou tout autre organisme qui détermine, seul ou conjointement, les finalités et les moyens du Traitement des Données personnelles. Dans les cas où les finalités et les moyens du Traitement sont déterminés par la législation de l'Union européenne (ci-après « **UE** ») ou de ses États membres, le Contrôleur (ou les critères pour désigner ce dernier) peut être désigné par ces législations.

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

Les « **Données personnelles** » sont toutes les informations relatives à une personne physique identifiée ou identifiable (la « **Personne concernée** ») ; une personne physique identifiable est une personne susceptible d'être identifiée, directement ou indirectement, en particulier en se référant à des données d'identification comme un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs facteurs propres à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de ladite personne physique.

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

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

Une « **Entité traitant les informations** » est une personne physique ou juridique, une autorité publique, une agence ou tout autre organisme qui traite des données personnelles au nom du Contrôleur.

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

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

La « **Violation des données** » est une violation de la sécurité qui entraîne accidentellement ou illicitement l'accès à ou la destruction, la perte, l'altération, la divulgation non autorisée de Données personnelles ou confidentielles Microsoft transmises, stockées ou traitées.

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section A : Gestion		
1	Tout contrat applicable entre Microsoft et le fournisseur (p. ex., contrat cadre, énoncé des travaux, bons de commande et autres commandes) spécifie les méthodes de protection des données confidentielles et sécurisées relativement aux Données personnelles et confidentielles Microsoft, le cas échéant. Pour les entreprises qui traitent les données, le contrat doit inclure la portée et la durée du Traitement, la nature et l'objectif dudit Traitement, le type de Données personnelles Microsoft et les catégories des Personnes concernées, ainsi que les droits et obligations de Microsoft.	Le fournisseur doit présenter le contrat applicable conclu entre Microsoft et lui-même. Pour les Entités traitant les informations, les descriptions du Traitement sont indiquées dans le contrat applicable (*p. ex.*, énoncé des travaux, bons de commande). Remarque : les entreprises possédant des bons de commande en vol peuvent ajouter la description nécessaire des activités de Traitement lors d'une étape ultérieure du processus d'achat.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
2	Confier la responsabilité relative au respect des exigences en matière de protection des données destinées aux fournisseurs à une personne ou un groupe désigné(e) au sein de la société.	Nom de la personne ou du groupe chargé de garantir la conformité aux EPD. Document décrivant l'autorité et la responsabilité de ladite personne ou dudit groupe et démontrant un rôle en matière de confidentialité et/ou de sécurité.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
3	Organiser, maintenir et réaliser annuellement des formations sur la confidentialité et la sécurité destinées aux employées ayant accès aux Données personnelles ou confidentielles Microsoft. Si votre société ne dispose pas de contenu préparé, vous pouvez utiliser ce modèle de document et l'adapter à votre situation.	Des registres de participation annuels sont disponibles. Le contenu de la formation inclut les principes de la confidentialité et de la sécurité.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
4	Traiter les Données personnelles Microsoft conformément aux instructions fournies en matière de transferts de Données personnelles Microsoft vers un pays tiers ou une autre organisation, à moins d'y être contraint par la Loi ; le cas échéant, l'Entité traitant les informations (fournisseur) doit signaler cette exigence légale au contrôleur (Microsoft) avant de procéder au Traitement, sauf si	Preuves des instructions documentées telles que définies dans un contrat (p. ex., un énoncé des travaux ou un bon de commande), ou capturées par le biais d'un système électronique utilisé lors de la Prestation.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

	la Loi interdit lesdites informations pour des motifs d'intérêt public importants.		

