MESURES DE SECURITE TECHNIQUES ET ORGANISATIONNELLES (TECHNICAL AND ORGANISATIONAL SECURITY MEASURES – « TOM »)

PARTIE 1 – PREAMBULE

1.1 OBJET

Le présent document a pour objet de décrire les mesures de sécurité techniques et organisationnelles mises en œuvre par Sigma Informatique en matière de protection des Données à Caractère Personnel lors de la réalisation des prestations de services qui lui sont confiées, y compris celles réalisées dans le cadre de sa certification d'hébergeur de données de santé « ci-après HDS ». Ces mesures ont vocation à protéger les Données à Caractère Personnel contre la destruction, la perte, l'altération, la divulgation non autorisée de Données à Caractère Personnel transmises, conservées ou Traitées d'une autre manière par Sigma Informatique, ou l'accès non autorisé à de telles Données.

Ces mesures constituent les mesures standards de Sigma Informatique applicables. Elles ne tiennent pas compte des mesures de sécurité techniques et organisationnelles qui pourraient être mises en œuvre spécifiquement pour un besoin particulier.

1.2 DEFINITIONS

Pour les besoins du présent document, les termes commençant par une majuscule ont la signification qui leur est attribuée ci-après, qu'ils soient exprimés au singulier, au pluriel, sous forme de verbe, de nom ou autre, à l'exception des termes prenant toujours une majuscule.

TERME	DEFINITION
Données à Caractère Personnel ou Données	Toute information se rapportant à une personne physique identifiée ou identifiable.
Données de Santé	L'ensemble des Données à Caractère Personnel se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro.
Sigma informatique	Sigma Informatique, Société par actions simplifiée, au capital de 1 729 600 EUR dont le siège social est situé à LA CHAPELLE-SUR-ERDRE (44240), ZI La Gesvrine - Rue Newton et immatriculée sous le numéro 872 803 390 R.C.S. NANTES.
Traitement	Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des Données ou des ensembles de Données à Caractère Personnel.

PARTIE 2 – MESURES DE SECURITE ORGANISATIONNELLES

2.1 GOUVERNANCE DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Sigma Informatique met en œuvre une gouvernance de la protection des Données à Caractère. La gouvernance de protection des Données à Caractère Personnel est déployée à l'ensemble des activités de Sigma Informatique.

Sigma Informatique a procédé à la désignation d'un délégué à la protection des données, joignable par téléphone au +33 (0) 2 40 37 14 00, par courrier électronique à dpo@sigma.fr ou par courrier postal en écrivant à Sigma Informatique - Attn DPO - 8 rue Newton - CS84533 - 44245 LA CHAPELLE SUR-ERDRE - FRANCE.

2.2 GOUVERNANCE DE LA SECURITE DES SYSTEMES D'INFORMATION

Sigma Informatique met en œuvre une gouvernance de la sécurité des systèmes d'information basée sur un Système de Management de la Sécurité de l'Information (SMSI) certifié ISO 27001 pour ses activités d'hébergement, d'infogérance et d'assistance aux utilisateurs.

2.3 GESTION DES RISQUES

Sigma Informatique a mis en place une démarche de maîtrise des risques de sécurité afin d'identifier les risques pesant sur la protection des Données à Caractère Personnel, d'évaluer leur probabilité de réalisation et de définir et valider les plans d'actions permettant de les maîtriser.

2.4 CLASSIFICATION DE L'INFORMATION

Les documents produits par Sigma Informatique sont classifiés et marqués selon qu'ils sont destinés au grand public, que leur diffusion est limitée à certaines catégories de destinataires ou qu'ils sont confidentiels et destinés aux seules personnes ayant besoin d'en prendre connaissance.

2.5 RESPECT DE LA CONFIDENTIALITE PAR LES COLLABORATEURS INTERVENANT SUR LES TRAITEMENTS

Sigma Informatique prend des mesures dans les contrats de travail afin que ses collaborateurs autorisés à Traiter les Données à Caractère Personnel respectent la confidentialité. Les collaborateurs peuvent également être amenés à conclure des engagements spécifiques de confidentialité compte tenu des Traitements auxquels ils participent.

