SELLIGENT MARKETING CLOUD
Conditions spécifiques relatives aux données de santé

(05-03-2021)

CONDITIONS SPECIFIQUES RELATIVES AUX DONNEES DE SANTE

(Mise en ligne le 5 mars 2021)

1. **Par dérogation à l'article 8 du Contrat-cadre de Services, il est convenu que des données relatives à la santé peuvent être hébergées sur la Plateforme Selligent dans le respect par le Client des conditions ci-après.**

2. Le Client reconnaît avoir mis en place, et s'engage à maintenir pendant toute la durée du Contrat, un système d'information de santé respectant la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) promulguée par l'Agence Française de la Santé Numérique, et toute autre texte venant compléter ou remplacer la PGSSI-S dans la mesure de son applicabilité aux donnes de santé traitées par le Client.

3. Le Client s'engage en particulier à se tenir informer des référentiels opposables inscrits dans la PGSSI-S et à les respecter, pendant toute la durée du Contrat.

4. Le Client s'engage à communiquer à Selligent, dans le Bon de Commande des Services à souscription, les informations suivantes, et à tenir Selligent informée sans délai de toutes modifications éventuelles de ces informations :
    i. La raison sociale du Client ;
    ii. Les nom et prénom du contact du Client ;
    iii. L'adresse mail du contact du Client ;
    iv. Le numéro de téléphone du contact du Client.

5. Le respect des engagements ci-dessus est une condition sine qua non de l'hébergement des Données du Client relatives à la santé sur la Plateforme Selligent. Selligent a le droit de suspendre avec effet immédiat l'accès du Client à la Plateforme Selligent en cas de défaut de conformité aux engagements visés ci-dessus jusqu'à la démonstration par le Client qu'il a remédié à ce(s) défaut(s) de conformité. A défaut de conformité aux engagements visés ci-dessus dans un délai de 15 jours, ou toute autre délai imposé par une disposition légale applicable en la matière, Selligent aura le droit de supprimer toutes les Données du Client hébergées sur la Plateforme Selligent. Les redevances pour les Services à souscription restent intégralement dues pendant toute période de suspension, ou en cas de suppression des données pour défaut de conformité du Client.

6. Selligent dispose des certifications ISO/IEC 27001:2013 – ISO/IEC 27018:2014 et HDS.. Selligent communiquera au Client, sur demande de ce dernier, les rapports d'audit de certification. En cas de perte de la certification HDS, Selligent s'engage à restituer les données de santé au Client qui s'engage à ne plus les exporter sur la Plateforme Selligent. Les domaines d'application des certifications sont repris ci-dessous.

7. Les pays où les données relatives à la santé peuvent être hébergés sont la Belgique, les Pays-Bas et l'Allemagne. Selligent communiquera au Client tout changement de localisation des hébergements possibles des données relatives à la santé. Nonobstant toute disposition dérogatoire éventuellement incluse dans le DPA applicable entre les parties, les Services d'assistance impliquant un traitement des données relatives à la santé seront réalisés par Selligent SA et Selligent France.

Libellé certificat ISO/IEC 27001:2013

Delivery and support processes for a secure operation of the Selligent Software as a Service Solution to customers, as well as Selligent Internal Networks and Software Research and Development processes.
Traduction libre

Processus de livraison et de support pour une exploitation sécurisée de la solution logicielle Selligent en tant que service destiné aux clients, ainsi que des processus Selligent de réseaux internes et de recherche et développement de logiciels.

Domaine d'application ISO/IEC 27001:2013

ISO 27001:2013 Contrôles	Application
A.5 Politiques de sécurité de l'information	OUI
A.6 Organisation de la sécurité de l'information	OUI
A.7 Sécurité des ressources humaines	OUI
A.8 Gestion des actifs	OUI
A.9 Contrôle d'accès	OUI
A.10 Cryptographie	OUI
A.10.1 Mesures cryptographiques	OUI
A.11 Sécurité physique et environnementale	OUI
A.12 Sécurité liée à l'exploitation	OUI
A.12.1 Procédures et responsabilités liées à l'exploitation	OUI
A.12.2 Protection contre les logiciels malveillants	OUI
A.12.3 Sauvegarde	OUI
A.12.4 Journalisation et surveillance	OUI
A.12.5 Maîtrise des logiciels en exploitation	OUI
A.12.6 Gestion des vulnérabilités techniques	OUI
A.12.7 Considérations sur l'audit des systèmes d'information	OUI
A.13 Sécurité des communications	OUI
A.14 Acquisition, développement et maintenance des systèmes d'information	OUI
A.15 Relations avec les fournisseurs	OUI
A.16 Gestion des incidents liés à la sécurité de l'information	OUI
A.17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	OUI
A.18 Conformité	OUI

Libellé certificat HDS

« Processus de délivrance et d'assistance pour une exploitation sécurisée de la solution logiciel Selligent en tant que service, ainsi que les processus Selligent de gestion des réseaux internes et recherche et développement de logiciel »

La certification HDS de Selligent comprend les activités d'hébergeur infogéreur et d'hébergeur d'infrastructures. Plus spécifiquement, les activités 1 à 6 sont couvertes :

- La mise à disposition et le 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 ;
- La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé ;
- La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;
- La mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;
- L'administration et l'exploitation du système d'information contenant les données de santé;
- La sauvegarde de données de santé.

