POLITIQUE DE CONFIDENTIALITÉ MEDAVIZ

CONFORMITÉ RGPD HDS ISO

V5.0 AVRIL 2023 – DIFFUSION PUBLIQUE

Toute utilisation des Services Medaviz est soumise au préalable à la prise de connaissance et à l'acceptation expresse de notre Politique de confidentialité .

NOTRE POLITIQUE DE CONFIDENTIALITÉ EN UN COUP D'ŒIL

Le respect de la vie privée des Utilisateurs est un droit fondamental et l'une des valeurs essentielles de Medaviz. Les informations qui touchent à leur santé sont personnelles. À ce titre, elles doivent être protégées avec le plus grand soin.

Medaviz est certifié ISO-27001 et Hébergeur de Données de Santé (HDS). Medaviz s'engage à traiter l'ensemble des données collectées et conservées de manière conforme à la Réglementation en vigueur sur la protection des données à caractère personnel.

Par la présente Politique de confidentialité, Medaviz informe les Utilisateurs de la manière dont Medaviz et les Praticiens traitent les données à caractère personnel, décrit les mesures de sécurité mises en œuvre ainsi que les engagements pris dans le respect de la Réglementation en vigueur.

En fonction des données à caractère personnel traitées, Medaviz est susceptible d'agir soit en qualité de Responsable de traitement pour le compte des Utilisateurs, soit en qualité de Sous-traitant pour le compte de ses Partenaires et des Praticiens.

1. DÉFINITIONS

Les termes ci-après définis ont le sens et la portée donnés dans leur définition dans le cadre de la présente Politique de confidentialité.

Donnée à caractère personnel désigne une information qui permet d'identifier une personne physique directement (par exemple son nom/prénom), ou indirectement (par exemple son numéro de téléphone, son numéro de contrat, son pseudo).

Donnée à caractère personnel de santé désigne une information relative à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèle une information sur l'état de santé de cette personne.

Partenaire désigne toute organisation avec laquelle Medaviz signe un contrat de partenariat, qu'il soit commercial ou autre.

Personne concernée désigne celle qui peut être identifiée par les données utilisées dans le cadre du traitement de données à caractère personnel.

Réglementation désigne le Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 (le « Règlement Général sur la Protection des Données » ou « RGPD ») et de la loi n°78-17 du 6 janvier 1978 modifiée par la loi du 20 juin 2018 relative à l'informatique, aux fichiers et aux libertés .

Responsable de traitement désigne celui qui décide de la manière dont sera mis en œuvre le traitement des données à caractère personnel, notamment en déterminant à quoi vont servir les données et quels outils vont être mis en œuvre pour les traiter.

Sous-traitant désigne celui qui effectue des opérations sur les données pour le compte du responsable de traitement, qui lui confie certaines tâches et qui s'assure qu'il dispose des garanties techniques et organisationnelles, lui permettant de traiter les données à caractère personnel qui lui sont confiées conformément à la Réglementation.

Traitement de données à caractère personnel désigne une opération ou un ensemble organisé d'opérations effectué sur des données à caractère personnel (collecte, structuration, conservation, modification, communication...).

Utilisateur(s) désigne toute personne physique utilisant les Services Medaviz après création de son Compte personnel et acceptation de la présente Politique de confidentialité.

2. LE CONSENTEMENT DES PERSONNES CONCERNÉES

A. CONSENTEMENT PRÉALABLE

Les traitements de données à caractère personnel sont mis en œuvre par Medaviz au titre de la fourniture des Services Medaviz, à partir du recueil du consentement explicite et exprès de la personne concernée. Il se traduit par l'acceptation des Conditions Générales d'Utilisation (CGU) ou des Conditions Générales de Services (CGS) et de la Politique de Confidentialité par l'utilisateur.

Chaque Utilisateur peut retirer son consentement à tout moment, en adressant sa demande à l'adresse suivante : contact@medaviz.com. Dans ce cas, vous ne pourrez plus bénéficier des Services Medaviz.

B. CONSENTEMENT ACTES DE TÉLÉMÉDECINE

Le consentement à la pratique de la téléconsultation et à la collecte des données de santé est requis avant chaque mise en relation avec un Praticien.