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section B : Notification		
5	Le fournisseur doit utiliser la Déclaration de confidentialité Microsoft lorsqu'il collecte des Données personnelles au nom de Microsoft. La notification de confidentialité doit être claire et mise à disposition des Personnes concernées pour les aider à décider s'ils souhaitent confier leurs Données personnelles au fournisseur. Remarque : si votre entreprise est le Contrôleur de l'activité de Traitement, publiez votre propre notification de confidentialité. *Contacter SSPAHelp@microsoft.com pour accéder aux notifications Microsoft correspondantes.*	Le fournisseur utilise un lien fwdlink vers la Déclaration de confidentialité publiée par Microsoft. La Déclaration de confidentialité est publiée lors de la collecte des Données personnelles d'un utilisateur. Le cas échéant, une version hors connexion est disponible et est fournie avant la collecte des données. Toute Déclaration de confidentialité hors connexion utilisée constitue la dernière version publiée et est datée correctement. Pour les services aux employés Microsoft, la Notification de protection des données Microsoft est utilisée.	*<Conforme> <Non conforme> <Non applicable> <Conflit légal> <Conflit contractuel>*
6	Lors de la collecte de Données personnelles Microsoft via un appel téléphonique en direct ou enregistré, les fournisseurs doivent être prêts à discuter des pratiques applicables en matière de collecte, de gestion, d'utilisation et de conservation des données avec les Personnes concernées.	Un script des enregistrements vocaux explique le Traitement des Données personnelles Microsoft, ainsi que ▪ leur collecte, ▪ leur utilisation et ▪ leur conservation.	*<Conforme> <Non conforme> <Non applicable> <Conflit légal> <Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section C : Choix et consentement		
7	Lorsque le fournisseur a besoin du consentement comme base légale pour le Traitement des données, il doit obtenir et consigner un consentement de la Personne concernée pour toutes ses activités de Traitement (y compris les nouvelles et les activités mises à jour) avant de collecter les Données personnelles à son sujet.	Le fournisseur peut expliquer comment une Personne concernée donne son consentement pour une activité de Traitement, et que la portée dudit consentement couvre l'ensemble des activités de Traitement du fournisseur relativement aux Données personnelles de la Personne concernée. Le fournisseur peut expliquer comment une Personne concernée retire son consentement pour une activité de Traitement. Le fournisseur peut expliquer la vérification des préférences avant de lancer toute nouvelle activité de Traitement. Le fournisseur surveille l'efficacité de la gestion des préférences afin de garantir que le délai nécessaire pour honorer une modification des préférences correspond à l'exigence légale locale applicable la plus restrictive. Remarque : la preuve peut prendre la forme de captures d'écran de l'interaction utilisateur, d'une expérimentation du service ou d'une possibilité de consulter la documentation technique.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section C : Choix et consentement (suite)		
8	Les cookies sont de petits fichiers texte stockés par les sites Web et/ou les applications en ligne sur les appareils. Ces fichiers contiennent des informations utilisées pour reconnaître la Personne concernée ou un appareil. Les fournisseurs qui créent et gèrent des sites Web et des applications Microsoft doivent communiquer aux Personnes concernées des notifications claires sur l'utilisation des cookies et leur offrir un choix en la matière. Les fournisseurs qui créent et gèrent des sites Web et/ou des applications Microsoft doivent s'assurer que l'utilisation des cookies est conforme aux engagements de la Déclaration de confidentialité Microsoft et à la législation locale, notamment la réglementation établie par l'UE.	L'objectif de chaque cookie doit être consigné, et le type de cookie mis en œuvre doit être précisé. ▪ Les cookies permanents ne doivent pas être utilisés si les cookies de session suffisent. ▪ Si des cookies permanents sont utilisés, ils ne doivent pas être conservés plus de 2 ans après qu'un utilisateur a consulté le site. Pour les utilisateurs au sein de l'UE, la date d'expiration d'un cookie permanent ne doit pas dépasser 13 mois. Validation de la conformité avec les Lois de l'UE, le cas échéant, notamment ▪ l'utilisation de la convention de signalisation, « Confidentialité et cookies » pour la déclaration de confidentialité, et ▪ l'obtention du consentement de l'utilisateur avant l'utilisation de cookies à des fins « non essentielles » (par exemple, la publicité).	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section D : Collecte		
