ISO/IEC 27018:2025, Sécurité de l'information, cybersécurité et protection de la vie privée : Lignes directrices pour la protection des informations personnellement identifiables (IPI) dans les nuages publics agissant en tant que sous-traitants d'IPI (3e édition, 2025-08)

Protection des IPI dans le nuage public

36 exigences. Il n'existe pas de certificat accrédité pour cette norme. Version de 07/2026.

ISO/IEC 27018 n'est pas une norme de système de management, mais un ensemble de lignes directrices avec des mesures complémentaires venant s'ajouter à ISO/IEC 27002:2022. Il n'existe pas de certificat accrédité autonome pour ISO/IEC 27018. Les mesures sont intégrées à la déclaration d'applicabilité d'un système ISO/IEC 27001, et le certificat est alors délivré au titre d'ISO/IEC 27001 avec une référence à ISO/IEC 27018. La norme s'adresse au fournisseur d'un service de nuage public qui traite des informations personnellement identifiables pour le compte de ses clients du service en nuage. Une organisation qui se contente de consommer des services en nuage n'endosse pas ce rôle et doit évaluer raisonnablement les exigences vis-à-vis de ses fournisseurs, et non vis-à-vis d'elle-même. Pour Leanshift, cette liste de contrôle est donc avant tout une grille d'évaluation des fournisseurs. Chaque point peut être posé au fournisseur sous forme de question et sécurisé par le contrat de sous-traitance au titre de l'article 28 du RGPD. Le résultat d'une telle évaluation est un enregistrement interne de conformité ou un profil d'évaluation du fournisseur, et non un certificat. Sur la numérotation : les articles A.2 à A.12 suivent les principes de protection de la vie privée de l'annexe A de la norme, les points numérotés comme A.11.6 sont les mesures complémentaires qui y sont énumérées. Les points numérotés comme 8.10 ou 5.34 renvoient à des mesures d'ISO/IEC 27002:2022 que la norme précise pour le nuage. Les points portant le suffixe "(Grundsatz)", qui signifie principe, découlent du principe de l'article lui-même, lorsque l'annexe A ne prévoit pas de mesure complémentaire dédiée.

Entreprise	Date	Établi par

A.2 Consentement et choix 2

A.2.1 **Le fournisseur du service en nuage aide le client du service en nuage à répondre aux droits des personnes concernées, tels que l'accès, la rectification, l'effacement et l'opposition. Les responsabilités et les délais sont fixés contractuellement.** Document

Comment le prouver: Comme preuve sert le contrat de sous-traitance au titre de l'article 28 du RGPD avec une clause d'assistance pour l'exercice des droits des personnes concernées, ainsi que les moyens techniques du service lui-même : fonctions d'exportation, de correction et de suppression, ou une procédure de support documentée avec un délai de réponse. Question au fournisseur : quelle fonction ou quelle procédure proposez-vous pour que nous puissions traiter une demande d'accès ou d'effacement dans un délai d'un mois ?

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.2 (Grundsatz) **Les informations personnellement identifiables des clients du service en nuage ne sont traitées que sur instructions documentées du client. L'obtention du consentement des personnes concernées reste la tâche du client en sa qualité de responsable du traitement, et le fournisseur ne s'y substitue pas.**

Comment le prouver: Comme preuve sert la clause d'instructions du contrat de sous-traitance, ainsi que la preuve que le fournisseur ne fait aucun usage secondaire des données, par exemple la politique de confidentialité du service et la documentation produit. Question au fournisseur : traitez-vous les données de nos clients d'une quelconque manière en dehors de nos instructions, par exemple pour l'amélioration du produit ou l'entraînement de modèles ?