3. COMBIEN DE TEMPS LES DONNÉES À CARACTÈRE PERSONNEL SONT-ELLES CONSERVÉES ?

A. DONNÉES D'IDENTIFICATION

Toutes les données à caractère personnel collectées sont traitées et conservées pour une durée limitée en fonction de la finalité du traitement et de la Réglementation applicable aux Services. Medaviz détermine les durées de conservation des données à caractère personnel en sa qualité de Responsable de Traitement. Il s'agit des données à caractère personnel d'identification et elles sont conservées pendant la durée de la relation contractuelle avec Medaviz. Elles seront supprimées au plus tard 3 mois après la demande de fermeture du compte.

Pour des raisons de sécurité, en cas d'inactivité d'un compte supérieure à 60 mois, Medaviz le supprimera après information préalable de l'Utilisateur. (cf. Conditions Générales d'Utilisation ou Conditions Générales de Services).

B. DONNÉES DE SANTÉ

Par mesure de sécurité, Medaviz supprime également :

- toutes les données de santé collectées par les Praticiens au cours de la mise en relation avec le patient, à la clôture du compte ;
- tous les enregistrements réalisés dans le cadre du contrôle qualité du service 24h/7j après 4 mois. Tous les Utilisateurs sont informés que la conversation téléphonique est enregistrée ;
- tous les documents émis par un Praticien ou un Patient après 24 mois de la base active. Ils font l'objet d'un archivage intermédiaire sur un serveur HDS indépendant, conformément à la réglementation en vigueur.

Afin de se conformer aux obligations légales d'archivage s'imposant aux Praticiens, ceux-ci sont susceptibles de conserver, sur leurs propres outils, les données à caractère personnel des Utilisateurs pour des durées plus longues que celles indiquées ci-dessus.

En cas de demande de suppression du compte, Medaviz informera le Praticien de votre demande de suppression de votre compte et de toutes les données qu'il contient.

4. LES DROITS SUR LES DONNÉES À CARACTÈRE PERSONNELLES (HORS DONNÉES DE SANTÉ)

Conformément aux recommandations de la CNIL dont vous trouverez le lien à l'article LIENS UTILES ci-dessous, chaque personne concernée dispose des droits suivants :

- Droit d'accès : faculté de demander directement à Medaviz s'il détient des informations sur elle et qu'elles lui soient communiquées.
- Droit de rectification : faculté de rectifier les informations inexactes la concernant. Le droit de rectification complète le droit d'accès.
- Droit à l'oubli : faculté de demander l'effacement des informations la concernant, pour un motif prévu par la Réglementation.
- Droits à la limitation : faculté d'obtenir la limitation du traitement de ses données, pour un motif prévu par la Réglementation.
- Droit à la portabilité : faculté de demander à recevoir les données qu'elle a fournies à Medaviz, ou demander à Medaviz qu'elles soient transmises à un autre Responsable de traitement pour un motif prévu par la Réglementation.

La personne concernée peut également s'opposer, pour des raisons tenant à sa situation particulière, à ce que les données la concernant soient traitées, diffusées, transmises, conservées ou hébergées dans les conditions prévues par la Réglementation. Dans ce cas, l'Utilisateur reconnaît et accepte que Medaviz se trouve dans l'impossibilité de fournir les services de télémédecine, et sera donc dans l'obligation de supprimer le compte de l'Utilisateur ainsi que toutes les données personnelles qu'il contient.

Pour exercer les droits, la personne concernée peut contacter le délégué à la protection des données de Medaviz par email à l'adresse suivante : contact@medaviz.com. Pour faciliter les démarches, Medaviz invite chaque personne concernée, lors de l'envoi d'une demande d'exercice des droits, à :

- Indiquer quel(s) droit(s) elle souhaite exercer ;
- Mentionner clairement ses nom / prénom / numéro de téléphone associé au Compte personnel, coordonnées auxquels elle souhaite recevoir les réponses ;
- Nous transmettre des informations permettant une vérification de l'identité de la personne.

5. LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO)

Medaviz a désigné un délégué à la protection des données auprès de la CNIL afin de veiller au respect de la Réglementation et des règles décrites au sein de la présente Politique de confidentialité. Le délégué à la protection des données veille notamment :

- à établir et tenir à jour un registre des traitements de données à caractère personnel mis en œuvre dans l'entreprise ;
- à s'assurer de la conformité des pratiques avec la Réglementation et ses évolutions ;
- à sensibiliser l'ensemble des équipes aux exigences et bonnes pratiques en matière de protection des données à caractère personnel ;
- à l'exercice effectif des droits des personnes concernées.