9	Le fournisseur doit contrôler la collecte des Données personnelles et/ou confidentielles Microsoft afin de s'assurer que seules les données collectées sont celles requises pour la Prestation.	Le fournisseur peut fournir des documents qui montrent que les Données personnelles et/ou confidentielles Microsoft collectées sont nécessaires pour la Prestation.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
10	S'il collecte des Données personnelles auprès de tiers au nom de Microsoft, le fournisseur devra confirmer que les règles et pratiques de protection des données mises en place par lesdits tiers respectent les termes du contrat que le fournisseur a conclu avec Microsoft, ainsi que les exigences en matière de protection des données destinées aux fournisseurs.	Le fournisseur peut fournir une documentation de la diligence raisonnable exercée quant aux règles et pratiques de protection des données de tiers.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
11	Avant de collecter des Données personnelles Microsoft via l'installation ou l'utilisation de logiciels pouvant s'exécuter sur l'appareil d'une Personne concernée, il convient de préciser en détail la nécessité desdites informations dans le cadre d'un contrat conclu entre le fournisseur et Microsoft.	L'accord de Microsoft quant à l'utilisation de logiciels exécutables sur l'appareil d'une Personne concernée est indiqué dans le contrat conclu.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
12	Avant de collecter des Données personnelles sensibles Microsoft (données révélant l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, l'adhésion à un syndicat ; données génétiques ; données biométriques ; données relatives à la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique), il convient de préciser en détail la nécessité desdites Données personnelles Microsoft dans le cadre d'un contrat conclu entre le fournisseur et Microsoft.	La nécessité de collecter des Données personnelles Microsoft sensibles est indiquée dans le contrat conclu avec Microsoft.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section E : Conservation		
13	S'assurer que les Données personnelles et confidentielles Microsoft ne sont pas conservées plus longtemps que nécessaire pour fournir les services, sauf si une conservation continue des Données personnelles et/ou confidentielles Microsoft est requise par la Loi.	Le fournisseur respecte les exigences en matière de conservation des données ou les politiques de conservation des documents spécifiées par Microsoft dans le contrat (p. ex., l'énoncé des travaux ou le bon de commande).	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
14	S'assurer que, à l'entière discrétion de Microsoft, les Données personnelles ou confidentielles Microsoft que le fournisseur détient ou contrôle sont retournées à Microsoft ou détruites lors de la Prestation ou à la demande de Microsoft. Des processus doivent être mis en place au sein des applications pour s'assurer que les données sont bien effacées lorsqu'elles sont supprimées de l'application par l'utilisateur ou par un déclencheur comme l'âge des données. Lorsque la destruction de Données personnelles ou confidentielles Microsoft est nécessaire, le fournisseur doit brûler, pulvériser ou détruire les documents physiques contenant des Données personnelles et/ou confidentielles Microsoft de sorte que celles-ci ne puissent pas être lues ou reconstituées.	Archivage de la suppression des Données personnelles et confidentielles Microsoft (p. ex., renvoi à Microsoft pour destruction). Si une destruction est exigée ou demandée par Microsoft, le fournisseur doit fournir un certificat de destruction signé par l'un de ses agents.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section F : Personnes concernées		
	Les Personnes concernées ont le droit d'accéder à leurs Données personnelles, de les supprimer, les modifier et les exporter, ainsi que de limiter leur Traitement et de s'y opposer (« **Droits des Personnes concernées** »). Lorsqu'une Personne concernée souhaite exercer les droits que lui confère la Loi en vigueur pour ses Données personnelles, le fournisseur doit :		
15	Aider Microsoft, par les mesures techniques et organisationnelles appropriées, dans la mesure du possible, à respecter ses obligations de réponse aux demandes des Personnes concernées souhaitant exercer leurs droits.	Des processus et des procédures sont en place pour soutenir l'exécution des Droits des Personnes concernées.	*<Conforme> <Non conforme> <Non applicable> <Conflit légal> <Conflit contractuel>*
16	Répondre sans retard à toutes les demandes relatives aux Droits des Personnes concernées.	Le fournisseur réalise des tests périodiques pour s'assurer qu'il est en mesure d'appliquer les Droits des Personnes concernées.	*<Conforme> <Non conforme> <Non applicable> <Conflit légal> <Conflit contractuel>*