Domaine d'application certificat Hébergeur de Données de Santé

Exigences	Application	Conformité
ISO27001	Les hébergeurs d'infrastructure physique et les hébergeurs infogéreurs doivent être certifiés NF ISO 27001.	Oui
	Exigence complémentaire (chapitre 4.3 de la norme NF ISO 27001)	Oui
	Exigence complémentaire (chapitre 6.1.3 de la norme NF ISO 27001)	Oui
	Exigence complémentaire (Annexe A12.3 de la norme NF ISO 27001)	Oui
	Exigence complémentaire (Annexe A12.7 de la norme NF ISO 27001)	Oui
4.3. Exigences NF ISO 20000-1		
	4.3.1 Planification de nouveaux services ou de services modifiés (1/2)	Oui
	4.3.1 Planification de nouveaux services ou de services modifiés (2/2)	Oui
	4.3.2 Conception et implémentation des nouveaux services ou des services modifiés : Présentation des activités exécutées par les fournisseurs de services, clients et autres parties	Oui
	Exigence complémentaire (chapitre 5.3 de la norme NF ISO 20000-1)	Oui
	4.3.3. Continuité de services et gestion de la disponibilité : 4.3.3.1 Exigences de continuité et de disponibilité de services Le chapitre 6.3 de la norme NF ISO 20000-1 (1/2)	Oui

	4.3.3. Continuité de services et gestion de la disponibilité : 4.3.3.1 Exigences de continuité et de disponibilité de services Le chapitre 6.3 de la norme NF ISO 20000-1 (2/2)	Oui
	4.3.3. Continuité de services et gestion de la disponibilité : 4.3.3.2. Gestion de la capacité Le chapitre 6.5 de la norme NF ISO 20000-1	Oui
4.4. Exigences relatives à la protection des données de santé à caractère personnel		
	4.4.1. Droits des personnes: 4.4.1.1. Obligation de coopérer	Oui
	4.4.2. Finalité	Oui
	4.4.3. Communication des données: 4.4.3.1. Données temporaires	Oui
	"4.4.3.2. Notification en cas de communication de données à caractère personnel	Oui
	4.4.3. Communication des données: 4.4.3.3. Traçabilité en cas de communication	Oui
	4.4.3. Communication des données: 4.4.3.1. Intégrité et acquittement des échanges	Oui
	4.4.4. Transparence: 4.4.4.1. Obligation d'information en cas de sous-traitance	Oui
	4.4.5. Responsabilité 4.4.5.1. Notification en cas d'atteinte à la sécurité des données	Oui
	4.4.5. Responsabilité 4.4.5.2. Période de conservation des politiques de sécurité	Oui
	4.4.5. Responsabilité 4.4.5.3. Gestion des informations personnelles	Oui
	4.4.6. Sécurité des données 4.4.6.1. Les accords de confidentialité ou de non-divulgation	Oui
	4.4.6. Sécurité des données 4.4.6.2. Restriction sur l'usage de copies papier	Oui
	4.4.6. Sécurité des données 4.4.6.3 Contrôle et traçabilité lors de la restauration de données	Oui
	4.4.6. Sécurité des données 4.4.6.4. Protection des données présentes sur un support de stockage en dehors du lieu d'hébergement	Oui
	4.4.6. Sécurité des données 4.4.6.5. Utilisation de support de stockage portable	Oui
	4.4.6. Sécurité des données 4.4.6.6. Chiffrement des données personnelles transmises sur des réseaux publics	Oui
	4.4.6. Sécurité des données 4.4.6.7. Destruction des copies papier	Oui
	4.4.6. Sécurité des données 4.4.6.8. Utilisation d'identifiants uniques	Oui

	4.4.6. Sécurité des données 4.4.6.9. Gestion des habilitations	Oui
	4.4.6. Sécurité des données 4.4.6.10. Gestion des traces	Oui
	4.4.6. Sécurité des données 4.4.6.10. Gestion des traces (Exigence complémentaire)	Oui
	4.4.6. Sécurité des données 4.4.6.11. Gestion des identifiants	Oui
	4.4.6. Sécurité des données 4.4.6.12. Clauses contractuelles	Oui
	4.4.6. Sécurité des données 4.4.6.13. Sous-traitance du traitement des données personnelles	Oui
	4.4.6. Sécurité des données 4.4.6.14. Réutilisation des espaces de stockage	Oui
	4.4.7. Localisation des données 4.4.7.1. Lieux d'hébergement	Oui
4.5. Exigences complémentaires		
	4.5.1. Rôles et responsabilités	Oui
	4.5.2. Conformité aux référentiels opposables de la PGSSI-S	Oui
	4.5.3. Rapports d'audit	Oui
	4.5.4. Liste des contacts clients	Oui
	4.5.5. Régionalisation	Oui