Le délégué à la protection des données est joignable par mail à l'adresse suivante : contact@medaviz.com.

6. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

Chaque personne concernée dispose du droit d'introduire une réclamation auprès d'une autorité de contrôle de protection des données. En France, cette autorité est la

CNIL, voici ses coordonnées :
3 Place de Fontenoy, TSA 80715, 75334 PARIS CEDEX 07.
Tél. 01 53 73 22 22 – www.cnil.fr

7. LES RESPONSABLES DE TRAITEMENT

Au sens de la Réglementation, les personnes suivantes sont responsables des traitements des données collectées qui les concernent :

- Medaviz, au titre de la collecte des données à caractère personnel d'identification de l'Utilisateur (état civil, date de naissance et coordonnées), afin de vérifier l'éligibilité aux Services le cas échéant et de permettre la création de son Compte personnel.
- Tout Partenaire de Medaviz ayant conclu un contrat de mise à disposition des services Medaviz au profit de leurs bénéficiaires. À ce titre, elle traite les données à caractère personnel pour des finalités qui lui sont propres, distinctes de la finalité de mise en œuvre des Services Medaviz. Elle assume seule toute responsabilité à ce titre.
- Chaque Praticien ayant conclu un contrat avec Medaviz afin de proposer aux patients, des téléconsultations qu'il réalise en utilisant l'outil Medaviz. À ce titre, il traite les données à caractère personnel de santé des patients pour des finalités qui lui sont propres, distinctes de la finalité de mise en œuvre de l'outil. Il assume seul toute responsabilité à ce titre.
- Chaque Praticien ayant conclu un contrat de prestations médicales avec Medaviz afin de prodiguer les Services qu'il réalise en utilisant l'outil Medaviz. À ce titre, il traite les données à caractère personnel de santé des patients pour des finalités qui lui sont propres, distinctes de la finalité de mise en œuvre de l'outil. Il assume seul toute responsabilité à ce titre.

8. LES SOUS-TRAITANTS

La nature et la finalité des opérations sur les données sous-traitées lors des prestations est la maintenance et l'hébergement de la solution.

Les sous-traitants sont autorisés à traiter pour le compte des responsables de traitement les données à caractère personnel nécessaires pour fournir les Services Medaviz. Pour l'exécution des services, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes :

- la liste, les qualifications et les informations de contact des personnels du Partenaire intervenant dans le processus de maintenance et d'hébergement ;
- le cas échéant la liste, les qualifications et les informations de contact des personnels des autres sous-traitants du Partenaire intervenant dans le processus de maintenance et d'hébergement ;
- toutes les procédures, codes d'accès, moyens techniques ou physiques et tout autre documents utiles pour permettre l'exécution des prestations objet du contrat dans les meilleures conditions (télémaintenance, prise en main à distance, documentations techniques …);
- l'accès aux règlements du Partenaire.

A. MAINTENANCE LOGICIEL

Medaviz est responsable de la maintenance et du support des Services Medaviz. À ce titre, Medaviz agit en tant que Sous-traitant de toutes les données collectées. Les Sous-traitants de Medaviz agissent également en tant que Sous-traitant des données et se sont engagés à respecter tous les engagements pris par Medaviz.

B. HÉBERGEMENT DES DONNÉES

Se référer à l'article HÉBERGEURS DE DONNÉES DE SANTÉ (HDS) ci-dessous.

9. LES TRANSFERTS DE DONNÉES HORS UNION EUROPÉENNE

Transfert transfrontalier : Afin de fournir ses Services, Medaviz peut avoir recours à des prestataires se situant hors de l'Union européenne. Si le transfert a lieu vers un pays tiers dans lequel la législation n'a pas été reconnue comme offrant un niveau de protection adéquat des Données à caractère personnel, Medaviz veille à ce que les mesures adéquates soient mises en place conformément à la Loi Informatique et Libertés et au RGPD, et notamment, lorsque nécessaire à ce que des clauses contractuelles types (CCT) ou des clauses ad hoc équivalentes soient intégrées dans le contrat conclu entre Medaviz et le sous-traitant ultérieur.