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.3 Légitimité et spécification de la finalité 2

A.3.1 **La finalité pour laquelle le fournisseur traite les informations personnellement identifiables se limite à la fourniture du service convenu et est indiquée dans le contrat. Aucun traitement pour les finalités propres du fournisseur n'a lieu.** Document

Comment le prouver: Comme preuve sert le contrat de sous-traitance précisant l'objet, la nature, la finalité et la durée du traitement, ainsi que les catégories de personnes concernées au titre de l'article 28.3 du RGPD. Question au fournisseur : veuillez fournir l'annexe contractuelle décrivant de manière exhaustive la finalité du traitement. Pour les petites structures, l'avenant standard de sous-traitance des données du fournisseur suffit, à condition qu'il contienne ces informations.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.3.2 **Les informations personnellement identifiables confiées au fournisseur ne sont pas utilisées à des fins publicitaires, marketing ou à d'autres fins commerciales propres au fournisseur sans consentement exprès préalable. La fourniture du service n'est pas subordonnée à un tel consentement.**

Comment le prouver: Comme preuve sert une clause contractuelle explicite excluant tout usage commercial secondaire, ainsi que les conditions de service. Question au fournisseur : confirmez par écrit que les données clients ne sont pas utilisées à des fins publicitaires, de profilage ou d'entraînement de modèles d'IA. En l'absence de cet engagement, le service ne convient pas au traitement d'informations personnellement identifiables.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.4 Limitation de la collecte 1

A.4 (Grundsatz) **Au-delà des données que le client introduit dans le service, le fournisseur ne collecte pas d'informations personnellement identifiables supplémentaires pour ses propres finalités, telles que la télémétrie, les profils d'utilisation ou l'analyse de contenu. Les données opérationnelles et les métadonnées collectées sont identifiées et justifiées.**

Comment le prouver: Comme preuve sert une liste des données que le service enregistre en plus des données de contenu (journaux d'accès, télémétrie, données de diagnostic) avec leur finalité et leur durée de conservation, ainsi qu'une capture d'écran du paramètre permettant de désactiver la télémétrie optionnelle. Question au fournisseur : quelles données d'utilisation, de télémétrie et de diagnostic collectez-vous en plus, à quoi servent-elles, et pouvons-nous désactiver cette collecte ?

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5 Minimisation des données 2

A.5.1 **Les fichiers temporaires créés lors du traitement d'informations personnellement identifiables, tels que le stockage provisoire, les caches ou les journaux d'annulation, sont supprimés de manière sécurisée dans un délai défini.**

Comment le prouver: Comme preuve sert une procédure d'exploitation ou de suppression avec un délai de conservation défini pour les données temporaires, étayée par la configuration du système, par exemple une durée de vie de cache (TTL) ou une tâche de nettoyage planifiée avec son journal d'exécution. Question au fournisseur : au bout de quel délai les caches, les fichiers temporaires et les états intermédiaires sont-ils supprimés, et comment cela est-il contrôlé ?

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

8.11 **Dès lors que l'exploitation, les tests ou le support ne nécessitent pas de données réelles, les informations personnellement identifiables sont masquées, pseudonymisées ou anonymisées. Le volume de données traitées reste limité à ce dont le service a réellement besoin.**

Comment le prouver: Comme preuve sert une règle déterminant quels environnements peuvent voir des données réelles, ainsi que des captures d'écran ou des scripts du masquage utilisé dans les systèmes de test et de développement. Question au fournisseur : vos équipes de support et de développement travaillent-elles avec des données de production et, le cas échéant, avec quelles garanties ? Pour les petites structures, il suffit d'avoir une règle selon laquelle les systèmes de test fonctionnent exclusivement avec des données d'exemple générées.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.6 Limitation de l'utilisation, de la conservation et de la divulgation 3

A.6.1 **Lorsque le fournisseur reçoit une demande juridiquement contraignante de divulgation d'informations personnellement identifiables, par exemple de la part d'une autorité publique, il en informe au préalable le client du service en nuage, dans la mesure où la loi le permet.**

Comment le prouver: Comme preuve sert une clause contractuelle de notification et un processus interne pour les demandes des autorités avec un responsable désigné. Question au fournisseur : nous informez-vous avant de transmettre des données, et publiez-vous un rapport de transparence sur les demandes des autorités ? Un rapport de transparence à jour constitue une preuve solide.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.6.2 **Lorsque le fournisseur divulgue des informations personnellement identifiables à des tiers, il enregistre l'événement de manière traçable : qui a reçu les données, quand cela s'est produit, quelles données étaient concernées et sur quelle base repose la divulgation.** Document

