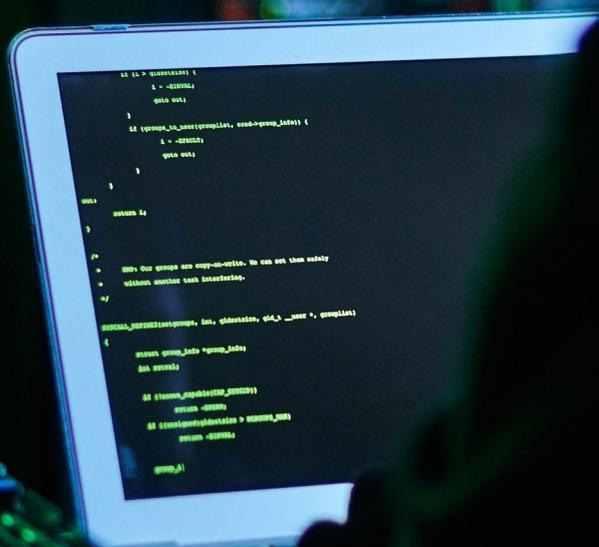


light up

#4
OCTOBRE
2022

L'ACTUALITÉ DE LA TRANSFORMATION
ET DE L'INNOVATION ASSURANCE



**INSURANCE
& FINANCIAL
SERVICES**
BY HARDIS GROUP

sommaire



INTERVIEW

Un assureur face aux enjeux climatiques

ANTOINE POINCARE
DIRECTEUR AXA CLIMATE SCHOOL

3



INTERVIEW

La cyber Assurance gagne en maturité

DIEGO SAINZ
RÉFÉRENT TECHNIQUE CYBER CHEZ VERSPIEREN

6



INTERVIEW

Flex

Les services à portée de clic

ROSA NAIT SAADA
DIRECTRICE DE FLEX

9



INTERVIEW

Zenioo

Courtier ou insurtech?

EMMANUEL LEGRAS CEO DE ZENIOO
HERVÉ LARCHER CTO DE ZENIOO

13



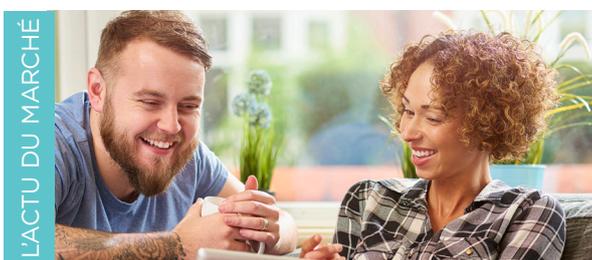
DOSSIER

DORA

la future réglementation de la sécurité numérique obligatoire des « entités financières »

LAURENT CHAILLOU
CONSULTANT SENIOR ASSURANCE HARDIS GROUP

16



L'ACTU DU MARCHÉ

L'actu du marché

PAR NOS ÉQUIPES

22

Un assureur face aux enjeux climatiques

ANTOINE POINCARE DIRECTEUR AXA CLIMATE SCHOOL



Après vos études à HEC, vos premières expériences ont lieu dans l'audiovisuel auprès d'Emmanuel CHAIN puis dans la formation des entreprises sur le thème de la transformation digitale. Vous rejoignez ensuite AXA Climate afin de créer et développer une nouvelle offre visant à former les entreprises aux enjeux de la transition climatique.

Pouvez-vous nous présenter AXA Climate School et son positionnement dans la stratégie globale d'AXA Climate ?

La Climate School est une Business Unit lancée en avril 2021 au sein d'AXA Climate. Nous proposons à nos clients des parcours de formation en marque blanche visant à leur permettre d'appréhender et anticiper les bouleversements que leurs métiers connaîtront du fait de la transition climatique. Notre positionnement est celui d'un contenu très qualitatif, sur le fond et sur la forme, tout en proposant des tarifs très compétitifs. À la différence des supports habituels de type e-learning, l'ADN de nos formations repose sur un Story Telling fort et un contenu validé par des journalistes et scientifiques. AXA Climate est une filiale du groupe AXA qui propose des produits et des services qui ont tous leur existence propre et dont le point commun est la transition climatique. Il ne s'agit pas de vente additionnelle qui viendrait enrichir la valeur perçue d'un contrat d'assurance. Nos quatre grands métiers sont :

- **L'Assurance Climatique** (que l'on opère via des produits d'assurance paramétrique)
- **Le Conseil en Adaptation** qui permet aux clients d'identifier les zones géographiques où leurs opérations sont exposées aux changements climatiques et d'être aidés pour s'adapter à ces risques
- **L'investissement dans l'agriculture régénérative**
- **La formation** (avec ce premier produit : la Climate School)

Quelles sont les spécificités de votre offre de formation ?

Après la transformation digitale, la transition durable est un nouveau choc majeur face auquel les grandes entreprises présentent des défis de compréhension et d'appréhension globale. Leur besoin est donc un moyen de se mettre en ordre de marche avec une solution qui présente les avantages d'être facilement accessible et extrapolable à l'ensemble des collaborateurs d'un groupe qui, la plupart du temps, sont implantés aux quatre coins de la planète. Schématiquement les entreprises avaient le choix entre des interventions « prise de conscience » pour Comex d'un côté, et le déploiement d'ateliers de



sensibilisation « présentiels » de leurs équipes sur le réchauffement climatique de l'autre. Nous voulons proposer en complément une troisième voie avec des contenus vidéos asynchrones pour passer à l'échelle. Comme ces types de formations et d'offres n'avaient pas l'air d'exister sur le marché, nous avons décidé de la créer nous-même. S'agissant d'un produit avec une existence propre et en marque blanche, l'objectif n'est pas de faire baisser le niveau de risque ou la sinistralité bien que cela contribue à long terme au grand dessein. La transition durable est une transformation fondamentalement scientifique qui nécessite de multiplier les interactions avec les scientifiques pour comprendre les limites planétaires et se demander si son entreprise est compatible avec ces limites et sinon réinventer son modèle. Notre formation apporte des réponses à trois niveaux :

- **Le niveau « Planète »** pour comprendre ce qui se passe à l'échelle du climat, de la biodiversité et des ressources naturelles.
- **Le niveau « Entreprise »** avec la traduction de la partie précédente au monde de l'entreprise : Bilan Carbone, les Scopes 1, 2 et 3, l'Analyse du cycle de vie ou l'économie circulaire par exemple
- **Le niveau « métier »**, « Comment la transition durable va avoir un impact sur mon métier et le transformer » à travers des cours spécifiques par métier (IT, Marketing, juridique etc) qui visent à faire comprendre la façon dont chaque métier va se transformer et comment initier les premiers pas de l'adaptation

Nous investissons majoritairement dans la production des contenus. Depuis 10 ans la

“

La transition durable est une transformation fondamentalement scientifique.

formation en ligne a plutôt vu un investissement sur les technologies et un désinvestissement sur les contenus, nous sommes donc à l'inverse de cette tendance car nous sommes convaincus que pour créer de l'engagement la clé reste le contenu qui se doit d'être très beau et bien raconté. Pour satisfaire à cet objectif, chacun de nos cours fait l'objet d'un double regard, celui d'un ingénieur pédagogique puis d'un journaliste, sans oublier au préalable une plume de fond sur la transition environnementale, plutôt scientifique ou métier. Nous avons fabriqué un produit principalement à destination des grandes groupes internationaux et cela impose quelques points de passage. Tout d'abord, toutes nos vidéos sont aujourd'hui tournées en Français, en Anglais et en Allemand avec la participation de journalistes et présentateurs qui ont une aura forte. Ensuite l'expérience pour nos clients doit être simple et sans couture : nos cours viennent s'insérer dans leurs plateformes de formation. Pour résumer, ce que l'on essaye c'est d'être utile, qualitatif et simple. Un dernier exemple sur le « simple » : nous sommes flexibles sur la manière dont nous délivrons nos cours avec une offre assez granulaire qui s'articule autour d'un catalogue d'environ deux cents mini capsules vidéo dans lequel le client vient piocher pour composer ses modules de formations.