Medaviz n'effectue aucun transfert de données de santé hors de l'Union Européenne. Certains de nos Sous-traitants ne disposent pas encore de centre de données basés dans l'Union Européenne mais ils ne traitent pas de données de santé. Medaviz a engagé des échanges avec ces derniers pour que des centres de données, localisés dans l'Union Européenne, soient disponibles. Parmi ces Sous-traitants :

- Twilio, services de téléphonie, VoIP, vidéo et messagerie pour l'intégration aux logiciels web et mobiles. La politique RGPD de ce prestataire comporte des Binding Corporate Rules (BCR) approuvés par les autorités européennes de protection des données.
- Stripe, prestataire de service de paiement, permet de gérer les paiements en ligne des téléconsultations. La politique RGPD de ce prestataire comporte des mesures supplémentaires au Privacy Shield fondé sur les EU Standard Contractual Clauses (SCCs, article 46 3 du RGPD). Garantie contre les transferts CCT (Clauses Contractuelles Types).

Conformément à notre page *Confidentialité et sécurité* dont vous trouverez le lien à l'article LIENS UTILES ci-dessous.

10. LA FINALITÉ DES TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL

Les traitements des données à caractère personnel collectées sont strictement nécessaires à l'accomplissement des activités et des services proposés

par Medaviz. Par ailleurs, les données collectées dans le cadre de l'utilisation de ces services pourront être traitées par Medaviz, après avoir été anonymisées, dans l'objectif de permettre à Medaviz d'améliorer les performances et les fonctionnalités de ses Services. Les données anonymisées pourront également être exploitées dans le cadre d'études ou d'évaluation dans le domaine de la santé, auxquelles Medaviz pourrait participer sauf opposition de l'Utilisateur.

LES DONNÉES À CARACTÈRE PERSONNEL NE SONT JAMAIS TRANSMISES À DES ORGANISATIONS EXTERNES, NOTAMMENT COMMERCIALES OU PUBLICITAIRES.

11. OBLIGATIONS DU RESPONSABLE DE TRAITEMENT VIS-À-VIS DU SOUS-TRAITANT

Le responsable de traitement s'engage à :

- fournir au Sous-traitant les données visées à l'article 7 des présentes clauses ;
- documenter par écrit toute instruction concernant le traitement des données par le sous-traitant ;
- veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le Règlement européen sur la protection des données de la part du sous-traitant ;
- à respecter la PGSSI-S (Politique Générale de Sécurité des Systèmes d'Information de Santé) de l'Agence du Numérique en Santé (ANS) et mettre en œuvre un système d'information de santé respectant cette PGSSI-S, dont vous trouverez le lien à l'article LIENS UTILES ci-dessous.

12. OBLIGATIONS DU SOUS-TRAITANT VIS-À-VIS DU RESPONSABLE DE TRAITEMENT

Medaviz respecte les principes suivants :

- Les données à caractère personnel sont utilisées uniquement pour des finalités explicites, légitimes et déterminées en lien direct avec l'activité de chaque Responsable de traitement ;
- Seules les données à caractère personnel strictement nécessaires sont collectées et traitées ;
- Les personnes concernées sont informées préalablement et régulièrement, de manière claire et transparente, notamment sur la finalité d'utilisation de leurs données, le caractère facultatif ou obligatoire de leurs réponses dans les formulaires, des droits dont ils disposent en matière de protection des données et des modalités d'exercice effectif de ces droits, des destinataires ;
- Chaque fois que la Réglementation l'impose, un consentement explicite, éclairé, actif et non équivoque de la personne concernée est recueilli au titre du traitement de ses données à caractère personnel ;
- Les données ne sont pas conservées par les différents responsables de traitement au-delà de la durée nécessaire pour les opérations pour lesquelles elles ont été collectées et ce en tenant compte de la nature des opérations, ou de celles prévues par les normes et autorisations de la CNIL ou par la loi ;
- Les données à caractère personnel ne sont pas communiquées ni cédées à des tiers, sauf aux destinataires autorisés dans le cadre strict des finalités préalablement définies ;
- Medaviz confie les données à caractère personnel à des prestataires Sous-traitants choisis en fonction de garanties techniques et organisationnelles appropriées, afin de garantir la protection des données qui leur sont confiées sous les instructions de Medaviz ;
- Medaviz et ses Sous-traitants sont engagés à veiller à toute violation éventuelle et exceptionnelle de données et à prendre toutes les mesures de protection et de correction consécutives à une violation en informant la CNIL et le cas échéant, les personnes concernées ;
- Medaviz s'engage à informer l'Utilisateur par tout moyen de toute demande de transmission de données confidentielles ou à caractère personnel à une autorité judiciaire ou administrative (UE ou hors UE), sauf à ce que cette notification soit interdite.
- Mettre en œuvre les mesures techniques et organisationnelles appropriées compte tenu de l'état des connaissances, des coûts, de la nature, de la portée, du contexte et des finalités des traitements afin de garantir un niveau de sécurité adapté aux risques.
- Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :
    - s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité,
    - reçoivent la formation nécessaire en matière de protection des données à caractère personnel,
    - font l'objet d'habilitations et de contrôles spécifiques pour traiter les données sensibles.
    - prennent en compte, en cas de modifications ou d'évolutions techniques de ses services, décidées par lui ou imposées par le cadre légal applicable, les principes de protection des données à caractère personnel et notamment de santé, dès la conception *Privacy by design,* ou par défaut *Privacy by default*,
    - mettent à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations.