Comment le prouver: Comme preuve sert un registre des divulgations ou un historique de tickets comportant ces champs, même s'il ne contient aucune entrée. Un registre vide mais tenu à jour est acceptable et constitue la solution pratique pour les petites structures. Question au fournisseur : tenez-vous un registre des divulgations de données, et pouvons-nous en obtenir des extraits ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

8.10 **Les informations personnellement identifiables sont supprimées une fois le délai de conservation convenu écoulé ou le contrat terminé, y compris les copies conservées dans les sauvegardes après leur cycle de rotation.**

Comment le prouver: Comme preuve sert un concept de suppression avec des délais de conservation par catégorie de données, la durée de conservation des sauvegardes et un journal ou une confirmation de suppression. Question au fournisseur : combien de temps nos données subsistent-elles dans vos sauvegardes après résiliation, et recevons-nous une confirmation écrite de leur suppression ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.7 Exactitude et qualité 2

A.7 (Grundsatz) **Le fournisseur ne modifie pas de sa propre initiative les informations personnellement identifiables qui lui sont confiées. Les corrections et mises à jour ne sont effectuées que sur instruction du client du service en nuage ou au moyen de fonctions que le client exploite lui-même.**

Comment le prouver: Comme preuve servent les fonctions d'édition du service ainsi que leur historique de modifications, ainsi que la clause d'instructions du contrat de sous-traitance. Question au fournisseur : pouvons-nous corriger les enregistrements nous-mêmes, et chaque modification est-elle journalisée de manière traçable ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

8.13 **L'intégrité des informations personnellement identifiables est protégée lors du stockage, de la transmission et de la restauration. Des sauvegardes existent et leur capacité de restauration a été testée.**

Comment le prouver: Comme preuve sert la configuration des sauvegardes, les mécanismes de somme de contrôle ou d'intégrité, et au moins un test de restauration documenté par an avec date et résultat. Question au fournisseur : à quelle fréquence testez-vous les restaurations, et quel délai de rétablissement garantissez-vous dans le niveau de service ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8 Ouverture, transparence et information 2

A.8.1 **Le recours à des sous-traitants ultérieurs traitant des informations personnellement identifiables est communiqué avant la conclusion du contrat. Les modifications de la liste sont notifiées au client en temps utile, afin qu'il puisse s'y opposer ou résilier le contrat.** Document

Comment le prouver: Comme preuve sert une liste à jour des sous-traitants ultérieurs, publiée ou mise à disposition contractuellement, avec nom, pays et finalité du traitement, ainsi qu'une règle de notification au titre de l'article 28.2 du RGPD. Question au fournisseur : où trouvons-nous votre liste de sous-traitants ultérieurs, avec quel délai de préavis notifiez-vous les changements, et comment pouvons-nous nous y opposer ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8 (Grundsatz) **Avant la conclusion du contrat, le fournisseur met à disposition des informations compréhensibles sur la manière dont les informations personnellement identifiables sont traitées, les garanties en place et les juridictions dans lesquelles le traitement a lieu.**

Comment le prouver: Comme preuve servent la politique de confidentialité, un livre blanc sur la sécurité, une page de centre de confiance et le contrat de sous-traitance incluant les mesures techniques et organisationnelles en annexe. Question au fournisseur : veuillez fournir la liste actuelle des mesures techniques et organisationnelles en annexe contractuelle, et non un simple support marketing.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.9 Participation individuelle et accès 2

A.9 (Grundsatz) **Le service met à la disposition du client du service en nuage les moyens techniques permettant de traiter lui-même les demandes d'accès, de rectification et d'effacement des personnes concernées, par exemple au moyen de fonctions d'exportation, de recherche et de suppression.**