Quel est le profil type des entreprises qui font appel à vos services ?

Plutôt des grands groupes du secteur privé environ une cinquantaine à ce jour, bientôt soixante, dont une trentaine qui opèrent en France. Nous sommes présents dans six pays : Angleterre, Allemagne, Inde, France, États-Unis et Pays-Bas. Ces clients ne sont pas nécessairement couverts par AXA. Il est important de préciser qu'au stade de la régulation, il n'existe aujourd'hui aucune obligation pour les entreprises de former leurs employés à la transition durable. Il s'agit donc avant tout d'une question de personne et c'est clairement la tendance que nous observons avec l'arrivée de Responsables RSE qui sont clairement engagés et sensibles à ce type de projet. Ensuite, il y a évidemment des secteurs qui sont plus exposés que d'autres comme la Finance et l'Assurance ou le Bâtiment. Mais à différents niveaux tous les secteurs sont concernés.



Comment va évoluer AXA Climate School dans les prochaines années ?

Au-delà de l'offre actuelle, nous travaillons sur de nouveaux produits autour de l'upskilling. Par exemple quelles nouvelles compétences doivent acquérir des acheteurs pour devenir des acheteurs verts. Les modalités seront différentes avec du synchrone et des rencontres avec les utilisateurs. Nous avons une volonté forte de créer une logique de communauté Alumni autour de cette communauté de métiers. Ces modalités sont plus longues que le « pur online » mais permettent de transformer les compétences plus profondément.

Observez-vous une hausse de la demande suite aux nombreuses catastrophes naturelles observées ces derniers mois à l'échelle planétaire que sont les incendies, la sécheresse et les inondations ?

Nous sommes sur une vitesse de croissance déjà très rapide avec un chiffre d'affaires d'environ un million d'euros qui va être multiplié quasiment par quatre. Le niveau de conscience du côté des responsables RSE est déjà élevé. Ce qui peut être anticipé est une augmentation du suivi des formations par les utilisateurs finaux, les collaborateurs des entreprises qui vont s'intéresser au sujet.

Compte tenu de votre engagement pour la cause climatique, comment vous positionnez vous par rapport au reliquat de climat-scepticisme qui reste malgré tout présent ?

Notre objectif est d'accélérer la bascule dans les entreprises car aujourd'hui il est dangereux de ne pas prendre le virage. Il est largement relaté dans la littérature sur le Change Management, qu'il est important de travailler en priorité sur les gens qui ont déjà envie de passer à l'action et qui peuvent « transmettre » la dynamique à leurs collègues. Cette stratégie a in fine pour conséquence de faire bouger la pyramide alors qu'il serait contre-productif de tenter de faire bouger tout le monde en même temps, les plus sceptiques compris. Le gros du travail, qui est le mien, consiste donc à faire l'interprète entre des vérités scientifiques et les raconter de la manière la plus pertinente et compréhensible possible. ■

La cyber Assurance

gagne en maturité

DIEGO SAINZ RÉFÉRENT TECHNIQUE CYBER CHEZ VERSPIEREN

Pouvez-vous nous présenter votre fonction chez Verspieren ?

Je suis le référent technique cyber du groupe Verspieren et le support technique de nos chargés de comptes et de clientèle sur les placements et les renouvellements d'assurances cyber et sur toutes les problématiques techniques que nous pourrions avoir, que ce soit avec l'un de nos partenaires assureurs ou avec l'un de nos clients. Je fais également du conseil en prévention cyber pour nos clients. A la base, je suis ingénieur en cybersécurité, j'ai une solide expérience en souscription cyber et avant de rejoindre le monde de l'assurance, j'ai eu une expérience de conseil en cybersécurité.

Que propose Verspieren comme solutions de cyber assurance ?

Verspieren a un véritable rôle d'accompagnement à 360 degrés sur le risque particulier cyber. Nous proposons des polices de cyber assurance pour des clients allant de la petite TPE jusqu'à des grands groupes du CAC 40. Ces polices d'assurance sont fournies par des assureurs positionnés sur le marché de l'assurance cyber avec lesquels nous avons des relations privilégiées. Notre connaissance du marché de l'assurance nous permet de proposer à chaque client la solution la plus adaptée à son contexte et de lui proposer plusieurs options. Par exemple, pour les plus petites entreprises, nous proposons des solutions de souscription facilitée pour obtenir des conditions d'assurance cyber compétitives adaptées à leur budget. Nous déterminons les meilleures conditions d'assurance pour nos clients en fonction de leurs risques et nous les aidons à remplir les exigences des assureurs (qui se durcissent ces dernières années) pour préparer les renouvellements de leurs polices.

Verspieren ne se contente pas de proposer des polices d'assurances mais assure aussi un véritable rôle de conseil et de prévention.

Verspieren ne se contente pas de proposer des polices d'assurance mais assure aussi un véritable rôle de conseil et de prévention et propose une assistance en cas de sinistre.

Nous accompagnons nos clients via des services de prévention et de gestion des risques cyber grâce à des solutions en interne ou via des partenaires qui sont experts



QUELQUES CHIFFRES



1 ENTREPRISE SUR 2
en France ciblée par un
ransomware en 2021*



**+200% DES VICTIMES
D'ATTAQUES PAR
RANSOMWARE**
entre juillet et novembre
2021 dans le monde*



**2.5 MILLIARDS €
DE PERTES CUMULÉES**
pour les entreprises
françaises victimes en 2021*



**2.82% DU CHIFFRE
D'AFFAIRES DE
L'ENTREPRISE VICTIME**
c'est le montant moyen
de la rançon fixée par les
cybercriminels. Il faut noter
que ce montant est compris
entre 0.7% (très grandes
entreprises) et 5% (TPE/
PME) du CA de la victime.**

*Source ANOZR WAY

** Source Checkpoint

dans leurs domaines. Par exemple, en partenariat avec Holiseum, nous proposons une solution "Tir à blanc de Ransomware". Il s'agit d'une simulation qui permet à nos clients de se mettre dans les conditions réelles d'une attaque par ransomware et d'en voir tous les impacts. Cela permet de mesurer le niveau d'exposition de leur Système d'Information et sa résilience face au risque précis du ransomware, afin de cibler les actions de sécurisation de manière optimale, sans attendre de subir une véritable attaque.

Nous proposons également une assistance en cas de sinistre afin de mettre en place des mesures pour circonscrire l'incident et accompagner sur la stratégie de remédiation.

Le rôle du courtier est d'autant plus important aujourd'hui que le marché de l'assurance cyber s'est durci et qu'il est compliqué pour certaines entreprises d'obtenir une assurance cyber. Il est donc important d'avoir un partenaire qui connaît bien les cyber assureurs et qui puisse trouver la meilleure solution pour chaque client.

Constatez-vous une augmentation des demandes en cyber assurance ?

Oui, nous constatons une augmentation des demandes. Par le passé les entreprises n'étaient pas convaincues de la nécessité de s'assurer en cyber et du fait que les assureurs tiendraient leurs promesses en cas de sinistre. La tendance s'est complètement inversée, notamment ces deux dernières années du fait de l'augmentation du nombre et de l'intensité des sinistres. Les entreprises ont compris l'importance d'augmenter leur niveau de prévention et de s'assurer face aux risques cyber.