17	Sauf indication contraire de Microsoft, le fournisseur renverra toutes les Personnes concernées qui le contactent directement à Microsoft pour faire valoir leurs Droits. Le fournisseur communiquera à la Personne concernée les étapes à suivre pour consulter ou faire valoir ses droits pour ses Données personnelles Microsoft. *Contacter SSPAHelp@microsoft.com pour obtenir de l'aide avec cette exigence.*	Le fournisseur communique les étapes à suivre pour accéder aux Données personnelles, ainsi que les méthodes disponibles pour mettre à jour ces données.	*<Conforme> <Non conforme> <Non applicable> <Conflit légal> <Conflit contractuel>*
18	Lorsque vous répondez directement à une Personne concernée effectuant une demande, vérifiez son identité.	Le fournisseur a consigné la méthode employée pour identifier les Personnes concernées de Microsoft.	*<Conforme> <Non conforme> <Non applicable> <Conflit légal> <Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section F : Personnes concernées (suite)		
	Lorsqu'une Personne concernée a été authentifiée, le fournisseur doit :		
19	Déterminer s'il possède ou contrôle des Données personnelles Microsoft sur cette Personne concernée.	Le fournisseur dispose de procédures pour déterminer s'il possède des Données personnelles.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
20	Déployer des efforts raisonnables pour localiser les Données personnelles Microsoft demandées et consigner des archives suffisantes en vue de démontrer qu'une recherche raisonnable a été effectuée.	Le fournisseur tient un registre expliquant les étapes suivies pour répondre aux demandes relatives aux Droits des Personnes concernées. La documentation inclut : ▪ la date et l'heure de la demande ; ▪ les actions entreprises pour répondre à cette demande ; et ▪ le moment où Microsoft en a eu connaissance.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
21	Enregistrer la date et l'heure des demandes relatives aux Droits des Personnes concernées et les opérations effectuées par le fournisseur en réponse à ces demandes. Fournir les demandes des Personnes concernées à la demande de Microsoft.	Le fournisseur conserve les demandes d'accès dans ses archives et consigne les modifications apportées aux Données personnelles.	
	Lorsqu'une Personne concernée a été authentifiée et que le fournisseur a confirmé qu'il possède les Données personnelles Microsoft demandées, le fournisseur doit :		
22	Pour les demandes d'obtention d'une copie des Données personnelles, fournir les Données personnelles Microsoft à la Personne concernée sous forme imprimée, électronique ou verbalement, selon le cas.	Le fournisseur transmet les Données personnelles à la Personne concernée dans un format compréhensible et pratique pour la Personne concernée et le fournisseur.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section F : Personnes concernées (suite)		
23	En cas de refus de la demande, à la discrétion de Microsoft, communiquer par écrit à la Personne concernée une explication conforme aux instructions fournies précédemment par Microsoft. *Contacter SSPAHelp@microsoft.com pour obtenir de l'aide avec cette exigence.*	Consigner les refus de demandes et archiver des preuves du processus d'examen et d'approbation de Microsoft.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
24	Le fournisseur doit prendre des précautions raisonnables pour s'assurer que les Données personnelles Microsoft communiquées à la Personne concernée ne peuvent pas être utilisées pour identifier une autre personne.	Le fournisseur doit démontrer que des précautions raisonnables sont prises de sorte qu'une autre personne ne puisse pas être identifiée à partir des données communiquées (p. ex., impossibilité de photocopier la totalité de la page de données lorsque les Données personnelles demandées pour une Personne concernée apparaissent sur une seule ligne).	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
25	Si une Personne concernée et un fournisseur ne sont pas d'accord sur l'exhaustivité et la précision des Données personnelles Microsoft, le fournisseur doit signaler le problème à Microsoft et collaborer comme il se doit pour résoudre le problème. *Contacter SSPAHelp@microsoft.com pour obtenir de l'aide avec cette exigence.*	Le fournisseur consigne les désaccords et signale le problème à Microsoft.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section G : Communication à des tiers		
	Si le fournisseur souhaite recourir à un sous-traitant pour traiter les Données personnelles ou confidentielles Microsoft, il doit :		
