

La présente Politique Générale relative à la protection des données à caractère personnel expose la manière dont EQUASENS traite et protège les Données à caractère personnel de ses Clients, soit en qualité de responsable de traitement soit en qualité de sous-traitant de ses Clients.

La présente Politique fait partie intégrante des Conditions Générales de Vente et d'Utilisation applicables à l'ensemble des Solutions commercialisées par EQUASENS sauf stipulations contraires.

Pour plus d'information sur les responsabilités et les manières dont sont traitées les Données à caractère personnel au travers des Solutions d'EQUASENS, nous vous invitons à consulter les éventuelles Conditions Spécifiques Produits applicables à chaque Solution commercialisée par EQUASENS et disponibles à l'adresse suivante : <https://espaceclient.pharmagest.com/conditions>.

Article 1. Définitions

Les définitions des termes figurant au présent article sont issues de l'article 4 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après « RGPD »). Les termes ayant une majuscule mais qui n'apparaissent pas dans cet article auront la définition correspondant à celle de l'Article 4 du règlement précédemment cité ou à celle des dispositions équivalentes des législations applicables en matière de protection des données, sauf disposition particulière.

- « **Donnée à caractère personnel** » : désigne toute information se rapportant à une personne physique identifiable ou identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, et dont l'identification peut être réalisée à partir d'une seule donnée ou à partir du croisement d'un ensemble de données.
- « **Données concernant la santé** » : désigne les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.
- « **Responsable de traitement** » : désigne la personne physique ou morale, publique ou privée, ou le service, qui détermine, seul ou avec d'autres, les finalités et les moyens du traitement.
- « **Sous-traitant** » : désigne la personne physique ou morale, publique ou privée, ou le service qui traite des données personnelles pour le compte du responsable de traitement.
- « **Traitement des données à caractère personnel** » : désigne une opération ou un ensemble d'opérations portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission ou diffusion, ou toute autre forme de mise à disposition, rapprochement).
- « **Violation de données à caractère personnel** » : désigne une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

- « **Conditions Spécifiques Produits** », « **Conditions Spécifiques** » ou « **CSP** » : désigne les Conditions Spécifiques propres à une Solution dérogeant ou complétant les Conditions Générales de Vente et d'Utilisation des Solutions de la Division Pharmagest d'EQUASENS .
- « **Contrat** » : désigne ensemble les Conditions Générales de Vente et d'Utilisation et leurs Annexes, ainsi que les Conditions Spécifiques Produits, le Bon de commande et, le cas échéant, les Conditions Particulières de Commande relatives à la Solution concernée.
- « **Solution(s)** » : désigne l'ensemble des licences logiciel, Matériels, Prestations de Service et Contrats de Services continus proposés par EQUASENS au Client.
- « **Société(s) Affiliée(s)** » : désigne toute entité, présente ou à venir, contrôlée directement ou indirectement par EQUASENS, le contrôle s'entendant de la possession, directe ou indirecte, de plus de 50 % des parts avec droits de vote, ou de plus de 50 % des droits de vote conférant le pouvoir de nommer les organes de direction de l'entité contrôlée

Article 2. Données traitées par EQUASENS en qualité de responsable de traitement

2.1. Dans le cadre des relations contractuelles entre EQUASENS et le Client

Nature des données traitées

Pour les besoins de la réalisation des Contrats signés entre EQUASENS et le Client, EQUASENS est amenée à recueillir et à traiter les données personnelles de son Client, telles que notamment l'identité et les coordonnées du titulaire de la pharmacie, le code CIP de la pharmacie, nom des membres de l'équipe officinale appelant le support, etc. A ce titre, EQUASENS agit en tant que responsable de traitement des données.

(a) Finalités de traitement

Les données personnelles recueillies auprès des Clients font l'objet d'un traitement informatique réalisé par EQUASENS. Elles sont enregistrées dans son fichier Clients et sont indispensables au traitement de sa commande et à l'exécution du Contrat. Ces informations et données personnelles sont également conservées à des fins de sécurité et de production de services, afin de respecter les obligations légales et réglementaires. Elles seront conservées aussi longtemps que nécessaire pour l'exécution des Contrats, l'amélioration de la qualité des Solutions, et des garanties éventuellement applicables.

(b) Confidentialité et sécurité des données

L'accès aux données personnelles est strictement limité aux employés d'EQUASENS habilités à les traiter en raison de leurs fonctions. Les informations recueillies pourront éventuellement être communiquées à des tiers liés à l'entreprise par un contrat, pour l'exécution de tâches sous-traitées, sans que l'autorisation du Client soit nécessaire. Le cas échéant, EQUASENS se porte fort du respect des conditions énoncées aux présentes et s'engage à ce que ces tiers appliquent le même degré de confidentialité et de protection à l'égard des données personnelles transmises.

Dans le cadre de l'exécution de leurs prestations, les tiers n'ont qu'un accès limité aux données et ont l'obligation de les utiliser en conformité avec les dispositions de la législation applicable en matière de protection des données personnelles.

En dehors des cas énoncés ci-dessus, EQUASENS s'interdit de vendre, louer, céder ou donner accès à des tiers aux données personnelles sans consentement préalable du Client, à moins d'y être contrainte en raison d'un motif légitime.

Le Client accepte cependant de recevoir des courriers électroniques contenant des offres en rapport avec l'ensemble de son activité professionnelle, les annonceurs conservant alors l'entière responsabilité de la teneur des messages dont le Client pourrait être destinataire.

Si les données sont amenées à être transférées en dehors de l'UE, le Client en sera informé et les garanties prises afin de sécuriser les données (par exemple, adoption de modèles de clauses types de protection validées par la CNIL, adoption d'un code de conduite, obtention d'une certification CNIL, etc.) lui seront précisées.

