



Prochains sommaires

Abonnez-vous



RGPD

RGPD : Asklepian aide les professionnels de santé à rattraper leur retard pour éviter les sanctions

janvier 2021 par Asklepian

En décembre 2020, deux médecins libéraux ont écopé d'amendes de 3000 et 6000 euros de la part de la Commission Nationale de l'Informatique et des Libertés (CNIL) pour avoir "insuffisamment protégé les données personnelles de leurs patients" et ne pas avoir notifié la commission de cette violation des données (source).

Cette sanction rappelle brutalement une règle essentielle aux professionnels de santé (professions libérales, généralistes et spécialistes, pharmacies, cabinets de radiologies, dentaires, chirurgies, cliniques, hôpitaux...) et ceux du secteur paramédical (ambulanciers, ostéopathes, psychologues...) : ils sont aussi concernés par l'obligation de se conformer au règlement général de protection des données (RGPD). Or dans le contexte actuel de pandémie de Covid-19 et de généralisation du dossier médical partagé qui va s'intensifier dans les deux ans à venir (source), ils sont appelés à traiter toujours plus de données sensibles.

De plus, parce qu'ils sont particulièrement dépendants des outils numériques, les professionnels de santé deviennent une cible de choix et les cyberattaques se multiplient. A titre d'exemple, le 21 décembre, l'hôpital d'Albertville (Savoie) a été victime d'un "rançongiciel" qui a endommagé son système d'information (source).

Les conséquences humaines et financières peuvent être très lourdes. Il est strictement indispensable de mettre en œuvre les mesures adéquates et pertinentes pour garantir un haut niveau de disponibilité, de confidentialité et d'intégrité des données pour éviter toutes pertes de données, atteintes à la vie privée, activités qui doit s'interrompre au détriment d'actes médicaux indispensables pour la vie des patients...

Or se conformer au RGPD peut être particulièrement complexe à mettre en œuvre. Il faut maîtriser ses systèmes et pouvoir démontrer que toutes les mesures de sécurisation technique et organisationnelle sont mises en œuvre, les postes de travail et l'informatique mobile, sécuriser les serveurs et les archives, utiliser des techniques de chiffrement... En bref, un vrai casse-tête pour ces professionnels dont ce n'est pas le métier et qui doivent jongler avec un planning surchargé ! Pour les aider à se conformer à leurs obligations, Asklepian leur propose un accompagnement sur-mesure pour sécuriser toutes les données et respecter le RGPD.

Une palette d'outils & de services spécialement adaptés aux professionnels de santé

Asklepian propose un programme d'accompagnement "à la carte" en fonction des besoins spécifiques de chacun.e : Prestation 1 : Les conseils de mise en conformité RGPD Ces sessions peuvent être organisées de façon collective ou individuelle. Pendant 9 mois, à raison d'un atelier par mois, les professionnels de santé vont être aidés, guidés, conseillés, relus et corrigés par un délégué à la protection des données certifié.

Ils profitent de :

- 9 séances collectives ou individuelles pour définir leurs objectifs, les trames documentaires et co-construire leur projet de mise en conformité ;
- 9 phases de travail individuel ;
- 9 phases de conseils personnalisés (relecture et correction).

Fabien Fernandez, le fondateur, souligne : « Ce programme d'accompagnement à la mise en conformité a été spécialement conçu pour s'adapter aux attentes et au planning surchargé des professionnels de santé. »

Prestation 2 : La mise en conformité RGPD clé en main

Très appréciée, cette prestation permet de n'avoir à se soucier de rien ! Les équipes d'Asklepian vont se charger de tout : elles réalisent tous les audits préalables, toute la documentation, effectuent des recommandations et accompagnent leur mise en œuvre. Durée : de 9 mois à 1 an.

Prestation 3 : L'externalisation des compétences de délégué à la protection des données

Les activités du délégué à la protection des données externalisées consistent à apporter une expertise sur le RGPD :

1. Informer et sensibiliser, diffuser une culture « Informatique et Libertés ».
2. Veiller au respect du cadre légal.
3. Informer et responsabiliser, alerter si besoin, son responsable de traitement.
4. Analyser, investiguer, auditer, contrôler
5. Établir et maintenir une documentation au titre de « l'Accountability » pour documenter toute la conformité.
6. Assurer la médiation avec les salariés et les patients.

Les événements

Jeu du Calendrier 2021



précédent

suivant

Voir tous les événements

algosecure
Keep It Safe and Secure

Entreprise experte en
cybersécurité



LE VPN FRANÇAIS
L'allié cybersécurité du secteur public

Vulnérabilités

- Vigil@nce - Das U-Boot : utilisation de (...)
- Vigil@nce - SDDM : élévation de privilèges via (...)
- Vigil@nce - tcpdump : déni de service via PPP (...)
- Vigil@nce - phpMyAdmin : exécution de code via (...)