Comment le prouver: Comme preuve sert la documentation produit des fonctions d'exportation et de suppression, étayée par un essai interne : traiter une demande d'accès de bout en bout et noter le temps nécessaire. Question au fournisseur : pouvons-nous retrouver, exporter et supprimer toutes les données d'une seule personne sans votre support ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

5.34 **Lorsque le client ne peut pas traiter lui-même une demande d'une personne concernée, le fournisseur apporte son assistance dans un délai convenu. Les demandes que les personnes concernées adressent directement au fournisseur sont transmises au client plutôt que d'être traitées par le fournisseur.**

Comment le prouver: Comme preuve sert la clause correspondante du contrat de sous-traitance avec un délai de réponse concret, ainsi qu'un historique de tickets de support à titre d'exemple réel. Question au fournisseur : quel délai garantissez-vous pour l'assistance à l'exercice des droits des personnes concernées, et quel en est le coût ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.10 Responsabilité 4

A.10.1 **Les violations touchant des informations personnellement identifiables sont signalées au client du service en nuage sans délai injustifié, en indiquant l'ampleur, les données concernées, la cause et les mesures prises. Un processus de notification avec responsabilités et délais est défini.** Document

Comment le prouver: Comme preuve sert le plan de réponse aux incidents avec sa chaîne d'escalade, le délai contractuel de notification (24 à 48 heures fonctionnent en pratique, afin que le client puisse encore respecter le délai de 72 heures de l'article 33 du RGPD) et les enregistrements d'incidents passés ou d'un exercice. Question au fournisseur : dans quel délai signalez-vous un incident, par quel canal, et quelles informations fournissez-vous à cette occasion ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.10.2 **Les politiques de sécurité, les procédures d'exploitation et les enregistrements correspondants sont conservés pendant un délai défini, afin que le traitement puisse être reconstitué a posteriori.** Document

Comment le prouver: Comme preuve sert une règle de conservation avec l'historique des versions des politiques, par exemple au moyen d'un registre documentaire ou d'un système de gestion de versions comportant la date d'approbation. Question au fournisseur : pendant combien de temps conservez-vous les versions des politiques et les enregistrements correspondants, et y avons-nous accès en cas d'audit ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.10.3 **Un dispositif défini existe pour la restitution, le transfert et la destruction des informations personnellement identifiables à la fin du contrat, précisant les formats, les délais et le traitement des copies.** Document

Comment le prouver: Comme preuve sert la clause de sortie du contrat de sous-traitance ainsi qu'une confirmation de suppression après la fin du contrat. Question au fournisseur : sous quel format et dans quel délai récupérons-nous nos données, quand toutes les copies sont-elles détruites, et recevons-nous une confirmation écrite ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

5.35 **L'efficacité des garanties est examinée de manière indépendante à intervalles réguliers, par exemple au moyen d'audits internes, de tests d'intrusion ou de rapports d'assurance de tiers. Les résultats sont mis à la disposition du client du service en nuage sous une forme appropriée.**

Comment le prouver: Comme preuve sert un certificat ISO/IEC 27001 avec une déclaration d'applicabilité incluant les mesures d'ISO/IEC 27018, ou un rapport SOC 2, ainsi que des synthèses récentes de tests d'intrusion. Question au fournisseur : veuillez fournir le certificat, son périmètre et la confirmation qu'ISO/IEC 27018 est reflété dans la déclaration d'applicabilité. Vérifiez si le périmètre couvre réellement le service que vous utilisez.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.11 Sécurité de l'information 13

A.11.1 **Toute personne ayant accès à des informations personnellement identifiables est tenue à la confidentialité, qu'elle soit employée directement ou engagée en externe.** Document

Comment le prouver: Comme preuve servent les accords ou engagements de confidentialité signés qui restent en vigueur après la fin de la relation. Question au fournisseur : l'ensemble du personnel et des prestataires ayant accès aux données sont-ils tenus à la confidentialité par écrit ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.11.2 **Les impressions et autres copies papier contenant des informations personnellement identifiables ne sont réalisées que lorsque cela est strictement nécessaire. L'étendue autorisée est régie par une règle.**