2.6 PROTECTION DES DONNEES DES LA CONCEPTION

La protection des Données à Caractère Personnel, y compris les exigences de sécurité, est intégrée dans la réalisation des développements informatiques, des services ou des Traitements réalisés par Sigma Informatique. L'approche « privacy by design » est réalisée dès la phase de conception du produit, du service ou du Traitement et ce, afin de pouvoir respecter le droit des personnes concernées, limiter les erreurs, les pertes, les modifications non autorisées ou le mauvais usage de ces Données. Les développements et les tests sont effectués dans des environnements informatiques distincts de ceux en production et sur la base des Données fictives ou anonymisées qui lui sont fournies.

2.7 CONTINUITE ET REPRISE D'ACTIVITE

Sigma Informatique a établi un Plan de Continuité d'Activité (PCA) afin de protéger ses activités essentielles des effets causés par les défaillances de ses systèmes d'information. Ce PCA inclut un bilan d'impact sur l'activité (BIA), un plan de continuité opérationnelle (PCO), un plan de continuité informatique (PCI) et un plan de reprise d'activité (PRA).

2.8 GESTION DES INCIDENTS

Sigma Informatique encadre le signalement des évènements liés à la sécurité des systèmes d'information et des Données à Caractère Personnel pour permettre la remontée d'alerte dans les meilleurs délais et leur notification, le cas échéant. Des outils spécifiques sont mis en œuvre pour identifier les incidents et les quantifier. Les incidents sont également analysés afin que des mesures correctives et palliatives soient prises dans la mesure du possible.

2.9 VEILLE RELATIVE AUX VULNERABILITES TECHNIQUES ET DE CYBERCRIMINALITE

Sigma Informatique procède à une veille sur les vulnérabilités techniques des systèmes d'exploitation et des logiciels à destination des équipes concernées par l'utilisation de ces outils ainsi qu'à une veille relative à la cybercriminalité. Cette veille est associée à une revue des risques conduisant à la mise en œuvre de mesures complémentaires visant à pallier les vulnérabilités, le cas échéant.

2.10 CENTRE OPERATIONNEL DE SECURITE

Sigma Informatique dispose d'un centre opérationnel de sécurité (Security Operations Center – SOC) assurant la gestion opérationnelle de la sécurité des systèmes d'information au quotidien, notamment la prévention des risques (veille, gestion des accès à privilèges, audits de sécurité et sensibilisation à la sécurité), la détection des menaces (exploitation des solutions de sécurité, corrélation et analyse des évènements de sécurité, contrôle des accès aux environnements sensibles), la réaction sur incident (traitement des incidents et gestion de crise cyber sécurité).

2.11 SENSIBILISATION ET FORMATION

Sigma Informatique sensibilise ses collaborateurs et les forme sur divers aspects de la protection des Données à Caractère Personnel compte tenu de leurs missions et tâches. Certaines des sensibilisations ont un caractère obligatoire afin de s'assurer que l'ensemble des collaborateurs même s'ils n'ont pas à Traiter de Données à Caractère Personnel soient informés des exigences règlementaires existantes et des bonnes pratiques à respecter.

2.12 CONTROLES PERIODIQUES

Les dispositifs de protection des Données à Caractère Personnel mis en place par Sigma Informatique pour s'assurer de la sécurité des Traitements font l'objet de tests périodiques pour vérifier leur efficacité. Sigma Informatique confie également des contrôles et vérifications à des organismes certifiés ou d'autres tiers reconnus pour leur compétence.

2.13 GESTION DE LA SOUS-TRAITANCE

Sigma Informatique a défini dans ses cahiers des charges un ensemble d'exigences de sécurité destinées à limiter les risques sur les Données à Caractère Personnel. Les contrats conclus avec les fournisseurs imposent des dispositions spécifiques relatives à la protection des Données à Caractère Personnel.

2.14 CERTIFICATIONS

Sigma Informatique détient la certification ISO 27001 pour ses activités d'hébergement, d'infogérance et d'assistance aux utilisateurs et la certification ISO 9001 sur l'ensemble de son périmètre d'activité.

