

	Mesures Organisationnelles et Techniques de Protection des Données à Caractère Personnel gérées par Sunnikan Consulting en tant que Prestataire	SOP-04b
		Version n°1.0, du 14 Septembre 2018

	Nom, Fonction	Signature, Date
Mise en application	Georges MARTIN Gérant	Georges MARTIN Signature numérique de Georges MARTIN DN : c=FR, l=FONTENAY SOUS BOIS, o=SUNNIKAN CONSULTING, ou=SUNNIKAN CONSULTING, ou=0002 40903224000064, ou=Direction, title=Gérant, cn=Georges MARTIN, serialNumber=0001 Date : 2018.09.14 17:05:59 +02'00'

Historique des versions

Version #	Date de mise en application	Principales modifications
Version n°1.0	14 Septembre 2018	Création du document

Table des matières

1	Introduction	2
2	Mesures Organisationnelles	2
2.1	Délégué à la Protection des Données	2
2.2	Responsabilités / Personnel Sunnikan	2
2.3	Sous-traitance par Sunnikan	2
3	Confidentialité (Art. 32.1.b) du RGPD)	2
3.1	Contrôle de l'accès aux locaux Sunnikan (Fontenay-sous-Bois)	2
3.2	Contrôle de l'accès aux systèmes informatisés et aux données / Prévention et détection d'intrusion dans les systèmes informatisés	3
3.3	Contrôle de la communication de données (Transfert ou copie non autorisé de données)	3
3.4	Contrôle d'accès pour l'utilisation d'espaces spécifiques des systèmes de traitement des données	3
3.5	Cloisonnement des Traitements	4
3.6	Pseudonymisation	4
3.7	Minimisation des données	4
3.8	Chiffrement des données	4
3.9	Maîtrise des documents contenant des données à caractère personnel	4
4	Intégrité (Art. 32.1.b) du RGPD)	5
4.1	Contrôle de la saisie des Données	5
4.2	Contrôle de la transmission des Données	5
5	Disponibilité et résilience (Art. 32.1.b) du RGPD)	5
5.1	Maîtrise de la disponibilité	5
5.2	Résilience	5
6	Archivage des documents et fichiers comprenant des données à caractère personnel	5
7	Procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des Mesures Techniques et Organisationnelles pour assurer la sécurité du traitement (Art. 32.1.d) du RGPD)	5
7.1	Gestion de la protection des données	5
7.2	Gestion des incidents	6
7.3	Protection des données par défaut (Art. 25, § 2 GDPR)	6
7.4	Supervision des activités	6

	Mesures Organisationnelles et Techniques de Protection des Données à Caractère Personnel gérées par Sunnikan Consulting en tant que Prestataire	SOP-04b
		Version n°1.0, du 14 Septembre 2018

1 Introduction

Ce document décrit les mesures organisationnelles et techniques mises en place par Sunnikan afin de garantir l'intégrité et la confidentialité des données à caractère personnel traitées par Sunnikan dans le cadre de ses prestations.

2 Mesures Organisationnelles

2.1 Délégué à la Protection des Données

Sunnikan a nommé un Délégué à la Protection des Données, déclaré à la CNIL, disponible aux coordonnées suivantes :

- dpd@sunnikan.com
- dpo@sunnikan.com
- Délégué à la Protection des Données à Caractère Personnel
Sunnikan Consulting
229-231, rue La Fontaine
94120 - Fontenay-sous-Bois
France

2.2 Responsabilités / Personnel Sunnikan

Chaque collaborateur Sunnikan a signé une clause de confidentialité et de protection des données dans le cadre de son contrat de travail.

Les responsabilités des collaborateurs Sunnikan relatives à la protection des données à caractère personnel sont définies dans les Définitions de Fonction correspondantes.

Le personnel Sunnikan est formé initialement et périodiquement :

- aux exigences de la réglementation applicable au traitement de données à caractère personnel,
- à la politique et aux procédures Sunnikan relatives au traitement de données à caractère personnel.

2.3 Sous-traitance par Sunnikan

De façon générale, Sunnikan ne sous-traite pas la réalisation de tout ou partie des prestations (pouvant comprendre un traitement de données à caractère personnel).

3 Confidentialité (Art. 32.1.b) du RGPD)

3.1 Contrôle de l'accès aux locaux Sunnikan (Fontenay-sous-Bois)

Sunnikan Consulting est situé dans un immeuble de bureaux :

229-231, rue La Fontaine
94120 - Fontenay-sous-Bois
France

L'accès au bâtiment est restreint par un digicode.