Comment le prouver: Comme preuve sert une règle sur le traitement des impressions, qui dans les centres de données consiste typiquement en une interdiction générale d'imprimer dans les zones hébergeant des données clients. Question au fournisseur : des données clients sont-elles imprimées dans le cadre de votre exploitation et, le cas échéant, sous quelles conditions ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.11.3 **Les restaurations à partir de sauvegardes sont autorisées au préalable et journalisées, y compris la personne à l'origine de la restauration et les données concernées.** Document

Comment le prouver: Comme preuve sert le journal des restaurations avec horodatage, origine et périmètre, généralement produit automatiquement par l'outil de sauvegarde. Question au fournisseur : journalisez-vous chaque restauration, et pouvons-nous consulter ces journaux en cas d'audit ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.11.4 **Les supports de stockage contenant des informations personnellement identifiables qui quittent les locaux sont protégés contre les accès non autorisés et la perte, en règle générale par chiffrement et un relevé de transport.**

Comment le prouver: Comme preuve sert la preuve du chiffrement (chiffrement intégral du support), les relevés de transport et de remise, et un inventaire des supports. Question au fournisseur : des supports contenant des données clients quittent-ils jamais vos sites, par exemple pour des sauvegardes, et comment sont-ils protégés pendant le transport ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.11.5 **L'utilisation de supports et d'appareils portables non chiffrés pour des informations personnellement identifiables est interdite ou limitée à des exceptions justifiées avec approbation documentée.**

Comment le prouver: Comme preuve sert une politique relative aux supports amovibles ainsi que son application technique, par exemple le chiffrement obligatoire des appareils ou le blocage des ports USB par gestion des appareils. Question au fournisseur : le personnel peut-il copier des données clients sur des appareils non chiffrés, et qu'est-ce qui l'empêche techniquement ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.11.6 **Les informations personnellement identifiables transmises sur des réseaux publics sont chiffrées. Les mécanismes utilisés reflètent l'état de l'art.**

Comment le prouver: Comme preuve sert la configuration TLS (version de protocole actuelle, sans chiffrements obsolètes) et un test de configuration externe consigné dans un rapport. Pratique pour les petites structures : effectuer une analyse TLS gratuite une fois par an et archiver le résultat. Question au fournisseur : quel chiffrement de transport appliquez-vous de manière obligatoire, et le chiffrement au repos est-il actif ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.11.7 **Les documents papier contenant des informations personnellement identifiables sont détruits de manière à exclure toute reconstitution.**

Comment le prouver: Comme preuve servent des destructeurs de papier d'un niveau de sécurité adéquat ou des certificats de destruction d'un prestataire travaillant selon la norme DIN 66399 ou une norme équivalente. Question au fournisseur : comment détruisez-vous les documents papier relatifs aux clients, et des certificats de destruction sont-ils archivés ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.11.8 **Les identifiants d'utilisateur sont attribués de manière exclusive à une personne et ne sont ni réattribués ni partagés. Les comptes partagés n'existent que dans des exceptions justifiées et avec une traçabilité supplémentaire.**

Comment le prouver: Comme preuve sert une liste d'utilisateurs du système d'identité exempte de comptes de groupe, ainsi que la règle selon laquelle les tâches administratives sont effectuées depuis un compte personnel. Question au fournisseur : votre personnel d'exploitation travaille-t-il avec des comptes personnels, et l'authentification multifacteur est-elle obligatoire ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.11.9 **Le fournisseur peut indiquer à tout moment quelles personnes ou quels rôles sont autorisés à accéder aux informations personnellement identifiables, et tient cette vue d'ensemble à jour.** Document

Comment le prouver: Comme preuve sert un aperçu des droits d'accès par rôle, étayé par une revue périodique des accès avec date et résultat. Pour les petites structures, un export semestriel de la liste des utilisateurs, validé, suffit. Question au fournisseur : combien de vos collaborateurs peuvent accéder à nos données, et à quelle fréquence le vérifiez-vous ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.11.10 **Les comptes utilisateurs sont gérés sur l'ensemble de leur cycle de vie : création, modification et désactivation rapide en cas de départ ou de changement de fonction.**

Comment le prouver: Comme preuve sert une procédure d'arrivée et de départ avec une liste de contrôle, ainsi que des journaux de comptes désactivés avec horodatage. Question au fournisseur : dans quel délai retirez-vous l'accès au personnel qui quitte l'entreprise, et comment le prouvez-vous ?