Cependant, l'offre a elle diminué. Certains assureurs ont ralenti les souscriptions et sont beaucoup plus sélectifs quant au niveau de maturité cyber des clients. Plusieurs rapports

d'organismes sur les risques des entreprises classent le risque cyber en numéro 1 ou 2 et soulignent l'importance de l'adresser car il peut avoir des conséquences financières catastrophiques.

Certains assureurs ont ralenti les souscriptions et sont beaucoup plus sélectifs quant au niveau de maturité cyber des clients.

Que pensez-vous du projet de loi de conditionner le remboursement des assurances par le dépôt d'une plainte dans un délai de quarante-huit heures ?

Il y a toujours eu un débat sur l'assurabilité des rançons. Selon certains organismes publics, les rançons pourraient financer le terrorisme et le fait de payer donnerait aux cybercriminels des motifs pour toujours demander plus et multiplier les attaques. Il y a quelques temps, le gouvernement était plutôt en défaveur de l'assurabilité du paiement des rançons.

De mon point de vue, ce récent projet de loi en faveur de l'assurabilité de l'indemnisation des rançons sous condition d'un dépôt d'une plainte dans un délai de quarante-huit heures est une bonne chose. C'est une garantie qui est proposée par la plupart des assureurs et il faut la maintenir pour bien assurer les clients, notamment avec l'explosion des ransomwares. Le fait de conditionner le remboursement des assurances par le dépôt d'une plainte permettrait à l'État de mieux identifier les attaques et d'avoir des indicateurs pour mieux lutter et mettre en place des moyens face à ces attaques.

Quand l'entreprise paie, ce n'est pas par malhonnêteté, c'est que toutes les mesures de sécurité mises en place n'ont pas fonctionné et que la situation est catastrophique.

Pouvez-vous nous expliquer les processus et mécanismes de tarification des assurances cyber ? Sur quels critères se basent-elles ?

Pour établir les tarifications, les assureurs s'intéressent à plusieurs facteurs. Il y a d'abord le facteur de dimensionnement de l'entreprise ou de l'organisme : le chiffre d'affaires, le nombre de filiales, la présence ou non de filiales à l'étranger... Le deuxième facteur est le niveau de maturité du client en matière de protection cyber. L'assureur détermine le risque du client : probabilité qu'une attaque puisse survenir et l'impact qu'elle pourrait avoir sur l'entreprise et son activité. Enfin, il y a évidemment les conditions des assurances (limite, franchise...) qui vont moduler la tarification.





Constatez-vous une augmentation des déclarations d'attaques cyber ? Si oui, quels sont les types les plus fréquents ?

Les premières années de l'assurance cyber en France, il y avait peu de sinistres en nombre et en termes de montants indemnisés. Mais ces dernières années, nous constatons effectivement une augmentation très significative des déclarations de sinistres, surtout de ransomwares, aussi bien en nombre qu'en intensité. Par le passé, l'impact financier moyen pour une TPE / PME était de l'ordre de quelques dizaines de milliers d'euros contre des centaines de milliers d'euros aujourd'hui. Pour un grand compte cela peut atteindre de manière assez systématique plusieurs millions d'euros contre quelques centaines de milliers d'euros auparavant.

Ces deux dernières années, il y a eu un fort durcissement du marché. Les assureurs augmentent les primes et les franchises afin de pérenniser la branche cyber et d'avoir des meilleurs résultats techniques.

Les attaques les plus fréquentes sont celles de type ransomware, c'est la majorité des sinistres indemnisés. Viennent ensuite les fuites et divulgations de données, puis le phishing et la compromission des messageries d'entreprises, puis les attaques en déni de service et enfin les défauts de conformité RGPD. Il faut aussi noter les accidents ou erreurs humaines.

L'explosion de la sinistralité des ETI risque-t-elle d'impacter fortement le marché de la cyber assurance ?

Elle a déjà impacté le marché de l'assurance. Les assureurs sont beaucoup plus sélectifs et de plus en plus d'entreprises ne se voient pas proposer de solutions d'assurance cyber. Les conditions ne sont plus les mêmes qu'auparavant. Mais on se dirige vers une stabilisation plus pérenne du marché.

Pensez-vous que la France a la capacité de se défendre par rapport à d'autres pays beaucoup plus avancés et équipés sur ce sujet ?

La France est dans le top 3 des pays les plus attaqués d'Europe. Elle est relativement en retard par rapport à d'autres pays quant à ses capacités à se défendre contre les cyber attaques. Par exemple, l'Australie dispose d'un ministère dédié à la cyber sécurité, les USA ont beaucoup plus de moyens pour lutter, des pays comme la Russie ou la Chine ont des capacités très importantes aussi bien défensivement qu'offensivement...

Dernièrement la France a subi de nombreuses attaques qui ont ciblé les entités publiques, les collectivités, les hôpitaux... Ces attaques ont été très impactantes.

Cependant l'Etat réagit face à ces attaques en mettant en place des plans de cyberdéfense. On peut par exemple citer le plan à 1 milliard présenté en 2021 par Emmanuel Macron pour renforcer la sécurité des entreprises, des hôpitaux et des administrations. Il existe aussi des départements spécifiques dans la gendarmerie et la police qui s'étoffent ainsi que l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) pour accompagner les entreprises et les entités publiques. ■

Flex

Les services à portée de clic

ROSA NAIT SAADA DIRECTRICE DE FLEX



Pouvez-vous nous présenter Flex et nous dire à qui cela s'adresse ?

Flex, c'est une plateforme digitale de services qui va s'adresser à toute cible :

- **BtoBtoE** : des offres souscrites par l'entreprise (RH, facility manager, CSE...) pour les salariés afin de faciliter leur équilibre de vie ;
- **BtoB** : des services à destination du dirigeant pour l'aider à prendre soin de sa santé, tels que des bilans de santé, de l'écoute psychologique, un second avis médical... car le dirigeant c'est l'homme clé, il porte son entreprise. Mais aussi des services pour prendre soin de la santé de son entreprise, par exemple des services sur la bonne gestion de la trésorerie, sur le document unique - qui est une obligation réglementaire - ou sur la gestion de l'absentéisme parce qu'on sait que ce sont des problématiques pour de nombreuses entreprises et qu'elles sont souvent démunies. Ça les aide à gagner du temps et ça permet au dirigeant de se concentrer sur son cœur de métier, à savoir développer son activité.
- **BtoC** : nous avons lancé en début d'année un pack de services pour les seniors à partir de 65 ans autour du bien-vieillir.

Notre rôle est à la fois de proposer des services, mais aussi du conseil. Pour les entreprises nous commençons toujours par un diagnostic de leurs besoins pour comprendre quelles sont leurs difficultés, leurs priorités, le profil de leurs salariés, les services déjà mis en place, etc. A partir de là, nous allons proposer la meilleure solution.