Les locaux Sunnikan sont situés au 2^{ème} étage du bâtiment, restreignant les possibilités d'intrusion par une fenêtre.

	Mesures Organisationnelles et Techniques de Protection des Données à Caractère Personnel gérées par Sunnikan Consulting en tant que Prestataire	SOP-04b
		Version n°1.0, du 14 Septembre 2018

L'accès aux bureaux Sunnikan est restreint par :

- un badge (la journée),
- une clé de sécurité (la nuit).

Les badges et les clés sont alloués de façon nominative aux membres du personnel.

En cas d'absence, les locaux sont protégés par :

- un système de détection d'intrusion et de vidéoprotection, déclenché quand les locaux sont sous alarme, et géré à distance par la société VERISURE,
- un système de vidéoprotection interne activé la nuit et les week-ends.

3.2 Contrôle de l'accès aux systèmes informatisés et aux données / Prévention et détection d'intrusion dans les systèmes informatisés

Les systèmes informatiques comprennent : l'infrastructure réseau informatique, les postes individuels, des emplacements dans le nuage.

L'accès au réseau informatique est restreint par un système de gestion d'accès centralisé par identification et mot de passe personnels (Domaine Active Directory). Le mot de passe doit être changé périodiquement et doit obéir à des règles de complexité et d'antériorité conformes aux exigences de la CNIL.

Les droits d'accès aux systèmes informatisés sont décidés par le Gérant et attribués par l'Ingénieur Système et Réseaux. Le processus est documenté.

Une revue des accès est réalisée périodiquement.

Les personnes autorisées à accéder aux systèmes informatisés sont :

- les Consultant(es),
- les fonctions Support : Assistante, Gestionnaire de Mission, Ingénieur Systèmes et Réseaux.

Ce processus permet de garantir l'accès aux systèmes et aux données uniquement aux personnes autorisées.

Les documents relatifs aux prestations sont gérés sur la plate-forme SharePoint, et font l'objet d'un suivi de version ("audit trail") traçant tout ajout, modification, ou suppression de ces documents.

La prévention et la détection d'intrusion comprennent également les dispositifs suivants :

- Vérification périodique des journaux d'accès ("logs").
- Fonctionnalité de détection d'intrusion de la plate-forme Office 365.
- Détection heuristique d'intrusion par pare-feu SOPHOS XG.
- Cloisonnement physique des réseaux informatiques invités (accès Web invités) et du personnel.

Un système d'alertes de sécurité, basé sur une solution SYMANTEC, a été mis en place.

3.3 Contrôle de la communication de données (Transfert ou copie non autorisé de données)

Les documents relatifs aux prestations (et pouvant contenir des données à caractère personnel) sont hébergés sur une plate-forme SharePoint.

3.4 Contrôle d'accès pour l'utilisation d'espaces spécifiques des systèmes de traitement des données

Sunnikan utilise les espaces spécifiques suivants :

- un espace SharePoint (prestataire : Microsoft, serveur localisé en Europe), documentant les prestations,

	Mesures Organisationnelles et Techniques de Protection des Données à Caractère Personnel gérées par Sunnikan Consulting en tant que Prestataire	SOP-04b
		Version n°1.0, du 14 Septembre 2018

- une messagerie Exchange (prestataire : Microsoft, serveur localisé en Europe), incluant un répertoire des clients et prospects,
- un espace de stockage sur un serveur interne,
- un espace intranet interne, hébergé en France par le prestataire CELESTE, et géré par le prestataire FOCUS INOVA.

L'accès à ces espaces est restreint aux personnes autorisées à accéder aux systèmes informatisés.

En particulier, les accès VPN sont liés à un compte AD (Active Directory).

3.5 Cloisonnement des Traitements

Les documents relatifs aux prestations sont gérés dans des bibliothèques de documents de l'espace SharePoint, chaque prestation étant cloisonnée dans son propre site séparé des autres.

Les courriels relatifs aux prestations sont stockés et cloisonnés dans leur propre dossier d'une Boîte aux Lettres Exchange.

3.6 Pseudonymisation

Les données à caractère personnel des sujets participant à des recherches cliniques sont systématiquement pseudonymisées. De façon générale, les Consultants Sunnikan travaillent sur ces données.

En tant qu'Auditeurs, dans le cadre de leurs prestations sur site d'investigation (ex : audit de site d'investigation), les Consultants peuvent prendre connaissance de données directement nominatives dans le cadre de l'article L. 1121-3 du Code de la santé publique. Seules les données pseudonymisées font l'objet de prise de note.