(c) Exercice des droits

Conformément à la réglementation applicable, le Client dispose d'un droit d'accès, de rectification, d'effacement, et de portabilité des données le concernant, ainsi que du droit de s'opposer au traitement pour motif légitime, droits qu'il peut exercer en s'adressant au délégué à la protection des données d'EQUASENS, par e-mail à l'adresse : dpo@equasens.com, ou par voie postale à l'adresse suivante :

EQUASENS
DPO
5 Allée de Saint Cloud
BP 117
54601 VILLERS LES NANCY CEDEX

En cas de réclamation, le Client peut également adresser sa demande auprès de la Commission Nationale de l'Informatique et des Libertés.

2.2. Dans le cadre des relations entre EQUASENS et ses Sociétés Affiliées

EQUASENS est amenée à partager et à transmettre les données personnelles de ses Clients à ses Sociétés Affiliées telles que listées ci-après, sur le fondement de son intérêt légitime.

A ce titre, EQUASENS informe le Client qu'elle pourra échanger et transmettre à ses Sociétés Affiliées, l'identité et les coordonnées du titulaire de la pharmacie ainsi que le code CIP de la pharmacie pour les finalités d'amélioration de la qualité des produits et services proposés, d'information et d'actions de prospection commerciale, en lien avec la profession du Client, et d'élaboration de statistiques groupe.

A la date des présentes, les Sociétés Affiliées concernées sont les sociétés Asca Informatique, Atoopharm, EHLS, Kapelse, Healthlease, Nanceo. BGM, Multimeds.

Les données personnelles du Client pour les finalités décrites ci-dessus sont conservées jusqu'à l'exercice du droit d'opposition du Client le cas échéant, ou pendant toute la durée contractuelle et au terme du Contrat quelle qu'en soit la cause, pendant une période de cinq (5) ans.

Conformément à la réglementation applicable, le Client dispose à tout moment du droit de s'opposer au traitement effectué, droit qu'il peut exercer en s'adressant au délégué à la protection des données de chaque Société Affiliée ou au délégué à la protection des données d'EQUASENS dont les coordonnées figurent ci-dessus.

En cas de réclamation, le Client peut également adresser sa demande auprès de la Commission Nationale de l'Informatique et des Libertés.

Article 3. Données traitées par le Client en qualité de responsable de traitement

Dans le cadre de l'utilisation des Solutions fournies par EQUASENS au Client, ce dernier est amené à recueillir et à traiter les données personnelles de ses patients (ex : identité, numéro de carte vitale ou INS, historique de délivrance...), de ses collaborateurs (ex : identité) et d'autres professionnels de santé (ex : identité des médecins). Dans ce cadre, le Client agit en tant que responsable de traitement sur les données qu'il recueille et qu'il traite dans les Solutions.

(a) Obligations du Client

Conformément aux dispositions du RGPD, le Client s'engage à respecter les dispositions des articles 24 et 25 ainsi que les autres dispositions dudit règlement qui lui sont applicables (article 32 et suivants). Il doit par conséquent s'assurer de mettre en œuvre et de maintenir toutes les mesures techniques et organisationnelles nécessaires aux présentes.

Certaines fonctions du logiciel peuvent être amenées à transmettre des données personnelles du Patient à des services tiers (téléservices de l'assurance maladie, facturation SESAM-Vitale, etc.) ou permettent d'accéder à des services tiers via leur interface, par exemple en cliquant sur des liens hypertexte ou en utilisant un téléservice. Le Client doit par conséquent s'assurer d'avoir pris connaissance de la politique de protection des données propre à chacun de ces services, qui ne saurait en aucun cas engager la responsabilité d'EQUASENS.

(b) Responsabilité du Client

Le Client est seul responsable de l'utilisation et du traitement de ces données personnelles. EQUASENS dégage toute responsabilité au regard de l'utilisation des données personnelles de la patientèle du Client qui en est faite par ce dernier via l'utilisation des Solutions.

Les données concernant la santé sont stockées au sein du réseau local du Client ou dans les datacenters HDS d'EQUASENS et sont gérées sous la seule responsabilité du Client, qui est garant du respect des droits des personnes en matière de données à caractère personnel concernant la santé.

Sauf dispositions particulières contraires précisées dans les Conditions Spécifiques Produits, le Client reste seul propriétaire des fichiers de données à caractère personnel transmis à EQUASENS ainsi que des fichiers de données à caractère personnel modifiés ou créés par EQUASENS pour son compte dans le cadre de l'exécution du présent Contrat.

(c) Droit des personnes concernées

Le Client s'engage à fournir à sa patientèle l'ensemble des informations relatives à la protection des données à caractère personnel requises par le RGPD au moment de la collecte des données et pour toutes les opérations de traitement.

Conformément à la réglementation applicable, sa patientèle dispose également d'un droit d'accès, de rectification, d'effacement, et de portabilité des données la concernant, ainsi que du droit de s'opposer au traitement pour motif légitime, droits qu'elle peut exercer en s'adressant au délégué à la protection des données du Client, dans la limite des réglementations sanitaires applicables aux données de santé.

Article 4. Données traitées par EQUASENS en qualité de sous-traitant

Dans le cadre de la fourniture des Services, EQUASENS peut être amenée à traiter des données à caractère personnel, en sa qualité de sous-traitant du Client.

(a) Cas de sous-traitance

Lorsque les données personnelles sont stockées sur un serveur local du Client, EQUASENS n'y a pas accès et ne traitera pas ces données. Seul le Client est à même de saisir, modifier, accéder, supprimer, diffuser les données.