26	Obtenir le consentement écrit exprès de Microsoft avant d'engager des services de sous-traitance ou d'apporter des modifications liées à l'ajout ou au remplacement de sous-traitants. *Contacter SSPAHelp@microsoft.com pour obtenir de l'aide avec cette exigence.*	Vérifier que les Données personnelles de Microsoft sont uniquement traitées par des sociétés connues de Microsoft, ainsi que l'exige le contrat applicable (p. ex., un énoncé des travaux un addendum, un bon de commande) ou indique la base de données SSPA.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
27	Documenter la nature et la portée des Données personnelles et confidentielles Microsoft déléguées à des sous-traitants, en s'assurant que les informations collectées sont nécessaires à la Prestation.	Le fournisseur conserve dans ses archives les Données personnelles et confidentielles Microsoft communiquées ou transférées à des sous-traitants.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
28	S'assurer que le sous-traitant utilise les Données personnelles Microsoft conformément aux préférences de contact stipulées par la Personne concernée.	Montrer comment les préférences de la Personne concernée de Microsoft sont utilisées par les sous-traitants. Fournir des documents justificatifs comprenant le délai imparti à un sous-traitant pour honorer une modification de préférence.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
29	Limiter le traitement des Données personnelles Microsoft par le sous-traitant aux fins lui permettant de remplir ses obligations stipulées dans le contrat passé avec Microsoft.	Le fournisseur peut transmettre des documents qui montrent que les Données personnelles Microsoft communiquées à un sous-traitant sont nécessaires pour la Prestation.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
30	Vérifier les réclamations afin d'y rechercher des indications de traitement non autorisé ou illégal des Données personnelles Microsoft.	Le fournisseur peut prouver que des systèmes et des processus sont en place pour gérer les réclamations concernant une utilisation ou une communication non autorisée de Données personnelles Microsoft par un sous-traitant.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section G : Communication à des tiers (suite)		
31	Notifier rapidement Microsoft lorsqu'il est établi qu'un sous-traitant a traité des Données personnelles ou confidentielles Microsoft à des fins autres que celles liées à la Prestation.	Le fournisseur a fourni aux sous-traitants les instructions et les moyens nécessaires pour signaler toute utilisation abusive des données Microsoft.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
32	Prendre rapidement des mesures afin d'atténuer tout préjudice réel ou potentiel provoqué par le traitement non autorisé ou illégal des Données personnelles et confidentielles Microsoft par un sous-traitant.	Le fournisseur peut démontrer qu'il dispose d'un plan et de procédures en cas d'utilisation abusive des Données personnelles et confidentielles Microsoft par un sous-traitant.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
	Section H : Qualité		
33	Le fournisseur doit assurer l'intégrité de toutes les Données personnelles Microsoft, en vérifiant qu'elles sont exactes, complètes et pertinentes aux fins stipulées pour lesquelles elles ont été traitées.	Le fournisseur peut prouver que des procédures sont en place pour valider les Données personnelles de Microsoft lorsqu'elles sont collectées, créées et mises à jour. Le fournisseur peut prouver que des procédures de surveillance et d'échantillonnage sont en place pour vérifier continuellement l'exactitude des informations si nécessaire.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section I : Contrôle et application		
34	Le Fournisseur dispose d'un plan de réponse aux incidents qui l'oblige à informer Microsoft sans retard de toute Violation des données ou vulnérabilité liée au traitement de Données personnelles ou confidentielles Microsoft par le fournisseur. *Contacter SSPAHelp@microsoft.com pour signaler un incident.*	Le fournisseur dispose d'un plan de réponse aux incidents qui comprend une étape pour informer les clients (Microsoft), comme décrit dans cette section.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
35	Ne pas publier de communiqués de presse ou tout autre avis public relatant un incident potentiel ou avéré impliquant des Données personnelles ou confidentielles Microsoft sans avoir obtenu l'accord préalable de Microsoft, sauf en cas d'exigences légales contraires.	Le fournisseur accepte de se conformer à cette exigence si l'événement se produit.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
36	Mettre en œuvre un plan de résolution et contrôler la résolution des violations et vulnérabilités liées aux Données personnelles ou confidentielles Microsoft afin de s'assurer que des mesures correctives appropriées sont prises en temps opportun.	Le fournisseur a consigné les procédures à suivre pour remédier à une Violation des données jusqu'à la résolution du problème.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