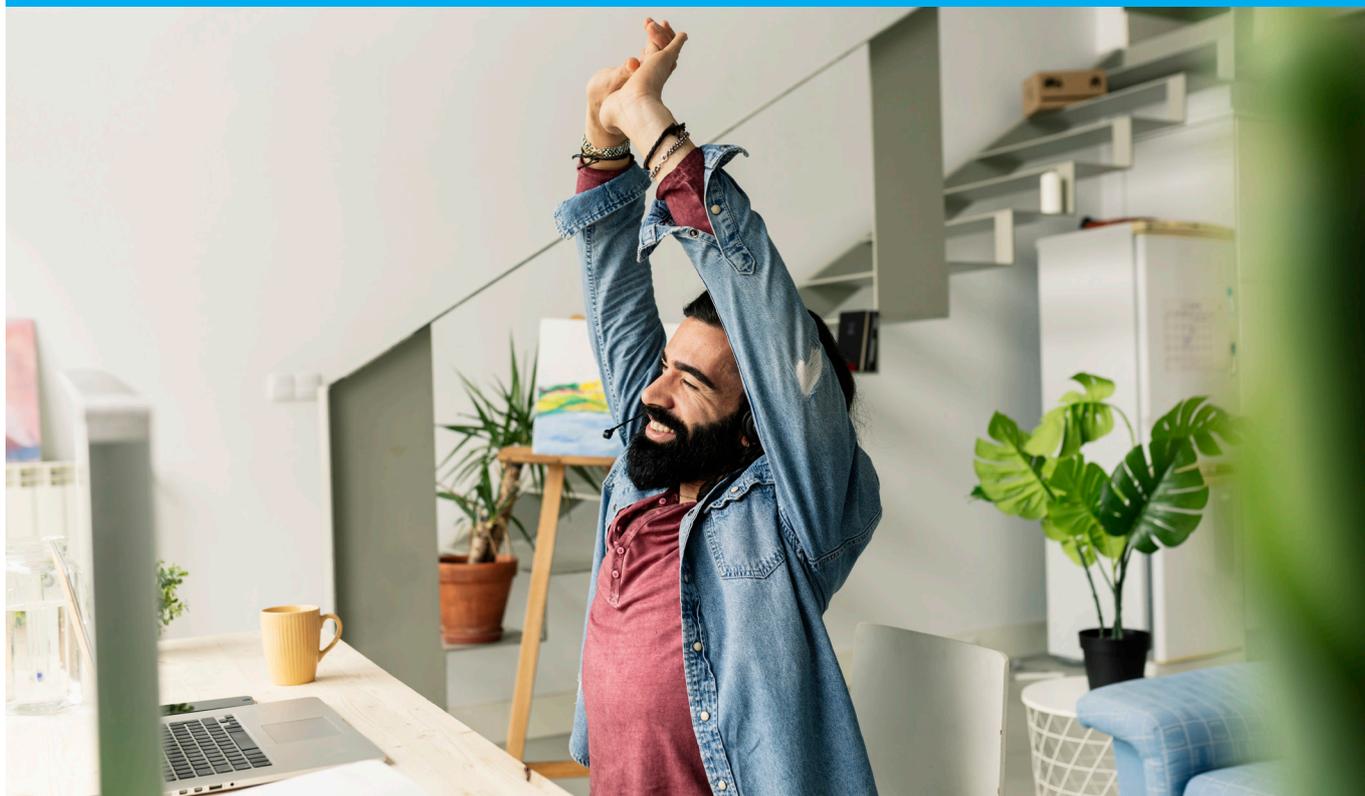
Cela peut être un pack qui va intégrer différents services ou alors des services à la carte qui vont répondre à un besoin bien spécifique, tel que les TMS (Troubles Musculo-Squelettiques) par exemple.

Nous nous occupons également de toute la mise en place, nous fournissons des indicateurs à l'entreprise pour lui dire combien de personnes ont utilisé le service et nous mettons en place un questionnaire de satisfaction pour voir quel est le ressenti, cette fois qualitatif, des collaborateurs.

Nous sommes vraiment sur toute la chaîne de valeur, du sourcing des meilleures solutions jusqu'à la mesure de la satisfaction utilisateur, en passant par le développement de l'usage des services - qui est un enjeu clé.

Les services QVCT (Qualité de Vie et des Conditions de Travail) existaient bien avant Flex, mais chaque acteur proposait une solution spécifique et c'était compliqué à mettre en place pour un DRH ou un dirigeant : trouver les

“
Nous sommes vraiment sur toute la chaîne de valeur, du sourcing des meilleures solutions jusqu'à la mesure de la satisfaction utilisateur, en passant par le développement de l'usage des services - qui est un enjeu clé.



bons prestataires, négocier les tarifs, regarder le volet RGPD, favoriser l'utilisation, s'assurer que les salariés soient satisfaits... Avec Flex, le DRH a un point d'entrée unique, c'est un gain de temps.

Quelles ont été les motivations du groupe La Mutuelle Générale pour se lancer dans cette nouvelle activité ?

Ce sont vraiment les retours clients et prospects. Nous avons parlé des services que nous proposons en inclusion lors d'un événement auprès d'une soixantaine de dirigeants et pratiquement 80% d'entre eux étaient intéressés par ces services mais ne souhaitaient pas changer de complémentaire santé tout de suite. C'était problématique puisqu'on ne pouvait pas les vendre seuls. En étudiant un peu le marché, nous nous sommes rendu compte qu'il existait des services, mais dispersés chez différents prestataires, avec des tarifs en fonction de la taille de l'entreprise, des qualités de service pas assez encadrées, etc. Nous nous sommes dit qu'il y avait quelque chose à faire pour pouvoir aider les entreprises avec une offre structurée, qui réponde vraiment à leurs besoins, et qui soit éprouvée. La Mutuelle Générale nous sert de Lab pour tester les différents services avant de les lancer, ce qui nous permet d'avoir une offre vraiment fiable et de qualité !

Le fait que La Mutuelle Générale, une mutuelle, puisse proposer tous ces services, avec une filiale start-up, en usage illimité et avec un tarif de centrale d'achat, ils trouvent ça génial, ça leur facilite la vie.

En étant une filiale, nous pouvons aller plus loin que les services en inclusion qui sont très limités

par la loi puisqu'ils doivent absolument être en lien avec le contrat santé ou prévoyance et ce n'est pas suffisant. Ça nous apporte également de la souplesse puisque nous pouvons mettre en place des services en cours d'année pour répondre à un besoin immédiat, sans avoir à attendre le renouvellement. Ces services peuvent également être portés par un budget RH ou formation, certains sont finançables par le CSE, ça laisse différentes possibilités de financement pour l'entreprise.

Concrètement, comment cela fonctionne ?

Nous avons mis en place une plateforme digitalisée et responsive pour faciliter l'accès à ces services en 2 clics.

Pour l'entreprise, nous avons créé Flex entreprise. Elle peut y charger son fichier de salariés, ajouter ou supprimer de nouveaux collaborateurs, mais aussi y retrouver tous les kits de communication qui vont lui permettre de faire connaître les services auprès de ses employés.

Pour les salariés, ils retrouvent l'ensemble de leurs services sur Flex abonnés et peuvent les utiliser en toute autonomie et autant de fois qu'ils le souhaitent. Nous voulons faire en sorte que le service soit utilisé au maximum.

Il nous est également arrivé de faire un « Flex by... le nom de l'entreprise » pour personnaliser l'expérience utilisateur en intégrant le nom et le logo de l'entreprise.

Et pour les entreprises qui ont déjà une plateforme de services, par exemple leur espace RH, nous sommes en train de développer des API pour exposer nos services directement sur leur site.

Comment cela aide les entreprises à progresser sur le sujet de la QVCT ?

Déjà en leur faisant prendre conscience des problématiques qui existent dans l'entreprise grâce au diagnostic. Et ensuite en leur proposant les bonnes solutions.

Nous rendons les services accessibles à toutes tailles d'entreprises. Parce qu'aujourd'hui il y a beaucoup de grandes entreprises qui proposent déjà des choses, nous réalisons un audit gratuit de tous les services qu'elles ont, combien elles paient, etc. Et grâce à Flex nous leur permettons de faire des économies avec des tarifs qui vont être mieux négociés, ou des services qui vont être plus étoffés ou encore de meilleure qualité, tout en facilitant leur accès à ces services avec nos plateformes.

Les plus petites entreprises n'ont souvent même pas conscience qu'elles peuvent mettre en place ces services ou elles pensent ne pas avoir les moyens. Avec Flex elles trouvent une réponse à leur besoin.