13. HÉBERGEURS DE DONNÉES DE SANTÉ (HDS)

La sécurité des données porte sur les mesures prises afin de protéger les données de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées, ainsi que l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

A. PÉRIMÈTRE DU CERTIFICAT DE CONFORMITÉ

Afin de respecter les dispositions du Code de la santé publique concernant les Données à caractère personnel de Santé, Medaviz a recours à Amazon Web Services en tant qu'Hébergeur de Données de Santé (HDS) bénéficiant de la certification de l'Agence du Numérique en Santé (ANS) :

- Pilier 1 : mise à disposition et maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé (sous-traité à AWS) ;
- Pilier 2 : mise à disposition et maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé (sous-traité à AWS) ;
- Pilier 3 : mise à disposition et maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information (Medaviz) ;
- Pilier 4 : mise à disposition et maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé (sous-traité à AWS) ;
- Pilier 5 : administration et exploitation du système d'information contenant les données de santé (Medaviz).

Medaviz est certifié HDS depuis avril 2023 afin de couvrir les piliers 3 et 5 ci-dessus. La certification HDS valorise notre niveau de sécurité.

B. GARANTIES DES PRESTATIONS RÉALISÉES

Medaviz garantit la disponibilité, l'intégrité, la confidentialité et l'auditabilité des données hébergées.

Medaviz est en mesure de fournir sur demande, des indicateurs de qualité et de performance, notamment le taux de disponibilité de la plateforme, le temps de réponse moyen de la plateforme, le taux d'erreur maximal dans le code. Ces indicateurs permettent la vérification du niveau de service annoncé, le niveau garanti, et la périodicité de leur mesure, conformément aux niveaux de services définis avec le Partenaire. Medaviz s'engage à un taux annuel de disponibilité minimal de la plateforme à 99% et à un temps de réponse moyen de 800 ms côté serveur (sur 12h, hors temps réseau).

Medaviz a recours à des prestataires techniques externes, dont Amazon Web Services (AWS) qui présente un niveau de garantie équivalent à celui de Medaviz.

Medaviz a mis en place une journalisation de toutes les actions relatives aux données de santé permettant de retrouver des traces d'incident ou d'abus. Des procédures de type PCA et PRA permettent également de couvrir toute défaillance éventuelle de sa part.

Medaviz s'engage à restituer, à la fin de la prestation, la totalité des données de santé au responsable de traitement et à détruire ces données de santé après l'accord formel du responsable de traitement et sans en garder de copie.

C. LOCALISATION DES DONNÉES HÉBERGÉES

Les données à caractère personnel (y compris de santé) sont hébergées par AWS qui a reçu la certification HDS (Hébergeur de Données de Santé) conformément à l'article L. 1111-8 du Code de la santé publique. Les centres de données sont basés dans l'Union Européenne : en France (région parisienne) ou en Allemagne (région de Francfort). Medaviz pourra ajouter d'autres sites qui seront exclusivement situés dans l'Union Européenne sans nécessiter l'accord du Responsable de traitement, à condition que ce changement n'affecte pas la prestation.

D. PERTE OU RETRAIT DE LA CERTIFICATION HDS

Medaviz s'engage à informer le Partenaire en cas de perte ou de retrait de la certification HDS. Si le Partenaire le souhaite, et après validation d'un devis, Medaviz pourra accompagner le Partenaire pour mettre en œuvre la réversibilité de la prestation d'hébergement de données de santé.