37	Mettre en place un processus de réclamation officiel afin de répondre à toutes les réclamations relatives à la protection des données et impliquant des Données personnelles Microsoft.	Le fournisseur a le moyen de recevoir des plaintes impliquant des Données personnelles Microsoft et dispose d'une procédure documentée de traitement des plaintes.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section J : Sécurité		
	Le fournisseur doit développer, mettre en œuvre et gérer un programme de sécurité des informations qui comprend des règles et des procédures destinées à la protection des Données personnelles et confidentielles de Microsoft conformément aux bonnes pratiques du secteur et à la Loi. Le programme de sécurité du fournisseur doit respecter les normes indiquées ci-dessous, exigences 38-56.	Cette liste de conditions n'est pas exhaustive, car certaines conditions peuvent être nécessaires pour respecter des réglementations (p. ex., HIPAA, GLBA) ou des exigences contractuelles. Un rapport ISO 27001 ou SOC 2 valide avec sécurité constitue des équivalents acceptables à la section J. Contacter SSPAHelp@microsoft.com pour appliquer cette substitution. Remarque : vous devrez fournir une documentation décrivant la portée de ces certifications/rapports.	
38	Réaliser des évaluations de sécurité du réseau annuelles, notamment : ▪ examiner les principales modifications apportées à l'environnement, par exemple, nouveau composant système, modification de la topologie du réseau ou des règles du pare-feu ; ▪ réaliser des analyses de vulnérabilité ; et ▪ archiver les journaux des modifications.	Le fournisseur a consigné les évaluations du réseau, les journaux des modifications et les résultats des analyses. Les journaux des modifications requis doivent suivre les modifications, fournir des informations sur le motif de la modification et inclure le nom et le titre de l'approbateur désigné.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
39	Le fournisseur doit définir, communiquer et mettre en œuvre une politique pour les appareils mobiles afin de sécuriser et de limiter l'accès aux Données personnelles ou confidentielles Microsoft et leur utilisation sur un appareil mobile.	Le fournisseur prouve qu'il utilise une politique de conformité pour les appareils mobiles dans laquelle le traitement des Données personnelles ou confidentielles de Microsoft nécessite l'utilisation d'un appareil mobile.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section J : Sécurité (suite)		
40	Toutes les ressources utilisées pour soutenir la Prestation doivent être prises en compte et avoir un propriétaire identifié. Le fournisseur est responsable d'en tenir un inventaire ; d'établir une utilisation acceptable et autorisée pour ces ressources ; et de leur assurer un niveau de sécurité adéquat tout au long de leur cycle de vie.	Inventaire des ressources en appareils utilisées pour soutenir la Prestation. L'inventaire de ces ressources doit comprendre : ▪ l'emplacement de l'appareil ; ▪ la classification des données sur la ressource ; ▪ l'archive de récupération des ressources lors de la résiliation d'un contrat de travail ou d'un accord commercial ; et ▪ l'archive de destruction du support de stockage des données lorsqu'il n'est plus nécessaire.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section J : Sécurité (suite)		
41	Établir et maintenir des procédures de gestion des droits d'accès pour empêcher tout accès non autorisé aux Données personnelles ou confidentielles Microsoft détenues par le fournisseur.	Le fournisseur prouve qu'il a mis en œuvre un plan de gestion des droits d'accès comprenant : ▪ des procédures de contrôle d'accès ; ▪ des procédures d'identification ; ▪ des procédures de blocage après plusieurs tentatives ; ▪ une réinitialisation des mots de passe aussi souvent que nécessaire (au maximum tous les 90 jours) ; ▪ des paramètres robustes pour la sélection d'informations d'authentification ; ▪ la désactivation des comptes utilisateur dans les 48 heures qui suivent la résiliation d'un contrat de travail. Le fournisseur prouve qu'il a établi un processus pour vérifier l'accès des utilisateurs aux Données personnelles et confidentielles de Microsoft, en appliquant le principe du privilège minimum. Ce processus doit inclure : ▪ des rôles utilisateur clairement définis ; ▪ des procédures permettant d'examiner et de justifier l'approbation de l'accès aux rôles ; ▪ une vérification que les utilisateurs dont les rôles donnent accès aux données de Microsoft disposent d'un justificatif pour occuper ce rôle/être dans ce groupe.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