Les documents des prestations peuvent comporter des données à caractère personnel (en particulier de santé) de patients et de professionnels de santé, dans le cadre d'une Méthodologie de Référence ou d'une autorisation de la CNIL.

3.7 Minimisation des données

Dans le cadre de leurs prestations, les Consultants ne collectent que les données strictement nécessaires à l'exécution de leur prestation.

3.8 Chiffrement des données

Les disques durs des ordinateurs du personnel Sunnikan (portables des Consultants, postes fixes des autres catégories de personnel) sont cryptés par la solution BitLocker.

3.9 Maîtrise des documents contenant des données à caractère personnel

Les documents de prestations pouvant comprendre des données à caractère personnel sont systématiquement gérés sur la plate-forme SharePoint qui dispose de fonctionnalités :

- de restriction d'accès aux personnes autorisées,
- de détection d'intrusion,
- de gestion des versions ("audit trail").

	Mesures Organisationnelles et Techniques de Protection des Données à Caractère Personnel gérées par Sunnikan Consulting en tant que Prestataire	SOP-04b
		Version n°1.0, du 14 Septembre 2018

4 Intégrité (Art. 32.1.b) du RGPD)

4.1 Contrôle de la saisie des Données

Les Consultants ne font pas de saisie de données à caractère personnel lors de leurs prestations. Lors de leurs prestations, les Consultants peuvent mentionner certaines données à caractère personnel de patients dans leurs Rapports d'Audit.

4.2 Contrôle de la transmission des Données

Sunnikan ne dispose pas d'une ligne téléphonique dédiée aux fax, et n'envoie, ni ne reçoit de fax.

5 Disponibilité et résilience (Art. 32.1.b) du RGPD)

5.1 Maîtrise de la disponibilité

Le système d'information Sunnikan est sous le contrôle permanent d'un Ingénieur Système et Réseaux (personnel Sunnikan à temps plein).

Des plans de continuité d'activité et de restauration d'activité sont en place.

5.2 Résilience

Les systèmes informatisés Sunnikan :

- sont dotés de redondances,
- sont monitorés en continu,
- sont maintenus par l'Ingénieur Système et Réseaux Sunnikan et par le prestataire FOCUS INOVA.

Les données font l'objet de sauvegardes périodiques, contrôlées et externalisées, conformément à des spécifications pré-établies.

6 Archivage des documents et fichiers comprenant des données à caractère personnel

Les documents (tant papier qu'électroniques) pouvant contenir des données personnelles sont stockés dans des endroits appropriés et sécurisés

7 Procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des Mesures Techniques et Organisationnelles pour assurer la sécurité du traitement (Art. 32.1.d) du RGPD)

7.1 Gestion de la protection des données

La procédure Sunnikan intitulée "Personal Data Protection" (SOP-04) détaille les modalités de suivi, d'analyse et d'évaluation régulière de l'efficacité des mesures organisationnelles et techniques destinées à assurer la sécurité des traitements de données personnelles, incluant :

- la revue périodique des systèmes informatisés,
- la revue périodique du système de management de la qualité,
- la revue périodique du système de protection des données à caractère personnel.

	Mesures Organisationnelles et Techniques de Protection des Données à Caractère Personnel gérées par Sunnikan Consulting en tant que Prestataire	SOP-04b
		Version n°1.0, du 14 Septembre 2018

7.2 Gestion des incidents

Les incidents pouvant impacter le traitement de données à caractère personnel sont gérés directement par :

- le Gérant de Sunnikan,
- l'Ingénieur Système et Réseaux Sunnikan,
- le Consultant Senior responsable de la prestation concernée (si applicable).

Le Gérant en informe le Délégué à la Protection des Données.

Les incidents significatifs sont spécifiquement documentés.

7.3 Protection des données par défaut (Art. 25, § 2 GDPR)

La protection par défaut des données à caractère personnel est, en particulier, assurée par les mécanismes suivants :

- la formation des Consultants et des Fonctions Support,
- l'utilisation exclusive de données pseudonymisées pour les données de santé,
- le cryptage des disques durs des ordinateurs portables des Consultants,
- la mise en application de la procédure Sunnikan relative à la protection des données à caractère personnel lors des prestations réalisées par Sunnikan.

7.4 Supervision des activités

Les activités impliquant la manipulation de données à caractère personnel lors des prestations sont encadrées par un Consultant Senior.

L'Ingénieur Système et Réseaux réalise un monitoring permanent et documenté du système d'information Sunnikan sur une plateforme GLPI.