All our news in english

- Vigil@nce - Das U-Boot: use after free via (...)
- Vigil@nce - SDDM: privilege escalation via X (...)
- Matrix PTZ IP Camera - Glitch-free & (...)
- Comment: Expiring Android versions leave (...)

Abonnez-vous gratuitement à
notre NEWSLETTER

Votre e-mail

☐ Newsletter FR

☐ Newsletter EN

☐ Vulnérabilités**S'ABONNER**[► Se désabonner](#)

7. Interagir avec l'autorité de contrôle.
8. Être le point de contact entre tous les acteurs sur tous les sujets autour de la protection des données (CNIL, responsables, sous-traitants, clients, salariés...).
9. Accompagner la mise en place de mesures techniques et organisationnelles.

Sa présence peut notamment permettre d'éviter le prononcé d'une amende ou même d'une astreinte par la CNIL, qui interdirait alors aux professionnels de santé de continuer le traitement des données.

Asklepian : une expertise avérée et une approche à 360° du RGPD

Asklepian est une référence en matière de sécurité informatique et des réseaux. Ses compétences de Délégué à la protection des données (DPO) sont d'ailleurs certifiées par l'AFNOR selon l'agrément CNIL. Asklepian est également membre de l'Association Française des Correspondants à la protection des Données à caractère personnel, ce qui lui permet de signer une charte de déontologie afin de promouvoir une culture de l'éthique parmi les DPO désignés auprès de la CNIL au titre du RGPD.

Libérateur d'énergie au service des entreprises, Asklepian peut intervenir dans plusieurs registres :

- Consultant en Stratégie et en Organisation ;
- Spécialiste en Protection des Données : diagnostics, audits, mise en oeuvre du RGPD, DPO externalisé... ;
- Accompagnement à la Transition Numérique et Expertise en simplification des processus de dématérialisation ;
- Conseils et services supports aux entreprises, et de la Gestion de projets.

Une spécialisation sur les secteurs sensibles

Fabien Fernandez a piloté les démarches de certification ISO27001 et Hébergement de données de santé d'un data-center de proximité. Il est également intervenu auprès des auditeurs de la session nationale de l'Institut des hautes études de défense nationale (IHEDN) en partageant des réflexions sur les enjeux de la souveraineté numérique et de la cybersécurité :

- Comment favoriser la cybersécurité nationale en proposant une stratégie de cyber sécurisation pour tout adapter au budget de chacun ?
- Comment démontrer sa conformité au RGPD et répondre au principe de l'accountability et comment parvenir à la maîtrise de ses systèmes ?
- La force d'un Data Center de proximité au service de son territoire : garantir un haut niveau de disponibilité, d'intégrité et de confidentialité sur ses données
- Comment sensibiliser le plus grand nombre aux enjeux de la souveraineté numérique ?

Un pôle de compétences

Asklepian dispose de services complémentaires pour accompagner ses clients dans tous les domaines liés à la protection des données : Un service Organisationnel pour mettre en œuvre les mesures organisationnelles adéquates et cohérentes afin de sécuriser les données à caractère personnel (optimisation des systèmes, définition/formalisation/simplification des procédures).

Un service Juridique pour sécuriser juridiquement la documentation lors de contractualisation avec des sous-traitants ou de rédactions de mentions d'information, légales ou politiques...

Un service Sécurité des systèmes d'information et Cybersécurité pour élaborer une stratégie de sécurisation du SI, sécuriser les infrastructures, proposer et piloter un plan de continuité et de reprise d'activité ou pour auditer et identifier des vulnérabilités du SI des organisations.

Une démarche pédagogique

Le service juridique d'Asklepian, en relation constante avec l'équipe commerciale, effectue notamment une veille juridique et technologique quotidienne pour garantir à ses clients des connaissances actualisées en permanence.

En parallèle, Asklepian a lancé une web-série qui comporte 36 épisodes, 1 teaser et 1 film d'entreprise. Elle aborde tous les thèmes du RGPD, chaque semaine, dans une vidéo en format court et adaptée aux réseaux sociaux. Elle est diffusée sur le compte LinkedIn d'Asklepian.

[Twitter](#)[J'aime 0](#)[Partager](#)[► Voir les articles précédents](#)

[Actu](#) [Dossiers](#) [Cyber Sécurité](#) [RGPD](#) [Vulnérabilités](#) [Malwares](#) [Agenda](#) [Guide](#) [Carrière](#) [GS Days](#) [JOBS](#) [Contact](#) [A propos](#) [Mentions légales](#) [S'identifier](#)

ADMIN

Global Security Mag Copyright 2011