EQUASENS ne traite des données personnelles en tant que sous-traitant que dans le cas a) d'un hébergement HDS des données à caractère personnel, ou b) de l'export de données à caractère personnel vers un tiers à la demande du Client ou c) des reprises de données à caractère personnel lors d'une installation ou d'un transfert de serveur ou d) d'une éventuelle intervention de maintenance sur site ou à distance, réalisée à la demande du Client.

(b) Obligations d'EQUASENS

EQUASENS s'engage à respecter ses obligations au titre des présentes Conditions Générales et des dispositions de l'Article 28 et des autres dispositions du RGPD qui lui sont applicables.

A ce titre, EQUASENS s'engage notamment à maintenir la confidentialité des données, y compris pour toutes les personnes qui ont accès aux données à caractère personnel, et à assurer la mise en œuvre et le maintien de toutes les mesures techniques et organisationnelles nécessaires aux présentes conformément à l'Article 32 RGPD. Le Client peut prendre connaissance desdites mesures techniques et organisationnelles qu'EQUASENS met en œuvre et qui sont reproduites en Annexe 1 de la présente Politique.

EQUASENS ne peut donner accès aux données à caractère personnel traitées pour le compte du Client ou les rectifier ou les effacer que sur les instructions de ce dernier. Si une personne concernée s'adresse directement à EQUASENS pour avoir accès à ses données à caractère personnel ou pour qu'elles soient rectifiées ou effacées ou pour exercer son droit d'opposition, EQUASENS transmettra cette demande au Client dès réception.

EQUASENS s'interdit en outre de détourner, commercialiser ou communiquer tout ou partie des desdits fichiers à d'autres fins que celles indiquées par le Client en sa qualité de responsable de traitement.

(c) Sous-traitance en cascade

La sous-traitance auprès de sous-traitants de second rang ou de tiers indépendants nécessite l'accord préalable écrit du Client. Lorsque le Client donne son accord quant à cette sous-traitance de second rang, EQUASENS doit conclure avec le(s) sous-traitant(s) de second rang des accords contractuels permettant de refléter les stipulations de protection des données à caractère personnel convenues entre le Client et EQUASENS, y compris, mais sans limitation, les mesures de sécurité techniques et organisationnelles. Lorsqu'un sous-traitant de second rang est impliqué, le Client se verra conférer le droit de surveiller et de contrôler ce sous-traitant conformément au présent Contrat et tel que requis par le RGPD.

(d) Instructions du Client

EQUASENS est à tout moment tenue par les instructions du Client relatives à l'exécution du Contrat et au traitement des données à caractère personnel appartenant au Client. Le Client conserve un droit général de donner des instructions sur la nature, la portée et la méthode du traitement des données, qui peuvent être complétées par des instructions particulières, notamment dans le cas de la souscription à un service applicatif en ligne.

EQUASENS ne peut répondre à une demande d'information d'un tiers ou d'une personne concernée, sans l'accord préalable écrit du Client.

EQUASENS informe immédiatement le Client, à tout moment, s'il estime qu'une instruction du Client est de nature à constituer une Violation de Données à caractère personnel, une atteinte aux droits de la patientèle du Client et plus globalement si une instruction du Client est contraire aux dispositions du RGPD. EQUASENS pourra suspendre la réalisation de l'instruction dans une telle hypothèse.

(e) Utilisation des données

EQUASENS ne doit pas utiliser les données à une autre fin que l'exécution du Contrat et notamment, ne doit pas divulguer des données aux tiers, sauf si elle a préalablement obtenu le consentement écrit du Client. Si EQUASENS est légalement tenue de divulguer des données à caractère personnel, elle en informera immédiatement le Client.

Aucune copie ni reproduction ne doit être produite sans que le Client en ait connaissance. Cette règle ne s'applique pas aux copies de sauvegarde, à la lecture des fichiers de connexion etc., lorsqu'ils sont nécessaires au traitement correct des données et à l'exécution du Contrat à la condition que le contenu des données reste inchangé et que le traitement n'interfère pas avec les intérêts du Client.

EQUASENS doit informer immédiatement le Client, avant tout traitement, s'il estime qu'une instruction du Client constitue une violation des dispositions légales en matière de protection des données. Il peut alors reporter l'exécution de l'instruction concernée jusqu'à la confirmation ou la révision de l'instruction par le Client.

(f) Responsabilité

Le Client est responsable envers la personne concernée des dommages que la personne concernée peut subir en raison d'un traitement illicite ou incorrect des données dans le cadre de l'exécution du Contrat qui constitue une violation des dispositions prévues par le RGPD ou d'autres dispositions relatives à la protection des données.

Si le Client était tenu de procéder à des paiements à un tiers (y compris les personnes concernées) en raison de tout traitement ou utilisation de données illicite ou en violation d'une obligation dont EQUASENS est responsable, ce dernier garantira et indemniserà le Client contre tout recours de tiers et ce, sans préjudice de toute autre action ou réclamation.

Chaque Partie apportera à l'autre une assistance raisonnable dans la défense contre les réclamations injustifiées.

(g) Suppression des données

Au terme du Contrat ou à tout moment sur demande du Client, EQUASENS devra retourner au Client toutes les données à caractère personnel, les documents en sa possession et tous les résultats des activités et données produites dans le cadre du Contrat, ou les supprimer conformément aux stipulations applicables à la protection des données à caractère personnel et ce, avec l'accord préalable du Client. Le fichier de suppression sera présenté au Client, sur demande.

EQUASENS doit conserver tout document permettant de justifier du traitement approprié des données à caractère personnel conformément aux présentes au-delà de la période contractuelle pendant la durée de conservation de cinq (5) années.

EQUASENS doit, sur demande du Client, remettre au Client cette documentation après l'expiration du Contrat.

L'obligation de confidentialité d'EQUASENS continuera de s'appliquer nonobstant le terme du Contrat sur toutes les données à caractère personnel ou les autres informations du Client qui ont été portées à sa connaissance pendant l'exécution du contrat.

(h) Autres données

Le Client autorise en outre expressément EQUASENS à collecter certaines données non nominatives et totalement anonymisées traitées par le système informatique de l'établissement du Client qui utilise les Solutions d'EQUASENS. Ces données, qui seront stockées sur support informatique par EQUASENS, notamment selon la technique de la blockchain, répondent à des finalités exclusivement statistiques et d'études (médicales) et ne seront croisées avec aucun autre fichier.

Article 5. Hébergement des données de santé

Les données de santé étant considérées comme des données sensibles, elles font l'objet d'une protection particulière afin de garantir le respect à la vie privée des personnes. L'hébergement de ces données doit en conséquence être réalisé dans des conditions de sécurité adaptées à leur criticité.

En qualité de sous-traitant des données personnelles, EQUASENS s'engage à héberger les données de santé à caractère personnel conformément à la certification HDS (Hébergeur agréé de Données de Santé) EQUASENS s'engage à disposer d'une équipe d'experts en charge de la partie conception, de l'exploitation et du support de l'hébergement des données de santé pour garantir un processus poussé de vérification de l'accès aux données et une évaluation des risques.

5.1. Périmètre du certificat de conformité d'hébergeur, dates de délivrance et de renouvellement

EQUASENS détient le certificat HDS711790 et exploite un Système de Management de la Sécurité de l'Information des hébergeurs de données de santé conforme aux exigences du Référentiel de certification HDS – Exigences et contrôles, v.1.1 – Juin 2018 pour le domaine d'application suivant :

Activité d'hébergement d'applications ou de services de santé, destinés à des fins de suivi médical des patients, qui consiste en un hébergement et/ou des sauvegardes sécurisés des données de santé ou de vie réelle à caractère personnel, dans ses centres de données. Les données sont collectées ou produites par des éditeurs, des fournisseurs de services, des professionnels de santé, des établissements sanitaires et médicaux-sociaux, des professions paramédicales, des patients ou toutes autres personnes physiques ou morales habilitées à manipuler des données de santé. EQUASENS se positionne en tant qu'hébergeur d'infrastructure physique et hébergeur infogéreur, proposant des services de type IAAS. Le domaine d'application est le suivant :

- Mise à disposition ou maintien en condition opérationnelle de locaux permettant d'héberger l'infrastructure matérielle du système d'information de santé ;
- Mise à disposition ou maintien en condition opérationnelle de l'infrastructure matérielle du système d'information de santé ;
- Mise à disposition ou maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information de santé ;
- Infogérance d'exploitation du système d'information de santé ;
- Sauvegardes externalisées des données de santé conformément à la déclaration d'applicabilité version 1.0 du 03/09/2019.

L'organisation est certifiée ISO 27001:2013.

EQUASENS détient également le certificat IS 711789 et exploite un système de management de la sécurité de l'information qui est conforme aux exigences de la norme ISO/IEC 27001:2013

5.2. Description des prestations réalisées

EQUASENS fournit au Client un service visant à assurer :

- Le service d'hébergement, dans le respect des exigences issues du Décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel, au référentiel de certification HDS – Exigences et contrôles V1.1 publié par l'ANS, de l'environnement Client, et donc des applications et données personnelles de santé intégrées en son sein par le Client, dans des conditions de nature à garantir leur sécurité et confidentialité, ainsi que disponibilité, pérennité et intégrité ;
- La continuité de fourniture du service y compris en cas de sinistre majeur sur l'un des sites d'hébergement ;
- La restitution du contenu de l'environnement Client, au Client ou au tiers désigné par lui, en fin de contrat (réversibilité) et, sous réserve de l'accord formel du Client, la destruction des données de santé en fin de contrat.

5.3. Lieux d'hébergement

Les données personnelles sont hébergées dans l'Union Européenne.

5.4. Mesures de mises en œuvre pour garantir le respect des droits des personnes concernées

Les mesures de mises en œuvre pour garantir le respect des droits des personnes concernées sont détaillées dans la présente Politique ainsi que dans les Conditions Spécifiques Produits applicables à chaque Solution lorsqu'elles en prévoient.

5.5. Référent pour le traitement des incidents ayant un impact sur les données de santé hébergées

En cas d'incidents ayant un impact sur les données personnelles hébergées, EQUASENS s'engage à mettre en œuvre les stipulations de la présente Politique ainsi que celles des Conditions Spécifiques Produits applicables à chaque Solution lorsqu'elles en prévoient.

5.6. Modalités retenues pour encadrer les accès aux données personnelles de santé hébergées

EQUASENS s'engage à ne pas traiter les données hébergées à d'autres fins que celles détaillées dans la présente Politique ainsi que dans les Conditions Spécifiques Produits applicables à chaque Solution lorsqu'elles en prévoient.

En sa qualité de sous-traitant, EQUASENS s'engage à ne traiter les données personnelles de santé que sur les instructions documentées du Client.

EQUASENS reconnaît le caractère strictement confidentiel de toutes les données personnelles qu'elle traite et prend toutes précautions visées aux présentes afin de préserver la confidentialité des données personnelles de santé. EQUASENS s'engage notamment à ne pas divulguer, copier ou stocker, sous quelque forme que ce soit, tout ou partie des données personnelles traitées.

EQUASENS veille à ce que les personnes autorisées à traiter les données personnelles, en vertu de la présente Politique ainsi que des Conditions Spécifiques applicables à chaque Solution lorsqu'elles en prévoient, soient soumises à une obligation appropriée de confidentialité, notamment au moyen d'une clause de confidentialité dans leur contrat de travail et reçoivent les formations de sensibilisation adaptées à leurs fonctions.

EQUASENS prend en compte, s'agissant du service et de ses composants, les principes de protection des données personnelles dès la conception et par défaut.

5.7. Interdiction pour EQUASENS d'utiliser les données de santé hébergées à d'autres fins que l'exécution de l'activité d'hébergement de données de santé

Conformément à la présente Politique ainsi qu'aux Conditions Spécifiques applicables à chaque Solution lorsqu'elles en prévoient, EQUASENS s'interdit d'utiliser les données hébergées des Clients à d'autres fins que l'exécution des finalités prévues dans la présente Politique ainsi que dans les Conditions Spécifiques applicables à chaque Solution lorsqu'elles en prévoient.

5.8. Prestations à la fin de l'hébergement

Les Parties conviennent qu'en cas de cessation des relations contractuelles pour quelque cause que ce soit, et notamment en cas de retrait de la certification, EQUASENS restitue l'ensemble des applications et données personnelles de santé qui lui ont été confiées, au Client dans le délai de trois (3) mois à compter de la cessation des relations contractuelles.

En outre, à l'issue d'un délai de trois (3) mois à compter de la cessation des relations contractuelles, et après trois (3) relances adressées dans ce délai par EQUASENS au Client par tout moyen, EQUASENS détruit le contenu de l'environnement Client, sans que le Client ne puisse exiger une indemnisation de ce fait.

En effet, les Parties conviennent expressément que l'absence de réponse à ces relances dans le délai défini ci-dessus constitue un accord formel, bien que tacite, du Client à la destruction du contenu de l'environnement Client.

Lors de la restitution du contenu de l'environnement Client, les Parties s'engagent à signer un procès-verbal de restitution. Faute de signature de celui-ci dans un délai de cinq (5) jours à compter de la réception du procès-verbal, la restitution sera réputée tacitement acceptée. Le procès-verbal de restitution ou la tacite acceptation atteste de la fin de réversibilité.

A compter de la signature de ce procès-verbal de restitution ou de son acceptation tacite, EQUASENS est dégagée de toute responsabilité liée à la fourniture du service.

Dans l'hypothèse d'une liquidation judiciaire, EQUASENS s'engage à désigner un tiers responsable et habilité à recevoir le contenu de l'environnement Client dans un délai de trois (3) mois à compter de son prononcé.

En outre, à l'issue d'un délai de trois (3) mois à compter du prononcé et après trois (3) relances adressées dans ce délai par EQUASENS au Client par tout moyen, EQUASENS détruit le contenu de l'environnement Client, sans que le Client ne puisse exiger une indemnisation de ce fait.

En effet, les Parties conviennent expressément que l'absence de réponse à ces relances dans le délai défini ci-dessus constitue un accord formel, bien que tacite, du Client à la destruction du contenu de l'environnement Client.

5.9. Restitution à la fin de la prestation de la totalité des données de santé à caractère personnel au responsable de traitement

Conformément à la présente Politique ainsi qu'aux Conditions Spécifiques Produits applicables à chaque Solution lorsqu'elles en prévoient, EQUASENS s'engage à restituer à la fin du contrat, dans un délai maximum d'un (1) mois, les données des Clients aux Clients en tant que responsable de traitement desdites données.

5.10. Engagement de l'hébergeur de détruire, à la fin de la prestation, les données personnelles de santé après l'accord formel du responsable de traitement et sans en garder de copie.

Conformément à la présente Politique ainsi qu'aux Conditions Spécifiques Produits applicables à chaque Solution lorsqu'elles en prévoient, EQUASENS s'engage à détruire à la fin de la prestation d'hébergement réalisée dans le cadre du contrat les données des clients avec l'accord exprès et écrit des Clients sans garder de copie desdites données sauf nécessité

Article 6. Conservation des données

Les données personnelles sont conservées aussi longtemps que nécessaire ou qu'il est permis eu égard à l'objet ou aux objets de leur obtention et tel qu'exposé dans cette Politique. La détermination de la durée de conservation s'appuie sur les critères suivants : (i) la durée pendant laquelle EQUASENS entretient une relation continue avec le Client et pendant laquelle EQUASENS met les Solutions à disposition du Client ; (ii) le fait qu'EQUASENS soit ou non soumise à une obligation légale ; ou (iii) le fait que la conservation soit recommandée eu égard à la position juridique d'EQUASENS (par rapport à l'application des conditions d'utilisation des Solutions, aux règles de prescription applicables, aux litiges ou aux enquêtes réglementaires).

ANNEXE 1

MESURES TECHNIQUES ET ORGANISATIONNELLES DE SECURITE

1. PRÉAMBULE

- 1.1 EQUASENS s'engage expressément à mettre en œuvre, au minimum, les mesures techniques et organisationnelles de sécurité décrites ci-après, et à maintenir ces mesures en permanence, afin de garantir la sécurité et la confidentialité des Données à caractère personnel du Client ou des Données à caractère personnel traitées pour le compte du Client, et notamment d'empêcher tout Traitement de Données Personnelles qui n'aurait pas été préalablement autorisé ou qui ne serait pas justifié par des motifs légitimes, ainsi que contre toute perte accidentelle, destruction ou atteinte aux Données à caractère personnel.
- 1.2 EQUASENS pourra, à défaut de mettre en œuvre les mesures décrites ci-après à l'identique, implémenter toutes mesures techniques ou organisationnelles de nature à garantir un niveau de protection des Données à caractère personnel au moins équivalent à celui prévu par les mesures décrites dans la présente Annexe.
1. EQUASENS reconnaît et accepte qu'elle est, pendant toute la durée de la relation commerciale avec le Client, tenue d'implémenter les mesures techniques et organisationnelles décrites ci-après ou toute mesure équivalente ou au moins aussi efficace que celles décrites ci-après.

2. MESURES ORGANISATIONNELLES DE SÉCURITÉ DES DONNÉES PERSONNELLES

EQUASENS s'engage expressément à implémenter des mesures organisationnelles de sécurité destinées à préserver la sécurité des Données à caractère personnel du Client ou des Données à caractère personnel qu'elle traite pour le compte du Client.

- 1) **Désignation d'un DPO ou d'un référent à la protection des Données Personnelles.** – EQUASENS s'engage à nommer un Délégué à la Protection des Données ou une ou plusieurs personnes responsables de l'élaboration, de la mise en œuvre, de l'application, du maintien en vigueur et de la surveillance d'une politique de protection des Données à caractère personnel et de la vie privée, afin de s'assurer du respect du RGPD concernant les opérations de Traitement des Données Personnelles du Client ou réalisées pour le compte du Client. Le DPO ou la personne désignée par EQUASENS à ces fins devra :
 - a. Être indépendant(e) et relever directement du niveau de gestion approprié au sein de l'organisation afin d'assurer une gestion efficace des risques de Violations de Données à caractère personnel et d'entrave à la vie privée ;
 - b. Être impliqué(e) dans la gestion de toutes les questions relatives au traitement des Données à caractère personnel ;
 - c. Être expert(e) en matière de protection des Données à caractère personnel comme en attesteront ses diplômes et/ou expériences professionnelles passées ;
 - d. Servir de point de contact pour les autorités de contrôles ;
 - e. Informer la direction et les employés d'EQUASENS de leurs obligations à l'égard des Traitements de Données à caractère personnel ;
 - f. Assister le Client dans la conduite des audits qu'il pourrait être amené à réaliser chez EQUASENS.
- 2) **Établissement d'une politique de protection des Données Personnelles ou de tout document équivalent pour la gestion des Données à caractère personnel.** – EQUASENS s'engage à établir une politique de protection des Données à caractère personnel, une politique de confidentialité ou tout document de nature équivalente, dont l'objet est de rappeler les règles applicables en matière de protection et de gestion des Données Personnelles, et notamment :
 - a. Les principes de protection des Données à caractère personnel ;
 - b. La nature des Données à caractère personnel traitées par EQUASENS et les finalités de Traitement poursuivies ;

- c. Les règles en matière d'accès et de communication de ces Données ;
- d. Une présentation des mesures de sécurités implémentées par EQUASENS ;
- e. Les règles relatives à la conservation des Données à caractère personnel au sein d'EQUASENS ;
- f. Les sanctions en cas de non-respect des règles prévues par EQUASENS et par le RGPD ;
- g. Etc.

EQUASENS s'engage par ailleurs à communiquer toute politique de protection des Données Personnelles, politique de confidentialité ou document de nature équivalente qu'il aura établi sur première demande du Client. Dans ce cadre, le Client traitera le document transmis par EQUASENS comme une information confidentielle, dont l'usage par le Client sera strictement limité aux besoins de démonstration de la conformité du Traitement de Données à caractère personnel qu'il met en œuvre au RGPD.

3) **Établissement de procédures opérationnelles standardisées en matière de Traitements de Données Personnelles.** – En complément de la politique de protection des Données Personnelles, EQUASENS s'engage expressément à établir des procédures opérationnelles standardisées destinées à gérer efficacement diverses situations relatives aux Traitements de Données à caractère personnel qu'elle met en œuvre, et plus particulièrement :

- a. La gestion des demandes d'exercice des droits qui lui seraient adressées par des personnes concernées par les Traitements de Données à caractère personnel, afin notamment d'informer le Client de cette demande dans les meilleurs délais afin que le Client puisse se conformer à ses propres obligations ;
- b. La gestion des Violations de Données Personnelles, en vue de mettre en œuvre la procédure de notification de cette Violation de Données à caractère personnel auprès du Client en cas notamment d'atteinte à la confidentialité, à la disponibilité ou à l'intégrité des Données à caractère personnel qu'EQUASENS traite pour le compte du Client ;
- c. La gestion des contrôles et inspections mis en œuvre par les autorités de contrôles, en vue de connaître les bonnes pratiques à adopter dans ce contexte ;
- d. Et plus globalement toute procédure opérationnelle standardisée pertinente pour assurer un haut degré de sécurité et de protection des Données Personnelles.

4) **Établissement d'une charte informatique.** – EQUASENS s'engage à établir une charte informatique et à lui donner une force contraignante. La charte informatique d'EQUASENS devra *a minima* comporter les éléments suivants :

- a. Le rappel des règles de protection des Données à caractère personnel et les sanctions encourues en cas de non-respect de celles-ci ;
- b. Le champ d'application de la charte, qui inclut notamment :
 - i. Les modalités d'intervention des équipes chargées de la gestion des ressources informatiques au sein d'EQUASENS ;
 - ii. Les moyens d'authentification sur le système d'information utilisés par EQUASENS ;
 - iii. les règles de sécurité auxquelles les utilisateurs doivent se conformer, lesquelles doivent notamment inclure de signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement ; ne jamais divulguer et/ou confier son identifiant/mot de passe à un tiers ; ne pas installer, copier, modifier, détruire des logiciels sans autorisation d'EQUASENS ; verrouiller son ordinateur dès que l'on quitte son poste de travail ; ne pas accéder, tenter d'accéder, ou supprimer des informations si cela ne relève pas des tâches incombant à l'utilisateur ; respecter les procédures préalablement définies par l'organisme afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité.
- c. Les modalités d'utilisation des moyens informatiques et de télécommunications mis à disposition comme le poste de travail, les équipements nomades (notamment dans le cadre du télétravail), les espaces de stockage individuel, les réseaux locaux, les conditions d'utilisation des dispositifs personnels, l'Internet, la messagerie électronique, la téléphonie, etc.