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.11.11 **Les obligations de sécurité et de protection de la vie privée du fournisseur sont fixées contractuellement, y compris les mesures techniques et organisationnelles, le caractère contraignant des instructions du client et le droit d'audit du client.** Document

Comment le prouver: Comme preuve sert le contrat de sous-traitance signé au titre de l'article 28 du RGPD avec l'annexe des mesures et un droit d'audit ou d'information. Question au fournisseur : veuillez fournir le contrat de sous-traitance signé, annexes comprises, et non un simple renvoi aux conditions générales de service.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.11.12 **Les sous-traitants ultérieurs qui traitent des informations personnellement identifiables sont soumis au moins aux mêmes obligations que le fournisseur lui-même. Leur sélection et leur suivi continu sont régis par un processus défini.**

Comment le prouver: Comme preuve sert la répercussion des obligations dans les contrats avec les sous-traitants ultérieurs (article 28.4 du RGPD) et une évaluation des fournisseurs avec une date. Question au fournisseur : comment évaluez-vous vos sous-traitants ultérieurs, et quelles preuves leur exigez-vous ?

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.11.13 **Avant la réutilisation d'un espace de stockage, il est garanti qu'aucune donnée des utilisateurs précédents ne reste accessible, ni sur les supports physiques ni dans les environnements virtualisés.**

Comment le prouver: Comme preuve sert la procédure d'assainissement ou d'effacement appliquée lors de la libération du stockage, les enregistrements de destruction des supports, et la séparation entre clients décrite dans le document d'architecture. Question au fournisseur : comment garantissez-vous qu'un espace de stockage réutilisé ne conserve aucune donnée résiduelle d'autres clients ?

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.12 Conformité en matière de protection de la vie privée 3

A.12.1 **Les pays dans lesquels les informations personnellement identifiables sont stockées et traitées sont indiqués et connus du client du service en nuage. Les modifications des lieux de stockage sont notifiées.** Document

Comment le prouver: Comme preuve sert l'aperçu des sites et régions du fournisseur, dans le contrat ou dans la documentation, ainsi qu'une capture d'écran du paramètre de région du service utilisé. Question au fournisseur : dans quels pays nos données sont-elles stockées, depuis quels pays y accède-t-on, par exemple pour le support, et pouvons-nous fixer la région ?

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.12.2 **Les transferts d'informations personnellement identifiables vers des pays tiers sont connus, justifiés et couverts par des garanties appropriées.** Document

Comment le prouver: Comme preuve servent les clauses contractuelles types ou une décision d'adéquation, étayées par une analyse d'impact relative au transfert, qui peut être brève pour les petites structures : catégories de données concernées, pays de destination, risque, mesures supplémentaires prises. Question au fournisseur : sur quelle base juridique transférez-vous des données vers des pays tiers, et quelles mesures supplémentaires appliquez-vous ?

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

5.31 **Les exigences légales et contractuelles applicables au traitement des informations personnellement identifiables sont identifiées et tenues à jour à mesure que la situation juridique évolue. Les juridictions concurrentes sont évaluées.**

Comment le prouver: Comme preuve sert un aperçu des exigences applicables (RGPD, règles nationales, obligations sectorielles) avec un responsable et une date de révision. Dans une petite structure, une liste d'une page révisée annuellement suffit. Question au fournisseur : vous-même ou vos sous-traitants ultérieurs êtes-vous soumis à des juridictions permettant aux autorités d'accéder à nos données, et comment gérez-vous cela ?

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification