JOURNAL SPÉCIAL DES SOCIÉTÉS

Asklépian, la start-up qui accompagne les entreprises dans leur mise en conformité au RGPD - Entretien avec son fondateur, Fabien Fernandez

Publié le 22/03/2021 10:10

ACTUALITE

Ecoutez

Depuis mai 2018, les entreprises françaises sont dans l'obligation de se conformer au règlement général de protection des données, plus connu sous l'acronyme RGPD. Loin de la théorie, la mise en pratique n'est pas toujours simple. Dans ce contexte, Asklépian vise à les accompagner dans leur mise en conformité, avec un accompagnement sur mesure. En pleine crise sanitaire, elle met actuellement un point d'honneur à soutenir les professionnels de santé dans cette démarche, ces derniers étant devenus la cible des cyberattaques.

Pouvez-vous nous présenter Asklépian ?

Nous vivons à l'époque du big data : ces dernières années, la quantité de données a explosé, à cause de la dématérialisation des activités professionnelles, personnelles, administratives, de la numérisation, de la vidéo-surveillance, des réseaux sociaux et de la géolocalisation.

Bon nombre des données recueillies par les entreprises sont donc éminemment sensibles. La transition numérique dans laquelle est engagée la société ne fait qu'augmenter les risques. D'un côté, les données sont à la base du développement économique des entreprises, mais, de l'autre, elles peuvent être leur talon d'Achille. Mal protégées, elles sont à la merci des pirates qui utilisent des techniques toujours plus sophistiquées pour déjouer les systèmes de sécurité.

Le 25 mai 2018, le Règlement Général sur la Protection des Données européen (RGPD) est entrée en application, conférant aux entreprises une immense responsabilité : celle de protéger les données à caractère personnel de leurs clients, partenaires et collaborateurs, sous peine d'amendes et de sanctions.

Deux ans plus tard, le bilan est contrasté. Le RGPD a entraîné une prise de conscience des risques liés aux données, mais malheureusement, trop d'entreprises ne sont toujours pas en conformité avec les exigences de la nouvelle législation.

Le contexte sanitaire exceptionnel que nous traversons, avec la pandémie de coronavirus, n'a pas arrangé les choses. Les organisations ont adopté le télétravail en masse, ce qui a bousculé les procédures internes au détriment des mesures de sécurité techniques et organisationnelles… et pour le plus grand bonheur des criminels.

Aujourd'hui, les entreprises et les organisations ne peuvent plus faire face seules aux nouveaux enjeux de la protection des données. Elles ont besoin d'un accompagnement, d'un interlocuteur qui leur fournisse les informations et les outils dont elles ont besoin pour être en conformité avec le RGPD.

C'est pour cela que j'ai créé Asklépian. Notre mission est de faciliter la vie des organisations, en les aidant dans la maîtrise et la documentation de leurs systèmes

numériques et physiques.

Quel regard portez-vous, de façon générale, sur la mise en conformité des entreprises françaises ?

Les données, plus que l'or noir du 21e siècle, constituent un atout stratégique majeur pour les États : renseignement, profilage, surveillance, bonne administration du territoire… mais aussi pour l'ensemble du monde économique et professionnel dont les données sont maintenant à la base de leur développement.

Les utilisations des données personnelles sont multiples et les organisations n'ont pas attendu l'avènement de l'ère numérique pour en tirer profit.

Le numérique est partout, dans toutes les activités humaines, et il soutient l'ensemble des métiers (qu'ils soient privés ou publics). Au départ, le but est de créer du progrès, relier les uns aux autres, faciliter les activités. La technologie a permis de nous relier toujours plus nombreux (quantité), toujours plus vite (référentiel temporel), en partageant énormément d'éléments, et ce à l'autre bout du monde (référentiel espace – le cyber espace). C'est une chance, mais ne négligeons pas, tous ensemble, le risque, les risques associés à ces transmissions de données.

La CNIL et l'ANSSI ont vraiment mis les moyens pour communiquer, éduquer, expliquer et synthétiser… Il y a trois ans, les entreprises françaises se sont mises un coup de pression par peur des sanctions de la CNIL… Je suis convaincu que l'on ne doit pas aborder sa conformité par peur d'une sanction, mais bien uniquement dans le but de sécuriser ses systèmes. La peur de la sanction est vite retombée et bon nombre d'entreprises sont bien loin d'avoir abordé leur mise en conformité eu égard aux exigences du RGPD.

Mais la situation a bien changé. Les entrepreneurs connaissent tous quelqu'un qui connaît quelqu'un qui a été victime d'une cyberattaque ou qui s'est retrouvé avec son système informatique paralysé. Le nombre de cyberattaques a explosé avec la Covid-19.

Les entrepreneurs doivent prendre la mesure des enjeux d'une bonne sécurisation : cela passe par une bonne maîtrise de ses systèmes, de son environnement et par la mise en œuvre de mesures organisationnelles et techniques documentées.

Nous devons renforcer les actions de sensibilisation et proposer des prestations qui correspondent à toutes les configurations. Chez Asklépian, nous avons fait le choix de concevoir une méthodologie qui s'adapte à toutes les entreprises, à toutes les associations et à toutes les collectivités.

« Le RGPD a entraîné une prise de conscience des risques liés aux données, mais malheureusement, trop d'entreprises ne sont toujours pas en conformité avec les exigences de la nouvelle législation. »

Ces compétences entrepreneuriales, mais aussi de protection des données, ne s'improvisent pas. Pouvez-vous revenir sur votre parcours ?

Je suis un des premiers Délégué à la protection des données (DPO) certifiés sous l'agrément de la CNIL. Je suis titulaire d'une licence pluridisciplinaire en Sciences Fondamentales Appliquées de l'Université de Bourgogne avec des surspécialisations en informatique.

Fort de dix ans d'expérience dans des fonctions publiques étatiques ou territoriales, j'ai eu la chance d'avoir un parcours riche et varié qui m'a donné de solides connaissances de l'organisation administrative de la France dans différents domaines techniques.

En 2018, j'ai participé à la mise en œuvre de la réforme de décentralisation du stationnement sur l'ensemble de la ville de Bordeaux. Cela m'a permis de développer des connaissances techniques supplémentaires en finances et marchés publics, et de construire une réelle expertise des politiques publiques territoriales/locales.

En 2019, je fonde Asklépian. Au fur et à mesure des missions que j'effectue en France et à l'étranger, je constate que, malgré le Brexit, il n'existe pas de solution fiable de protection des données pour les entreprises britanniques et basées en dehors de l'Union européenne. Je décide alors de créer une nouvelle offre d'*Outsourcing UE Representative* à destination du Royaume-Uni qui pourrait se développer en Afrique du nord, au Canada, aux États-Unis et en Asie.

Vos compétences de Délégué à la protection des données (DPO) sont certifiées par l'AFNOR selon l'agrément CNIL. Qu'est-ce que cela signifie ?

Nos compétences de délégués à la protection des données d'Asklépian sont reconnues et certifiées conformément au référentiel de certification des compétences du DPO de la CNIL. J'ai obtenu cette certification par l'AFNOR, le premier organisme agrémenté. Cette certification est un vecteur de confiance pour notre réseau (clients, collaborateurs, sous-traitants, fournisseurs…) puisque nous avons validé les 17 compétences et savoir-faire attendus d'un délégué à la protection des données.

Nous avons piloté les démarches de certification ISO 27001 et Hébergement de données de santé d'un data-center de proximité.

Notre expérience a été saluée lors de mon intervention auprès des auditeurs de la session nationale de l'Institut des hautes études de défense nationale (IHEDN), lors de laquelle j'ai partagé 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 ?

Concrètement, comment accompagnez-vous les entreprises à se conformer au RGPD ?

Nous avons développé une méthode Asklépian que nous avons protégée. Elle s'adapte à tous ! Le but n'est pas de subir le RGPD, mais d'en faire une force.

Bien plus que de sécuriser les systèmes, nous allons aider les responsables à mieux identifier pour mieux maîtriser leurs systèmes. Nous allons donc en profiter pour tout revoir dans l'organisation.

La mise en œuvre du RGPD doit absolument être abordée de manière transversale par une bonne coordination des services et des acteurs, en se structurant sur trois piliers :

1. Le pilier organisationnel : prendre le temps de définir son contexte, son environnement, ses activités, ses fonctions, son organisation, ses compétences internes/externes, ses process, pour répondre aux Quoi ? Pourquoi ? Qui ? Pourquoi ? Où-Quand ? Combien ? et enfin Comment ? La fameuse procédure.
2. Le pilier technique : et dans cet ordre-là ! Vous l'aurez compris, c'est dans ce pilier que sera abordée la mise en œuvre de mesures de sécurisations techniques. Il ne s'agit pas de se limiter à l'installation d'un antivirus gratuit. Nous accompagnons nos clients, leurs informaticiens internes/externes à définir des stratégies adaptées. On ne sécurise pas l'accès à des documents sur un serveur avant d'avoir clairement défini préalablement la procédure organisationnelle…
3. Le pilier documentaire : pour formaliser, pour expliquer, pour démontrer, pour rendre compte, pour suivre, pour agir, pour preuves opposables.

Ces réglementations sont pertinentes pour optimiser les organisations : mieux maîtriser son système pour protéger les DCP mais aussi gagner en rentabilité, en efficacité tout en redonnant du sens aux activités de leurs collaborateurs.

Je vais prendre le temps de vous raconter une anecdote pour illustrer la force du RGPD et les bénéfices pour une entreprise. Un cabinet médical qui continuait d'imprimer une page A4 d'étiquettes autocollantes pour chaque patient ; 40 000 patients par an. À l'époque, ces étiquettes permettaient d'assurer le suivi du patient durant son parcours. Aujourd'hui les résultats sont consultables en ligne, les CD sont imprimés, les logiciels tracent le parcours patient bref… ces étiquettes n'ont plus que l'utilité de permettre l'appel du patient en salle d'attente et de finir dans un container en l'état sur la rue dans l'attente du ramassage des ordures. Revoir le parcours patient a permis d'économiser ce stock de papier, mais aussi les imprimantes, les contrats de maintenance liés à ces imprimantes… Bénéfices : 6 à 10 000 €/an.

Asklépian s'adapte aux secteurs d'activité et à chaque entreprise et propose un programme d'accompagnement « à la carte » en fonction des besoins spécifiques de chacun.e.

En pleine crise sanitaire, considérez-vous que les professionnels de santé sont assez préparés ?

En décembre 2020, deux médecins libéraux ont écopé d'amendes de 3 000 et 6 000 euros de la part de la 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, 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. À titre d'exemple, le 21 décembre dernier, l'hôpital d'Albertville (Savoie) a été victime d'un « rançongiciel » qui a endommagé son système d'information.

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 mise 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, Asklépian leur propose un accompagnement sur mesure pour sécuriser toutes les données et respecter le RGPD.

Quelles sont concrètement les conséquences de ces attaques ?

Il en existe plusieurs, et certaines sont fatales.

1) Tout d'abord, une sanction administrative et/ou financière pour ne pas avoir suffisamment sécurisé ses systèmes.

2) Une paralysie de ses systèmes, et donc de ses équipes, qui peut durer des mois… voire ne jamais se résoudre si les sauvegardes et restaurations n'ont pas été suffisamment anticipées.

3) Une très mauvaise image pour son entreprise, son association ou pour la collectivité qui ferait fuir sa clientèle/ses usagers.

Comment les entreprises en général – et les professionnels de santé en particulier – peuvent-ils s'assurer de la protection et de la confidentialité de leurs données ?

Je conseillerai de faire appel à des sociétés spécialisées dont les compétences sont certifiées… Des audits, des contrôles, des tests d'intrusions…

Il ne faut dormir sur ses deux oreilles… Nous vivons dans un monde où la technologie nous dépasse. Tout va très très vite… Il faut donc sans cesse se remettre en question, sans cesse adapter ses mesures techniques…

Aussi, nos organisations ne sont jamais figées… le *turn-over* implique de nouvelles méthodes, de nouvelles approches… et nous devons accompagner nos entreprises à suivre ces changements pour garder la maîtrise.

Mais je crois qu'il existe une manière de pouvoir répondre à la question rapidement. Si un de vos clients ou salariés exerce sont droit de rectification d'une donnée (son adresse suite à un déménagement, son nom suite à un mariage-divorce…).

1) Savez-vous quelles données vous pouvez modifier ?

2) Savez-vous où sont stockées ces données ?

3) Pouvez-vous toutes les rectifier ? Rapidement, dans le mois ?

4) Avez-vous une procédure pour en oublier aucune ?

5) Qui devez-vous informer ? Cette donnée qui vous a été confiée a-t-elle été envoyée à des destinataires ?

Votre capacité à répondre à ces quelques questions vous donne déjà un premier niveau de maîtrise.

Il faut rajouter les durées de conservation, les notifications d'information, les bases légales qui vous autorise à effectuer des opérations sur des données…

Quid des protections des données au niveau mondial ?

Et si la France retrouvait sa souveraineté numérique ? Les utilisateurs sont imprudents mais ils n'ont pas conscience des risques ni de la valeur de leurs données personnelles. Ce n'est qu'une photo, ce n'est que mon nom et mon prénom, ce n'est que ma date de naissance… Tous les jours, nous accompagnons des salariés qui au début de notre mission ne comprennent pas les enjeux.

Le nombre de cyberattaque ne fait que croître et personne n'est épargné.

Je vais prendre le temps de rappeler par une caricature, sans doute, qu'il y a moins de 80 ans, des individus faisaient l'objet de déportations par simple suspicion d'affiliation à une communauté religieuse. Il n'y aurait plus de doute aujourd'hui, plus de suspicion : les données de navigation Internet, par exemple, permettent de mieux connaître l'utilisateur, sur ses goûts, ses centres d'intérêt, ses réflexions…

À notre époque, notre planète connaît encore des guerres, le terrorisme... et la maîtrise des technologies de communication et d'information dans ces contextes de conflits est indispensable pour prendre un avantage sur son adversaire ; pour se protéger, pour anticiper, pour assurer sa supériorité opérationnelle. À l'ère numérique, avec la numérisation des activités et l'explosion des données disponibles, ces enjeux sécuritaires et militaires autour de la donnée sont d'une actualité préoccupante.

Il est donc indispensable que les administrations, que l'Union européenne, que l'État, que les opérateurs soient plus présents pour assurer notre protection nationale.

Depuis la récente invalidation du Privacy shield qui régissait le transfert de données personnelles en dehors de l'UE, les consciences s'éveillent sur la nécessité d'une souveraineté numérique afin de limiter/stopper cette dépendance envers les USA.

Mais nous voyons bien que la remise en cause de projets d'envergure sur fond de souveraineté numérique avec Health DATA HUB, hébergement proposé par Microsoft. La mise sous contrôle de la CNIL en l'attente d'une solution est un problème criant : en situation d'urgence et pour la réalisation d'une mission d'intérêt public : on ne peut pas faire sans les américains.

Voilà le cyber espace paradoxal dans lequel nous vivons : dans le but de servir les intérêts publics de la nation, nous devons laisser la possibilité aux services de renseignements d'un État étranger à accéder à des données stratégiques pour l'État français : les données de santé de nos citoyens dans le cas du Health Data Hub.

Enfin, quels sont vos projets à court et moyen termes ?

Je souhaite en premier lieu continuer le développement d'Asklépian pour étoffer notre offre de services et continuer d'accompagner nos clients dans tous les domaines liés à la protection des données. Renforcer nos services Organisationnel, service Juridique et service Sécurité des systèmes d'information et Cybersécurité.

J'entends également continuer notre campagne de communication pour une démarche pédagogique. En 2020, Asklépian a lancé sa nouvelle web-série qui est diffusée jusqu'en septembre 2021. En parallèle, sa veille juridique et technologique sera prochainement diffusée dans un format accessible au plus grand nombre.

Propos recueillis par Constance Périn

RGPD ; cyber ; cyberattaque ; Asklépian ; covid ; donnée ; protection ; entreprise ; santé ; CNIL

Journal Spécial des Sociétés - 8 rue Saint Augustin - 75002 Paris - Tél
01 47 03 10 10