Sigma Informatique détient également une certification délivrée par Bureau Veritas en date du 16 mai 2019 valable trois (3) ans et portant sur les périmètres d'activité suivants :

- Hébergeur d'infrastructure physique, soit :
  - La mise à disposition et maintien en conditions opérationnelles des sites physiques permettant d'héberger l'infrastructure matérielle du Système d'Information utilisé pour le Traitement des Données de Santé,
  - La mise à disposition et maintien en conditions opérationnelles de l'infrastructure matérielle du Système d'Information utilisé pour le Traitement de Données de Santé.
- Hébergeur Infogéreur, soit
  - La mise à disposition et maintien en conditions opérationnelles des sites physiques permettant d'héberger l'infrastructure virtuelle du Système d'Information utilisé pour le Traitement de Données de Santé, ou
  - La mise à disposition et maintien en conditions opérationnelles de la plateforme d'hébergement d'application du Système d'Information,
  - L'administration et l'exploitation du Système d'Information contenant les Données de Santé,
  - La sauvegarde de Données de Santé.

SIGMA INFORMATIQUE peut sur demande fournir les rapports d'audit de certification ISO 27001 et Hébergeur de données de santé.

2.15 ASSURANCES

Sigma Informatique est assurée pour les risques susceptibles de se réaliser dans le cadre de son activité au travers d'assurances de type responsabilité civile professionnelle, dommages aux biens et risques cyber.

MESURES DE SECURITE ORGANISATIONNELLES COMPLEMENTAIRES HDS OU SUR DEMANDE

2.16 ENGAGEMENT DE CONFIDENTIALITE DES ADMINISTRATEURS

Les administrateurs, ingénieurs ou techniciens réalisant l'administration, l'exploitation ou la maintenance des Systèmes d'Information signent un engagement de confidentialité associé à la charte de l'administrateur informatique de Sigma Informatique. Cette charte définit les règles de sécurité encadrant les missions des administrateurs informatiques de Sigma Informatique, règles que ces collaborateurs s'engagent à respecter.

Cette charte s'applique à tous les administrateurs informatiques intervenant dans le cadre d'une relation contractuelle avec Sigma Informatique, quel que soit leur statut (salarié, prestataire ou intérimaire).

2.17 INTERDICTION DES COPIES PAPIERS

Dans le cadre des activités liées à la santé, les collaborateurs de Sigma Informatique ont l'interdiction de recourir à des copies papier de toute Donnée de Santé, sauf instruction spécifique et après validation du RSSI de Sigma Informatique.

2.18 INTERDICTION DES SUPPORTS AMOVIBLES

Dans le cadre des activités liées à la santé, les collaborateurs de Sigma Informatique ont l'interdiction de recourir à des supports amovibles pour le stockage de Données de Santé. Dans le cas où une instruction spécifique nécessiterait le recours à un support amovible, celui-ci est obligatoirement chiffré et utilisé uniquement après validation du RSSI de Sigma Informatique.

2.19 CONTROLE REGULIER DES ACTIVITES DES ADMINISTRATEURS

Un contrôle des activités des administrateurs est effectué par analyse des traces du bastion et par échantillonnage sur l'ensemble des systèmes cibles.

PARTIE 3 – MESURES DE SECURITE TECHNIQUES

3.1 CONTROLE D'ACCES PHYSIQUE ET SECURITE DES BATIMENTS

L'ensemble des sites de Sigma Informatique dans lesquels des Traitements de Données à Caractère Personnel sont réalisés sont sécurisés. Les sites sont équipés d'un système de contrôle d'accès physique par badge et/ou digicode.

Ces sites sont protégés contre l'intrusion physique par un système de détection d'intrusion avec alarme, associé à une prestation de télésurveillance, un système de vidéosurveillance et des restrictions d'accès à certains locaux aux seuls collaborateurs autorisés compte tenu de leurs fonctions. Ces sites sont également protégés contre l'incendie par une centrale de détection associée à des détecteurs de fumée et des extincteurs à usage manuel.

Les datacenters de Sigma Informatique font l'objet de mesures de sécurité complémentaires, à savoir une solution de détection incendie couplée à une solution d'extinction automatique, des dispositifs de secours électrique (onduleurs et groupes électrogènes) et une protection contre l'inondation ou des constructions hors zone inondable.

3.2 CONTROLE D'ACCES LOGIQUE ET HABILITATIONS

Sigma Informatique applique un contrôle d'accès logique basé sur les principes de moindre privilège et de séparation des tâches. Tous les utilisateurs pouvant accéder à un système d'information sont authentifiés par un compte nominatif. Sigma Informatique applique une politique de mot de passe imposant une complexité et un renouvellement régulier ainsi qu'une politique d'habilitation sur la base du moindre privilège et de la séparation des rôles.

3.3 CLOISONNEMENT DES DONNEES

Sigma Informatique utilise différentes solutions lui permettant de s'assurer de la séparation des Données afin qu'elles ne soient pas accessibles par d'autres clients de Sigma Informatique ou de ses collaborateurs n'ayant pas besoin d'y accéder dans le cadre de leurs missions. Les solutions de cloisonnement reposent sur des cloisonnements physiques (serveur physique dédié), cloisonnements réseaux (firewalling, VLAN) et des solutions de cloisonnement logicielles (bases des données, fichiers).

3.4 TRACABILITE

Les activités des utilisateurs et administrateurs des systèmes d'informations et les évènements liés à la sécurité sont journalisés. La journalisation comprend à minima l'identifiant, la date, l'heure de la connexion et la date et l'heure de la déconnexion. Selon la sensibilité des Données à Caractère Personnel, les actions sur les Données sont aussi journalisées.

3.5 SECURISATION DES ECHANGES ET FLUX DE DONNEES

Sigma Informatique utilise des protocoles garantissant la confidentialité et l'authentification des serveurs pour tous transferts de fichiers tels que les protocoles SFTP et HTTPS. Les supports utilisés pour les échanges de Données permettent également le chiffrement des fichiers ou des Données ou leur confidentialité par l'usage de clés de chiffrement ou de mots de passe. Des sondes de détection et de prévention d'intrusion analysent les flux à destination des serveurs de Sigma Informatique. Le cloisonnement réseau et le filtrage des flux sont réalisés selon la règle de l'interdiction par défaut.

3.6 SECURISATION DES POSTES DE TRAVAIL ET DE L'INFORMATIQUE MOBILE

Les postes de travail des collaborateurs de SIGMA INFORMATIQUE contiennent des mécanismes de verrouillage de session, des pare-feux, un antivirus. L'accès aux postes de travail se fait au travers d'un chiffrement de partition. Le mot de passe de la partition est différent de ceux requis pour accéder aux applicatifs et systèmes d'informations accessibles depuis les postes de travail. Les postes de travail nomades sont également chiffrés.

3.7 SECURISATION DES SERVEURS

Les accès aux outils et interfaces d'administration des serveurs sont limités aux seules personnes habilitées. Les administrateurs disposent de mots de passe spécifiques. Les systèmes d'exploitation des serveurs sont régulièrement mis à jour.

3.8 SECURISATION DES SITES WEB ET LOGICIELS

Sigma Informatique utilise des protocoles TLS sur les sites web, notamment pour les pages d'authentification, de formulaire, sur lesquelles sont affichées ou transmises des Données à Caractère Personnel. Les comptes administrateurs sont limités aux équipes en charge des actions d'administration sur les sites web et logiciel.

3.9 PROTECTION CONTRE LES VIRUS ET PROGRAMMES MALVEILLANTS

Sigma Informatique met en œuvre des mesures de détection et de prévention contre les virus et les programmes malveillants (vers, chevaux de Troie, logiciels espion, rançongiciels, etc…). Les codes mobiles (objets flash, composants Active X, etc…) en provenance d'Internet sont filtrés de manière à bloquer les programmes d'origine douteuse ou référencés comme malveillants.

3.10 CRYPTOGRAPHIE

Sigma Informatique met en œuvre des protocoles de chiffrement, de hachage et de signature électronique et encadre la gestion des clés cryptographiques et certificats numériques éventuellement associés.

3.11 LOCALISATION DES DONNEES

Les serveurs dans lesquels les Données à Caractère Personnel sont conservées sont situés en France et sur le territoire de l'Union Européenne. Les Traitements de Données à Caractère Personnel réalisés par les collaborateurs de Sigma Informatique exclusivement sont réalisés en France.

3.12 SAUVEGARDES

Les sauvegardes incrémentales et complètes des Données sont réalisées à intervalles réguliers. Les sauvegardes des Données sont stockées dans un lieu différent du lieu primaire de conservation des Données à Caractère Personnel. Les sauvegardes sur bande font aussi l'objet d'un chiffrement.

3.13 ARCHIVAGE

Les Données à Caractère Personnel qui ne sont plus en archive courante par Sigma Informatique sont conservées en archive intermédiaire pendant les délais de prescription. Elles sont accessibles de manière ponctuelle et exceptionnelle aux seules personnes autorisées à y avoir accès.

3.14 DESTRUCTION DES DONNEES

La destruction des Données à Caractère Personnel est réalisée de manière irréversible et définitive, y compris préalablement à toute réutilisation des supports. Les supports de Données en fin de vie sont physiquement détruits après effacement des Données.

MESURES DE SECURITE TECHNIQUES COMPLEMENTAIRES HDS OU SUR DEMANDE

3.15 CLOISONNEMENT RESEAU ET BASTION DE SECURITE

À travers la mise en œuvre d'un bastion de sécurité, point d'entrée unique vers les systèmes administrés, Sigma Informatique met en œuvre un cloisonnement entre les réseaux administrés et son réseau bureautique.

3.16 CHIFFREMENT DES FLUX SUR LES RESEAUX PUBLICS

Les outils et services standards utilisés pour les transferts de Données à Caractère Personnel sur les réseaux publics font usage de protocoles et d'algorithmes de chiffrement.

3.17 UTILISATION D'IDENTIFIANTS UNIQUES

L'accès aux systèmes et en particulier ceux Traitant les Données à Caractère Personnel s'effectue par l'intermédiaire du bastion de sécurité, imposant l'usage d'identifiants uniques et nominatifs.

3.18 AUTHENTIFICATION FORTE DES ADMINISTRATEURS

L'accès aux serveurs par les administrateurs de SIGMA INFORMATIQUE fait l'objet d'une authentification forte à travers le bastion de sécurité. Cette solution d'authentification forte peut être proposée, sous-réserve que cette solution soit souscrite par le Client, pour les accès d'administration des clients et tiers, tels que les éditeurs.

3.19 TRACABILITE DES ACTIONS DES ADMINISTRATEURS

Les accès et les actions des administrateurs système et opérateurs techniques vers les systèmes administrés sont tracés nominativement par la mise en œuvre du bastion de sécurité. Les traces peuvent être fournies sur demande.

3.20 TRACABILITE TECHNIQUE ET DE SECURITE

Sigma Informatique assure la traçabilité des actions des utilisateurs, des défaillances et des événements liés à la sécurité de l'information pour les composants et systèmes supportant une activité de mise à disposition d'infrastructure virtuelle, de mise à disposition de plateforme logicielle, d'administration/exploitation et de sauvegarde externalisée, dans la limite des activités sous-traitées à Sigma Informatique.

3.21 ARCHIVAGE CHIFFRE SUR BANDE

Sigma Informatique fournit, sous réserve de souscription à ce service, une rétention longue avec externalisation des données sur bandes. Les copies sont chiffrées sur bandes par AES 256 et stockées dans deux datacenters dans des bandothèques ignifugées.

PARTIE 4 – MODIFICATION DES MESURES

Sigma Informatique se réserve le droit de modifier tout ou partie des Mesures de Sécurité Techniques et Organisationnelles à tout moment et ce, sans préavis. Toutefois, ces modifications n'auront pas pour objet de dégrader le niveau de protection des Données à Caractère Personnel.

_ _

FIN DU DOCUMENT