Ce qui leur plaît chez Flex, c'est qu'une fois qu'elles ont choisi la solution, elles n'ont pratiquement plus rien à faire. On ne leur rajoute pas un problème, on leur apporte la solution.

Est-ce qu'il y a des types de services qui attirent davantage aujourd'hui ou qui sont plus utilisés que d'autres ?

Cela dépend vraiment de l'entreprise et du profil de ses collaborateurs. Aujourd'hui, on voit que tout ce qui est autour de la parentalité séduit énormément parce que c'est un vrai sujet et que ça prend du temps même sur sa vie professionnelle. Prendre soin de la santé des collaborateurs, c'est également de plus en plus une demande des entreprises. Elles nous demandent des actions autour des addictions, du sommeil, de l'alimentation, de l'ergonomie du poste de travail sur site ou en télétravail, de l'écoute psychologique... Ces sujets-là ont pris de l'ampleur avec la crise sanitaire.

Nous constatons également un besoin fort autour du recrutement, les entreprises ont besoin de développer leur marque employeur pour attirer et fidéliser les talents. La mise en place de services utiles et qui aident leurs salariés est un véritable outil différenciant.

Quels sont les prochains services qui vont être mis en place par Flex ?

Nous travaillons sur des formations ludiques afin d'apprendre tout en pratiquant, avec notamment un Escape Game autour des TMS ainsi qu'un module en réalité virtuelle sur l'utilisation des extincteurs, car peu de personnes savent les utiliser alors que c'est indispensable

et ça risque même de devenir obligatoire au domicile, avec le télétravail.

Nous allons aussi proposer de la sensibilisation au phishing afin de faire en sorte que tous les collaborateurs soient formés pour éviter de mettre en risque toute l'entreprise.

Enfin, nous allons également développer encore plus les formations puisque nous sommes désormais certifiés Qualiopi. Nous travaillons notamment sur une formation des CSE pour compléter notre pack « Avantages CSE » qui contient des services éligibles aux œuvres sociales et culturelles.

Mais même si nous avons une roadmap, elle évolue en fonction des besoins des clients. Nous sommes vraiment en mode startup, donc nous pouvons arrêter un service, en débiter un autre et c'est ce qui fait aussi le plus de Flex, nous ne sommes jamais fermés à proposer un nouveau service à partir du moment où il répond à un besoin. Nous sommes Flex !



D'un point de vue technique, comment cela fonctionne ?

Nous avons fait le choix de ne pas partir sur une marketplace qui existe car il y a beaucoup de limitations et nous ne voulions pas être dépendant d'un tiers qui pourrait être un frein dans notre logique de start-up et de test and learn. Nous avons plutôt choisi les briques qui nous semblent être les meilleures sur le marché pour pouvoir proposer la meilleure expérience client, en restant maître de ce que nous faisons.

Nous proposons un parcours sans couture pour l'utilisateur, sans besoin de recréer un compte ou de se reconnecter sur différentes interfaces.

Et quel est le modèle économique ?

Nous avons 2 types de modèles économiques. On peut s'abonner à des services ou pack de services avec un abonnement d'un an, ou on peut prendre un service à l'acte et on ne paie que ce qu'on a choisi. Ça apporte de la souplesse. Certaines entreprises n'ont pas beaucoup de budget ou n'ont pas la maturité suffisante sur les services QVCT, elles vont alors commencer par un service à la carte, voir si ça répond au besoin et si ça leur plaît. Ensuite, quand elles sont convaincues, généralement elles passent sur un pack. D'autres vont tout de suite souscrire à un pack parce que ça correspond exactement à leur besoin et qu'elles y voient une source d'économie.

Est-ce que vous envisagez de travailler avec d'autres acteurs de la protection sociale, que ce soit pour des services en inclusion ou pour apporter une réponse complète à un client ?

On ne se ferme à rien, si un cas se présentait, on pourrait l'étudier et le mettre en place.

Aujourd'hui, nous travaillons avec beaucoup de courtiers qui proposent nos services avec un contrat d'assurance qui n'est pas celui de La Mutuelle Générale. Nous avons également été approchés par des bancassureurs.



Quel est le délai de mise en place une fois qu'une entreprise ou un particulier a choisi Flex ?

C'est très rapide, ça peut être mis en place en moins d'un mois. Tout est automatisé.

Et pour des services à l'acte ça peut être très rapide aussi. Nous avons eu le cas d'une entreprise où un collaborateur a été agressé par un client dans une agence, en 2 jours nous avons monté une cellule de psychologues pour pouvoir intervenir sur site.

Notre objectif est d'être présent pour pouvoir répondre à la demande immédiate et solutionner le problème, pour décharger à la fois le salarié, mais aussi l'entreprise.

Est-ce que vous constatez un accroissement de la demande au niveau des entreprises ?

Cela s'est vraiment accéléré en terme de demandes, d'écoutes et d'opportunités. Nous voyons qu'il y a vraiment un avant et un après crise sanitaire.

Et nous voyons également apparaître des concurrents et nous en sommes très contents parce que plus il va y en avoir, plus les entreprises vont être sensibilisées et plus les services entreront dans les mœurs des entreprises.

Quelle est la force de Flex par rapport à ces concurrents qui arrivent sur le marché ?

Aujourd'hui nos concurrents sont encore très orientés cœur de métier santé/prévoyance ou alors avec une approche pilote auprès des clients pour tester des services. Nous, nous ne demandons pas à nos clients de tester les services, nous les avons déjà testés et éprouvés pour eux, c'est un gage de qualité !

Notre force est également notre plateforme digitale, qui n'existe pas ailleurs, ainsi que cette agilité dans notre socle technologique qui nous permet de lancer un service rapidement et de le retirer s'il ne fonctionne pas.

Tout passe par Flex, nous avons également notre service relation client qui gère le SAV, nous sommes le point d'entrée unique et ça leur facilite la vie. ■

En clair, nous sommes un « Amazon » des services !

Zenioo

Courtier ou insurtech?

EMMANUEL LEGRAS CEO DE ZENIOO
HERVÉ LARCHER CTO DE ZENIOO

D'où vous est venue l'idée de Zenioo ?

Emmanuel Legras - Fin 2019, nous sommes 3 anciens dirigeants d'APRIL qui décidons de nous lancer dans une nouvelle aventure. Nous partageons le constat que le marché du courtage est innovant et dynamique mais que la transformation d'une idée en un produit ou service concret est souvent fortement pénalisée par le poids de l'histoire et les systèmes monolithiques et souvent verticaux. La nécessité d'accroître la digitalisation des outils et des relations est renforcée par la pandémie et conforte notre modèle.

Comment se traduit votre projet vis-à-vis de ce constat ?

Emmanuel Legras - De ce constat nous dégagons 3 principes :

- Apporter une **solution différente et innovante dédiée au monde du courtage**,
- Proposer des **services et produits avec un maximum d'agilité**,
- Profiter de la page blanche qu'est le SI pour proposer une **solution modulaire** qui n'est plus contrainte par un lourd héritage système.

Sur cette base, nous créons ZENIOO en juillet 2020. Deux ans après, la société compte 22 collaborateurs dont 10 commerciaux.

Notre volonté est de devenir un fournisseur de produits et services dédiés à l'assistance à la vente pour les courtiers. Notre place de marché doit :

- Présenter, exposer, expliquer et comparer les produits,
- Ne pas répliquer les systèmes de tarification mais utiliser ceux existants de nos partenaires métiers ou technologiques, pour éviter les risques d'erreurs,
- S'appuyer sur les services et processus de gestion de nos partenaires de gestion

Quelle est votre solution pour proposer ces services en évitant les inconvénients d'un SI historique ?

Emmanuel Legras - Hervé Larcher nous a proposé de bâtir la conception du SI ZENIO en embarquant la technologie low code. Le concept existe depuis une quarantaine d'années mais ce n'est que depuis très récemment que des solutions concrètes sont disponibles dont les leaders sont : OutSystems, Microsoft, Mendix, Salesforce, ServiceNow. Gartner estime pour 2024 que 65% des

zenioo



Emmanuel Legras

“ La transformation d'une idée en un produit ou service concret est souvent fortement pénalisée par le poids de l'histoire et les systèmes monolithiques. ”

applications seront développées avec des solutions low code.

Hervé Larcher - Nous avons fait le choix de travailler avec Outsystems avec la volonté de passer de la théorie à la pratique en construisant notre SI en low code.

Si de nombreux développements concrets et opérationnels sont réalisés dans le monde, en France, ces solutions sont majoritairement vues comme un outil facilitateur pour créer des POC (Proof of Concept).

Nous sommes devenus un partenaire privilégié d'OutSystems France et notre solution a été primée « Prix du public » au forum MIA dédié au no-code / low-code de mai 2022.

Quels sont les points positifs que vous avez relevés avec cette solution ?

Hervé Larcher - Cette solution permet de nous libérer de contraintes habituelles dans les projets de développement comme maîtriser la scalabilité, la sécurité, l'opérabilité, la robustesse, la dette technique. Cela reste toujours un sujet évidemment mais nous n'avons pas besoin d'une ou plusieurs équipes dédiées pour le gérer.

Par exemple, s'assurer que notre solution sera bien opérationnelle sur le nouvel iPhone n'est plus un sujet, il nous reste à nous concentrer sur la solution et la réponse aux besoins de nos clients courtiers.

Hors ces facilités techniques ?

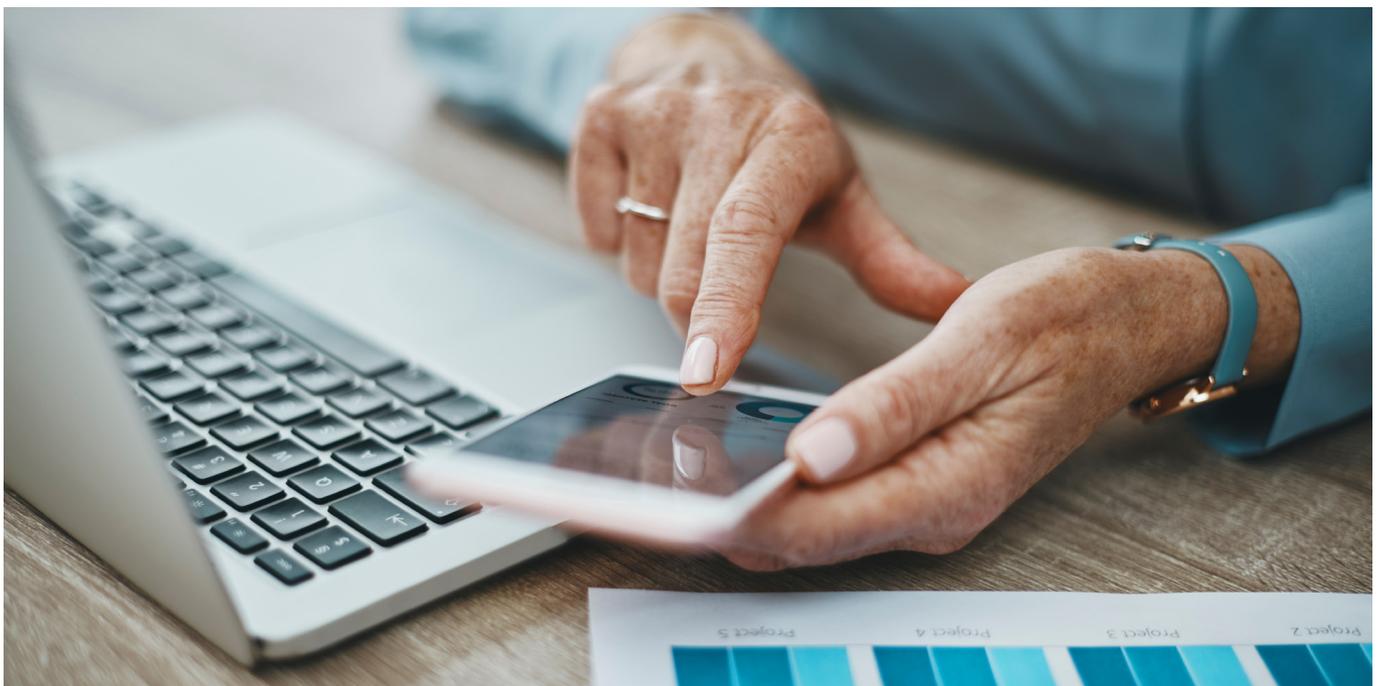
Hervé Larcher - Nous pouvons nous concentrer sur la réponse aux besoins et cela permet de raccourcir considérablement le « Time to Delivery ».

Par exemple, fin octobre 2020, nous avons lancé nos premiers développements. En avril 2021 nous étions en phase de test de commercialisation, avec trois offres sur deux marchés et deux gestionnaires.



Hervé Larcher

Nous avons fait le choix de travailler avec Outsystems avec la volonté de passer de la théorie à la pratique en construisant notre SI en low code.



En six mois, nous avons mis en place :

- **Un outil de gestion de l'onboarding des courtiers digitalisés** – des interconnexions avec des services complémentaires type ORIAS,
- **Une solution de lecture de certains documents, signature en ligne, une solution éditique,**
- **Une solution de gestion des projets ventes** avec un parcours de souscription, un comparateur, la connexion à un tarificateur et un système de gestion.

Sur cette période, nous avons intégré plus de 80 services de 14 entités différentes avec la philosophie d'avoir un système multi-back, multi-branches, multi produits, multi partenaires.

De fin juin 2021 à septembre 2021, nous avons réussi à réaliser et proposer à nos courtiers un parcours Emprunteur complet.

En octobre 2021, en association avec certains de nos courtiers, nous décidons de porter nos applicatifs de signature sur mobile et le déploiement sera effectué en production en décembre 2021 pour les contrats santé.

De novembre 2021 à mi-février 2022 nous avons, non seulement proposé un nouveau parcours sur deux produits santé (une offre senior et sa jumelle pour les familles), mais aussi intégré un nouveau partenaire de gestion.

Nous avons intégré plus de 80 services de 14 entités différentes avec la philosophie d'avoir un système multi-back, multi-branches, multi produits, multi partenaires.

Ces exemples démontrent l'agilité de notre solution et sa capacité à s'intégrer avec d'autres systèmes.

Nos résultats nous confortent dans nos choix car nous arrivons à produire des parcours en un temps plus court ou à minima aussi important que les solutions fondées sur des systèmes Legacy plus verticaux et avec nettement moins de moyens à engager pour la réalisation.

Vous indiquez l'intégration de ZENIOO avec d'autres systèmes, comment cela se traduit ?

Emmanuel Legras - Notre solution modulaire permet de s'interfacer rapidement avec de nouveaux partenaires. Nos courtiers peuvent aussi profiter de cette modularité de la même manière en marque blanche complète ou en sélectionnant les services ou modules dont ils ont besoin en les intégrant dans leurs outils.

Actuellement nous sommes connectés à 5 gestionnaires différents dont certains sont multibranches, pour 16 produits et 7 assureurs.

Quelles sont les évolutions à venir ?

Emmanuel Legras - Il s'agit de renforcer notre proposition sur la place de marché avec des produits tiers en partenariat, développer de nouvelles offres, par exemple, sur le risque cyber, ce que nous venons de lancer en partenariat avec l'insurtech Stoik, ou le dommage.

Ce renforcement sera réalisé selon nos principes de mise en œuvre des parcours avec notre SI pour ne pas se cantonner à un simple positionnement de liens et apporter un vrai savoir-faire et un accompagnement à nos courtiers.

Nous souhaitons continuer à accompagner nos courtiers sur les services complémentaires : RH, formation, conformité et côté commercial, diagnostic et digitalisation. ■



DORA

La future réglementation de la sécurité numérique obligatoire des « entités financières »

LAURENT CHAILLOU CONSULTANT SENIOR ASSURANCE HARDIS GROUP



Le contexte

Cybersécurité, protection des données personnelles, anonymisation des connexions... depuis quelques temps ces sujets qui concernent aussi bien les individus que les entreprises de tous secteurs font régulièrement l'actualité.

Selon le dernier rapport de la Geneva Association, les rançongiciels représentaient 75 % de toutes les réclamations de cyber assurance en 2020, les rançongiciels seraient la catégorie d'événements de perte la plus coûteuse pour les assureurs en 2021.

En septembre 2020, suivant les orientations de la BCE et s'appuyant sur les principes de la Directive UE «NIS» (Network and Information Security), le projet de règlement européen DORA (Digital Operational Resilience Act) est proposé. Il concerne le secteur de la finance et des assurances et a vocation à renforcer la résilience opérationnelle informatique des acteurs financiers en mettant en place, notamment, un nouveau cadre obligatoire de gouvernance et de contrôle interne.

Le 10 mai 2022, lors de la présidence française, le projet de texte a fait l'objet d'un «accord technique», préambule à son adoption finale par le Parlement de l'UE et les États membres. S'agissant d'un Règlement (à l'instar du RGPD), il s'appliquera à tous les états membres dès sa validation.

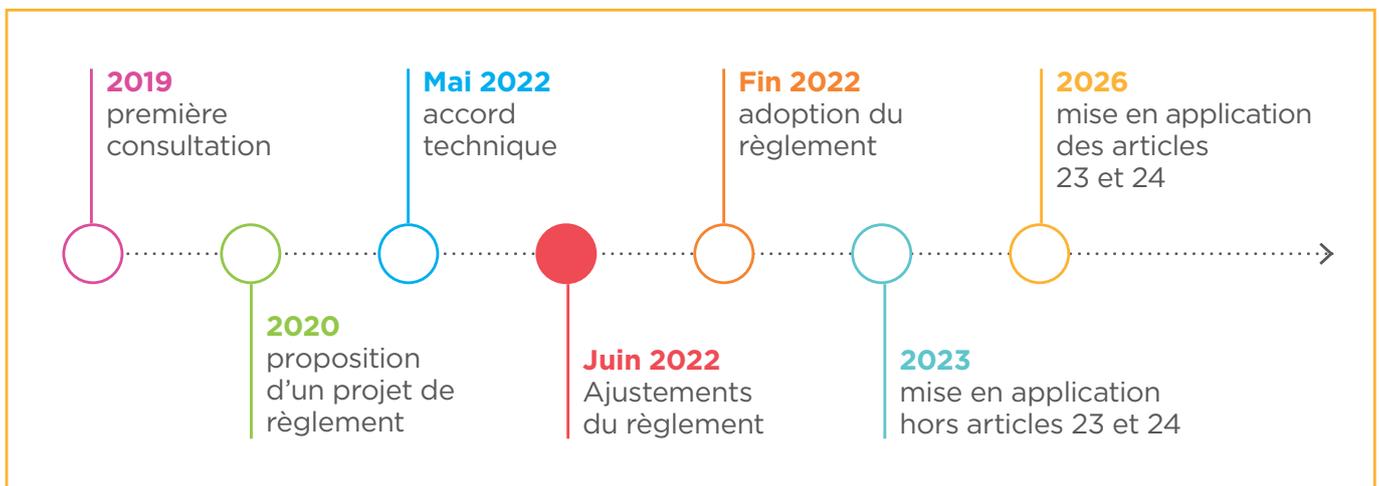
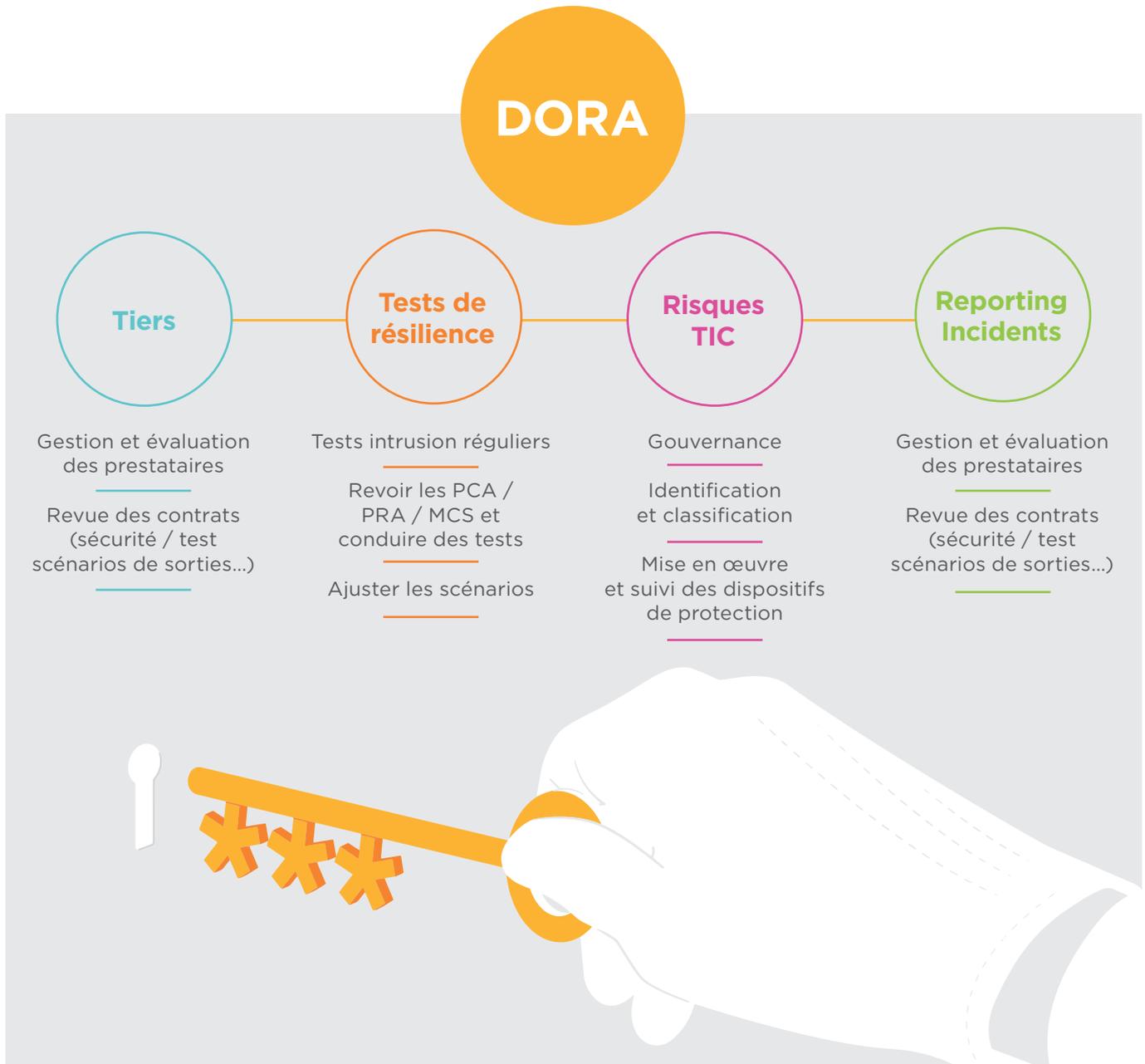
Ce nouveau cadre légal commun aux 27 pays de l'UE réglemente :

- **La gestion des risques** (identification et mise en place de politiques écrites de sécurité) ;
- **Le déploiement obligatoire d'outils logiciels de surveillance des systèmes d'information,**
- **La mise en œuvre de tests de résilience opérationnelle informatique ;**
- **La gestion des risques liés aux tiers** et particulièrement la supervision des prestataires critiques, avec rédaction de clauses contractuelles obligatoires;
- **L'uniformisation, la généralisation et l'obligation de détecter les vulnérabilités** et de rapporter les incidents de sécurité.