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

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section J : Sécurité (suite)		
45	Appliquer un programme de prévention des pertes de données (« **DLP** »). Les données doivent être correctement classifiées, étiquetées et protégées, et le fournisseur doit surveiller les systèmes d'informations utilisés lors du traitement des Données personnelles ou confidentielles Microsoft pour détecter les intrusions, les pertes et les activités non autorisées. Le programme DLP, au minimum, ▪ requiert l'utilisation d'un hôte standard, d'un réseau et de systèmes de détection des intrusions (« **IDS** ») cloud si vous conservez des Données personnelles ou confidentielles Microsoft ; ▪ requiert l'implémentation de systèmes de protection contre les intrusions (« **IPS** ») configurés pour surveiller et empêcher activement la perte de données ; ▪ en cas de violation du système, requiert l'analyse de ce dernier pour résoudre tous les problèmes de vulnérabilité restants ; ▪ requiert une description des procédures de surveillance du système avec les outils de détection ; et ▪ requiert la mise en place d'un processus de gestion et de réponse aux incidents à suivre lorsque des événements de Violation des données sont détectés.	IDS/IPS documentés déployés avec les procédures en place pour orienter la réponse en cas de détection d'une vulnérabilité ou d'une violation des données.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
46	Communiquer rapidement à la direction et à Microsoft les résultats de l'enquête en réponse à l'incident. *Contacter SSPAHelp@microsoft.com pour prévenir Microsoft.*	Des systèmes et des processus doivent être en place pour communiquer à Microsoft les résultats de l'enquête en réponse à l'incident.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section J : Sécurité (suite)		
47	Les administrateurs système, le personnel des opérations, la direction et les tiers doivent suivre une formation de sécurité annuelle.	Mettre en place un programme de formation en sécurité qui comprend les éléments suivants : ▪ Formation annuelle en matière de réponse aux incidents. ▪ Simulation d'événements et de mécanismes automatisés pour améliorer l'efficacité des réponses en cas de crise. Sensibilisation à la prévention des incidents, notamment en matière de risques associés au téléchargement de logiciels malveillants.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
48	Le fournisseur doit s'assurer que des processus de planification de sauvegarde protègent les Données personnelles et confidentielles Microsoft contre les utilisations, accès, divulgations, modifications et destructions non autorisés.	Le fournisseur peut prouver qu'il documente les procédures de réponse et de récupération détaillant la manière dont l'organisation gérera un événement perturbateur et assurera un certain niveau (prédéfini) de sécurité pour ses informations en fonction des objectifs de continuité de la sécurité des informations approuvés par la direction. Le fournisseur peut prouver qu'il a défini et mis en œuvre des procédures pour sauvegarder périodiquement, stocker en sécurité et récupérer efficacement les données critiques.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section J : Sécurité (suite)		
49	Mettre en place et tester des plans de continuité des activités et de récupération d'urgence.	Un plan de récupération d'urgence doit inclure tous les éléments suivants. ▪ Définition de critères pour déterminer si un système est critique au fonctionnement des activités du fournisseur. ▪ Établissement d'une liste des systèmes critiques (en fonction des critères définis) à récupérer en priorité en cas d'urgence. ▪ Définition d'une procédure de récupération d'urgence pour chaque système critique afin que les ingénieurs qui ne connaissent pas le système puissent récupérer l'application en 72 heures. ▪ Test et examen des plans de récupération d'urgence annuels (ou plus fréquents) pour s'assurer que les objectifs de récupération sont réalisables.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
50	Authentifier l'identité d'une personne avant de lui permettre d'accéder aux Données personnelles et confidentielles Microsoft.	Vérifier que tous les identifiants des utilisateurs sont uniques et qu'ils utilisent une méthode d'authentification standard comme Azure Active Directory. Un accès élevé (privilèges administratifs ou avancés) nécessite un second facteur, comme un authentificateur utilisant une carte à puce ou un téléphone.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section J : Sécurité (suite)		
51	Le fournisseur doit protéger les Données personnelles et confidentielles Microsoft en transit sur les réseaux avec un chiffrement reposant sur des certificats « **TLS** » (Transport Layer Security) ou « **IPsec** » (Internet Protocol Security). Ces méthodes sont décrites dans les normes NIST 800-52 et NIST 800-57 ; une norme industrielle équivalente peut également être utilisée. Le fournisseur doit refuser la remise de Données personnelles ou confidentielles Microsoft transmises de façon non chiffrée.	Le processus de création, de déploiement et de remplacement de certificats TLS ou autres doit être défini et appliqué.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
52	Tous les appareils du fournisseur (ordinateurs portables, stations de travail, etc.) qui accéderont à des Données personnelles ou confidentielles Microsoft ou les traiteront doivent utiliser le chiffrement sur disque.	Utiliser la spécification BitLocker ou une autre solution de chiffrement de disque équivalente pour chiffrer tous les appareils clients utilisés afin de gérer des Données personnelles ou confidentielles de Microsoft.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section J : Sécurité (suite)		
53	Des systèmes et des procédures (avec des normes industrielles actuelles comme décrit dans la norme NIST 800-111) doivent être mis en place pour chiffrer les Données personnelles et/ou confidentielles Microsoft au repos (lorsqu'elles sont stockées), y compris les suivantes : ▪ les données d'identification (par ex., noms d'utilisateur/mots de passe) ; ▪ les données des moyens de paiement (par ex., numéros de carte de crédit ou de compte bancaire) ; ▪ les données personnelles liées à l'immigration ; ▪ les données des profils médicaux (par ex., les numéros de dossier médical ou les marqueurs et identifiants biométriques, comme l'ADN, les empreintes digitales, les rétines et iris, les empreintes vocales, la structure des visages, les mesures de la main, utilisés à des fins d'authentification) ▪ les données d'identification émises par le gouvernement (par ex., numéros de sécurité sociale ou de permis de conduire) ▪ données appartenant à des clients Microsoft (p. ex., Sharepoint, documents O365, clients One Drive) ; ▪ documentation liée aux produits Microsoft non annoncés ; ▪ date de naissance ; ▪ informations de profil des enfants ; ▪ données géographiques en temps réel ; ▪ adresse physique personnelle (non professionnelle) ; ▪ numéros de téléphone personnels (non professionnels) ; ▪ religion ; ▪ opinions politiques ; ▪ orientation/préférence sexuelle ; ▪ réponses aux questions de sécurité (p. ex., 2fa, réinitialisation de mot de passe) o nom de jeune femme de la mère.	Vérifier que les Données personnelles et confidentielles Microsoft répertoriées dans cette ligne sont chiffrées au repos.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
54	Lors du traitement de cartes de crédit au nom de Microsoft, respecter les normes de traitement des cartes de crédit applicables en fonction de l'émetteur de la carte.	Prouver la conformité en fournissant chaque année une certification **PCI-DSS** (Payment Card Industry Data Services Standard). *Envoyer la certification PCI DSS à SSPA. Contacter*	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*