- d. Les conditions d'administration du système d'information, et l'existence, le cas échéant, de systèmes automatiques de filtrage, systèmes automatiques de traçabilité, gestion du poste de travail.
 - e. Les responsabilités et sanctions encourues par le salarié d'EQUASENS en cas de non-respect de la charte informatique.
- 5) **Sensibilisation et formation à la protection des Données à caractère personnel.** – EQUASENS s'engage à mettre en place des mesures de sensibilisation à la protection des Données à caractère personnel, et au signalement des incidents, afin de faire en sorte que son personnel concerné soit informé et conscient des risques et des conséquences possibles en cas de Violations de Données à caractère personnel. Ces mesures peuvent notamment inclure des sessions de formation périodiques appropriées pour son personnel ayant accès aux Données à caractère personnel, ainsi que des mises à jour régulières des procédures pertinentes en fonction des personnes concernées.
- 6) **Contrôle des accès physiques.** – Si les Données Personnelles sont hébergées chez EQUASENS, celui-ci s'engage à mettre en œuvre les éléments de contrôle d'accès adéquats.

3. MESURES TECHNIQUES DE SÉCURITÉ DES DONNÉES PERSONNELLES

EQUASENS s'engage expressément à implémenter des mesures techniques de sécurité destinées à préserver la sécurité des Données à caractère personnel qu'il traite pour le compte du Client.

- 1) **Contrôle des accès aux Données à caractère personnel et sécurisation des postes informatiques.** – En vue de restreindre et de contrôler l'accès aux Données à caractère personnel qu'il traite pour le compte du Client, EQUASENS s'engage expressément et irrévocablement à :
- a. Sécuriser l'accès aux Données à caractère personnel traitées pour le compte du Client au moyen d'un identifiant et d'un mot de passe personnels sur les postes informatiques des membres de son personnel ;
 - b. Imposer aux utilisateurs ayant accès aux Données à caractère personnel la création d'un mot de passe contenant a minima 8 caractères et composé au moins d'une majuscule, une minuscule, un chiffre et un caractère spécial ;
 - c. Imposer une restriction d'accès au compte utilisateur : blocage du compte utilisateur à la suite de trois échecs lors de tentatives de connexion aux postes informatiques et/ou aux serveurs donnant accès aux Données à caractère personnel ;
 - d. Contraindre les utilisateurs du système d'information d'EQUASENS à changer leur mot de passe au plus tard tous les trois (3) mois, dans le cadre d'une procédure de remplacement stricte du mot de passe (redirection vers une page de changement de mot de passe via une URL temporaire dont la validité est limitée à 24 heures maximum) ;
 - e. Application de la norme de flux https.

EQUASENS s'engage par ailleurs à tenir un registre précis et à jour des profils de ses utilisateurs autorisés à accéder aux Données à caractère personnel traitées par EQUASENS pour le compte du Client.

Au surplus, EQUASENS s'engage à :

- f. Installer un logiciel pare-feu et antivirus sur les postes de travail de ses employés susceptibles d'avoir accès aux Données à caractère personnel qu'il traite pour le compte du Client, ainsi que limiter l'ouverture des ports de communication à ceux strictement nécessaires au bon fonctionnement des applications installées sur lesdits postes de travail ;
 - g. Configurer les logiciels antivirus pour que les mises à jour de sécurité se fassent automatiquement dès que cela est nécessaire.
- 2) **Traçabilité et journalisation des accès aux Données à caractère personnel.** – EQUASENS s'engage à mettre en place des mesures permettant d'assurer la traçabilité des accès aux Données à caractère personnel traitées pour le compte du Client, et la journalisation des actions qui sont réalisées sur lesdites Données à caractère personnel. EQUASENS s'engage ainsi à prévoir un système permettant de conserver tous les événements qui sont réalisés sur les Données à caractère personnel sur une période glissante de six (6) mois, et notamment à conserver les traces des :

- a. Accès utilisateurs aux Données à caractère personnel (identité de l'utilisateur s'étant connecté à la base de données, date et heure de la connexion, date et heure de la déconnexion) ;
- b. Actions réalisées les Données à caractère personnel (type de Données à caractère personnel consultées, nature de l'action – enregistrement, copie, transfert, export, etc.) ;
- c. Tentatives d'accès ou d'intrusion sur les serveurs contenant les Données à caractère personnel, notamment en cas d'échecs répétés ;
- d. Mesures mises en œuvre pour gérer les incidents et les violations de Données à caractère personnel.

EQUASENS devra par ailleurs préciser la durée de conservation des fichiers journaux, et prévoir d'auditer fréquemment ces fichiers journaux pour s'assurer de leur conformité avec les exigences formulées par le Client. EQUASENS s'engage ainsi à implémenter un processus pour examiner les fichiers journaux répertoriant les événements relatifs aux Données à caractère personnel au moyen d'une surveillance continue et automatisée et de processus d'alerte, selon une périodicité déterminée, afin d'identifier les irrégularités et de proposer des mesures correctives adaptées.