14. LES MODIFICATIONS DE LA POLITIQUE DE CONFIDENTIALITÉ

La politique de confidentialité est susceptible d'évoluer. En cas d'évolution des éléments mentionnés dans la politique de confidentialité, Medaviz s'engage à en informer les personnes concernées, préalablement à la mise en œuvre des modifications qui pourraient impacter les données à caractère personnel. Medaviz s'efforcera d'indiquer quels impacts impliquent ces modifications. Le présent document a été validé par le Délégué à la protection des données préalablement à sa diffusion. Il fait l'objet d'une révision tous les ans.

15. LIENS UTILES

Pour plus d'informations, l'Utilisateur est invité à se référer :

- aux "Conditions Générales d'Utilisation" : https://my.medaviz.io/pdf/legal/conditions-generales-utilisation.pdf
- à la Politique de confidentialité patient : https://my.medaviz.io/pdf/legal/politique-confidentialite-patient.pdf
- à la page informations ISO-27001, HDS et conformité au Règlement Général sur la Protection des Données : https://www.medaviz.com/confidentialite-et-securite/
- au site Internet de la CNIL : https://www.cnil.fr/fr/comprendre-vos-droits
- Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) : https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire

CONDITIONS PARTICULIÈRES POUR LES PARTENAIRES ET LES PRATICIENS

1. LES SOUS-TRAITANTS

A. SOUS-TRAITANCE ULTÉRIEURE

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le responsable de traitement dispose d'un délai minimum de 2 mois à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du Règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

2. NOTIFICATION DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 72 heures après en avoir pris connaissance. Cette notification écrite est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente. La notification contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

3. DEMANDE DE TRANSMISSION DE DONNÉES

En cas de demandes légales d'accéder aux données à caractère personnel de Medaviz dans l'hypothèse où le Partenaire, dans le cadre des lois ou des obligations réglementaires en vigueur, reçoit la demande d'effectuer certaines opérations de traitement (y compris mais non limité à la divulgation aux autorités publiques) relatives aux données à caractère personnel de Medaviz, le Partenaire s'engage expressément à :

- informer Medaviz de cette demande dès que possible, sous réserve du respect des dispositions légales qui peuvent l'empêcher d'en informer Medaviz, afin d'obtenir le consentement exprès et écrit de Medaviz à ces opérations de traitement ;
- s'opposer si possible, (y compris par action légale), à une telle demande (notamment, en notifiant que Medaviz n'est pas le responsable de traitement des données qu'il traite pour le compte du Partenaire et de ses bénéficiaires) ;
- autoriser, si possible, Medaviz (s'il le décide) à participer à toute action engagée pour s'opposer à de tels traitements.

4. MESURES DE SÉCURITÉ – AUDIT

Le sous-traitant s'engage, dans la limite du périmètre de ses prestations à mettre en œuvre :

- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- la pseudonymisation des données à caractère personnel;

- les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque ;
- la formation des personnels à la sécurité des données ;
- un processus d'habilitation des accès aux systèmes d'information traitant des données contrôlé mensuellement et au départ de chaque collaborateur ;
- Une politique de sécurité des locaux ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Le sous-traitant met à la disposition du Partenaire la documentation nécessaire pour démontrer le respect de ses obligations au titre du RGPD. En cas de demande d'audit de la part du Partenaire, ce dernier devra respecter les conditions suivantes :

- informer Medaviz au moins 10 jours ouvrés avant la réalisation de l'audit ;
- la réalisation de l'audit ne devra pas perturber l'activité de Medaviz ;
- l'audit sera réalisé uniquement par un auditeur indépendant certifié et concernera uniquement la vérification de la conformité au RGPD.
- Le cadre de l'audit devra être communiqué au préalable à Medaviz ;
- Le Partenaire transmettra les conclusions de l'audit à Medaviz dès qu'il en aura lui-même connaissance ;
- l'ensemble des coûts lié aux opérations d'audit resteront à la charge du Partenaire.

Le Sous-traitant déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement comprenant :

- le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
- les catégories de traitements effectués pour le compte du responsable du traitement ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du Règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins ;
- dans la mesure du possible, la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Le sous-traitant remet sur demande écrite du responsable de traitement la documentation relative au respect des obligations du sous-traitant.