		SSPAHelp@microsoft.com en cas de questions.	

N°	Exigences en matière de protection des données destinées aux fournisseurs de Microsoft	Preuve de conformité	Réponse
	Section J : Sécurité (suite)		
55	Le fournisseur doit stocker les ressources physiques de Microsoft dans un environnement où les accès sont contrôlés.	Des systèmes et des processus doivent être mis en place pour gérer l'accès physique aux copies numériques, papier et sauvegardes des données Microsoft. La chaîne de responsabilité doit être suivie pour le déplacement et la destruction de supports physiques contenant des données Microsoft.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*
56	Rendre anonyme toutes les Données personnelles Microsoft utilisées dans un environnement de développement ou de test.	Les Données personnelles Microsoft ne doivent pas être utilisées dans des environnements de développement ou de test ; si cela n'est pas possible, elles doivent être suffisamment anonymes pour empêcher l'identification des Personnes concernées ou toute utilisation malintentionnée. Remarque : les données anonymisées sont différentes des données pseudonymisées. Les données anonymisées sont des données qui ne concernent pas une personne physique identifiée ou identifiable lorsque la personne concernée par les données à caractère personnel n'est pas ou plus identifiable.	*<Conforme>* *<Non conforme>* *<Non applicable>* *<Conflit légal>* *<Conflit contractuel>*