EQUASENS s'engage enfin à notifier, dans les plus brefs délais, toute anomalie ou tout incident de sécurité relatif aux Données à caractère personnel qu'elle traite pour le compte du Client.

- 3) **Mesures techniques de protection contre les intrusions.** – En vue d'assurer la sécurité et la confidentialité des Données à caractère personnel traitées pour le compte du Client, EQUASENS s'engage expressément à mettre en œuvre toute mesure adéquate permettant de prévenir les serveurs d'intrusions extérieures, notamment grâce à des procès tels que :
 - a. Protection de type filtrage de contenu sur internet (type Symantec ou tout système équivalent) ;
 - b. Protection WAF (Web Application Firewall), Firewall, reverse proxy ;
 - c. Limitation des flux de données ;
 - d. Segmentation réseau VLAN ;
 - e. Sécurisation des points d'accès (Wifi WPA) ;
 - f. Filtrage de port de VPN des partenaires externes ;
 - g. URL et contrôles d'accès nominatifs ;
 - h. Tests de pénétration avec rapport et plan de remédiation ;
 - i. Déploiement d'un système de détection des intrusions ;
 - j. Etc.
- 4) **Programmes de lutte contre les logiciels malveillants.** – De la même manière, EQUASENS s'engage à mettre en place les programmes informatiques nécessaires afin de lutter contre les logiciels malveillants (Malware) susceptibles de s'attaquer aux serveurs contenant les Données à caractère personnel traitées pour le compte du Client. Pour ce faire, EQUASENS mettra en œuvre les mesures suivantes ou toute mesure de même nature et d'un niveau de sécurité équivalent :
 - a. Politique de veille éditeurs (système + middleware) ;
 - b. Patch management en vue de gérer les correctifs de sécurité ;
 - c. Logiciels anti-malwares et anti-virus ;
 - d. Filtrage url et ports ;
 - e. Protection contre les menaces réseau avancées (ATP, Advanced threat protection tel que Microsoft Defender ATP) ;
 - f. Passerelles SMTP (DE TYPE F-Secure - Proofpoint) ;
 - g. Etc.
- 5) **Cloisonnement des Données.** – EQUASENS s'engage expressément à mettre en œuvre des mesures de cloisonnement fonctionnel (logique) et infra dédiée (physique) des Données à caractère personnel qu'il traite pour le compte du Client, de façon que lesdites Données à caractère personnel soient en permanence conservées à l'écart de toute autre donnée traitée par EQUASENS.

Dans ce cadre, EQUASENS s'engage à ne donner accès aux Données à caractère personnel qu'il traite pour le compte du Client qu'aux seuls employés qui ont un strict besoin d'y accéder pour la réalisation des prestations pour lesquelles le Client a recours aux services d'EQUASENS.

De plus, EQUASENS s'engage à contrôler régulièrement l'étanchéité des mesures de cloisonnement mises en place et, le cas échéant, à rétablir le strict cloisonnement des Données à caractère personnel.

- 6) **Maintenance corrective et évolutive.** – EQUASENS s'engage à mettre en œuvre des mesures de détection des incidents relatifs à la sécurité et la confidentialité des Données à caractère personnel, ainsi que les mesures de maintenance corrective destinées à rétablir la sécurité des Données à caractère personnel et, évolutives, en vue d'anticiper de nouveaux incidents de sécurité des Données à caractère personnel.
- 7) **Sauvegarde et restauration des Données.** – EQUASENS s'engage expressément à mettre en place une politique qui traite des exigences relatives à la sauvegarde, à la récupération et à l'archivage des Données à caractère personnel, ainsi qu'à l'éventuelle récupération et/ou restauration des Données à caractère personnel en cas d'incident technique ou de Violation de Données à caractère personnel.

EQUASENS garantit dans ce cadre que toute procédure de récupération et/ou restauration de Données à caractère personnel sera mise en place dans des conditions de nature à assurer que les Données à caractère personnel soient récupérées ou restaurées dans le respect de leur intégrité, ainsi qu'à mettre en place des mesures destinées à identifier une récupération et/ou restauration de Données à caractère personnel incomplète ou inexacte et à permettre sa résolution dans les plus brefs délais.

Dans ce cadre, EQUASENS doit établir une fréquence minimum de réalisation des sauvegardes de Données à caractère personnel traitées pour le compte du Client. EQUASENS s'engage par ailleurs à réaliser au minimum tous les six (6) mois des examens et tests de sauvegarde, ou en ce qui concerne les procédures de récupération et/ou restauration des Données à caractère personnel en cas d'incident technique ou de Violation de Données à caractère personnel.

EQUASENS s'engage par ailleurs à tenir un registre des procédures de restauration des Données à caractère personnel, contenant au minimum le nom de la personne au sein de son personnel en charge de la restauration des Données à caractère personnel, ainsi qu'une description des Données à caractère personnel restaurées.

- 8) **Mesures de sécurité physique.** – En vue de garantir la sécurité physique des Données à caractère personnel, et plus particulièrement les serveurs contenant lesdites Données à caractère personnel, EQUASENS s'engage à mettre en place les mesures permettant d'assurer la protection des Données à caractère personnel contre les sources de risques non humaines (notamment les incendies, tremblements de terre, inondations, etc.).

A ce titre, EQUASENS pourra notamment mettre en place :

- a. Un système de sécurité anti-incendie ;
- b. Un système d'alimentation électrique d'urgence ;
- c. Un système de surveillance de la température des serveurs ;
- d. Un système d'arrêt d'urgence des serveurs ;
- e. Etc.