Pour y voir plus clair, nous vous proposons le point de vue d'experts sur les impacts de ce nouveau règlement.



DORA en résumé





Douchka Pharose

CONSULTANTE
AUDITRICE INDÉPENDANTE

Douchka accompagne principalement des établissements financiers dans leur mise en conformité selon les réglementations en vigueur et dans l'optimisation de leurs processus internes. Elle propose également des formations dans le domaine de la conformité bancaire.

Les établissements financiers considèrent souvent l'arrivée d'une nouvelle réglementation comme une contrainte. Néanmoins la réglementation DORA sera bénéfique sous de nombreux aspects. Tout d'abord cette réglementation est nécessaire pour au moins deux raisons.

Jusqu'ici l'absence de règles détaillées et précises sur la résilience opérationnelle numérique a favorisé de nombreuses initiatives réglementaires et pratiques de surveillance au niveau national. Cette situation générerait un manque de coordination, des incohérences, des exigences redondantes et des risques non traités.

De plus, les risques numériques ne cessent d'augmenter. Cela est cohérent avec l'accélération du numérique par les consommateurs européens depuis la COVID19. L'intensification du télétravail a aussi fait émerger de nouveaux risques. Durant la période de confinement, entre février et avril 2020, on a pu constater un triplement des cyber-attaques contre les institutions financières dans le monde.

Cette réglementation a également un aspect très novateur dans le monde bancaire. Pour la première fois, un règlement unique sera applicable aussi bien aux établissements de crédit qu'aux tiers prestataires de services informatiques. Les « fournisseurs TIC » critiques seront contrôlés par une autorité de supervision. L'autorité pourra procéder à des contrôles sur pièces ou sur place et aura également le pouvoir de prononcer des sanctions en cas de non-conformité, notamment des pénalités financières et des astreintes journalières. Le régulateur pourra également demander à un établissement de mettre fin à un accord contractuel avec un prestataire évalué insuffisant.

Jusqu'ici les banques se retrouvaient parfois face à un mur dans la négociation avec leurs fournisseurs lors de la mise en conformité contractuelle selon les réglementations en vigueur (par ex. : *Les Orientations de l'EBA sur l'externalisation 2019*). Je suis convaincue que DORA sera un outil de négociation très utile aux banques qui favorisera une volonté commune de mise en conformité et de sécurisation. ■

DORA sera un outil de négociation très utile aux banques qui favorisera une volonté commune de mise en conformité et de sécurisation.





Marc-Antoine Ledieu

AVOCAT À LA COUR ET RSSI

Il est spécialiste du droit des contrats et de la sécurité des systèmes d'information et anime le blog <https://technique-et-droit-du-numérique.fr>. Il enseigne dans le Master 2 PRO « droit du numérique » à Paris II Panthéon-Assas.



Jean-Philippe Gaulier

RSSI ET DG CYBERZEN

RSSI et DG Cyberzen est un ancien RSSI de groupes internationaux dans lesquels il s'est illustré pour la gestion des fournisseurs IT, sujet pour lequel il a été primé aux « Assises de la Sécurité » par ses pairs en 2017, la protection des données personnelles, la protection en profondeur et la gouvernance de la cybersécurité au sein des organisations.

Il est le président de l'OSSIR depuis 2015 et contributeur régulier du premier podcast français NoLimitSecu.

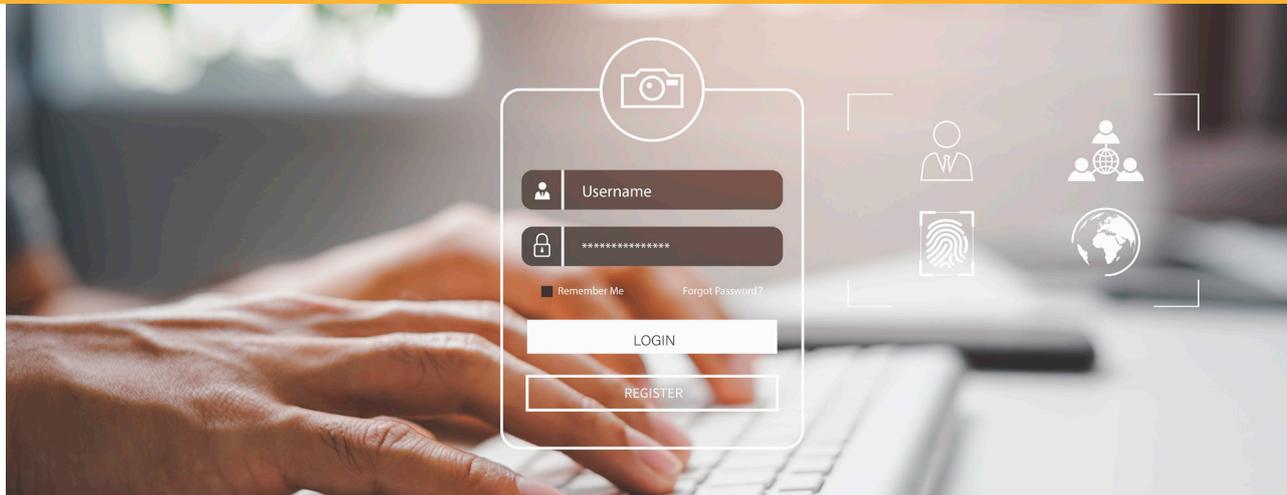
Qui est concerné ?

Les établissements de crédit et de paiement, les prestataires de services sur crypto-actifs, les entreprises d'assurance et leurs intermédiaires, les institutions de retraite professionnelle (20 catégories d'entreprises sont précisées), mais aussi leurs « prestataires de services informatiques », qu'il s'agisse de services « SaaS/ cloud » ou de la fourniture de logiciels « on premise » (installés directement dans le système d'information de l'entreprise utilisatrice).

DORA ne s'appliquera pas aux micro-entreprises du secteur (moins de 10 personnes et CA inférieur à 2 millions d'euros). Ce plafond en revanche ne concerne pas les prestataires IT.

Le projet DORA couvre également l'intégrité, la sûreté et la résilience des infrastructures et installations physiques, et les futures obligations relatives à la communication et à la gestion de crise font l'objet, à l'identique du reste de ce texte, d'obligations très détaillées.





Comment est définie la menace dans DORA ?

La menace provient de la « vulnérabilité systémique » du secteur et des « cyber-incidents » qui risquent de se propager de l'une des quelques 22 000 entités financières de l'UE à l'ensemble du système financier. La menace des rançongiciels a donc eu ce bénéfice de faire comprendre qu'une cyber-attaque ne s'arrête pas aux frontières géographiques d'un état.

La menace est donc le fait d'un problème matériel ou numérique externe, provenant directement d'un tiers malveillant ou indirectement d'une attaque dite de *supply chain*.

Le projet DORA couvre également l'intégrité, la sûreté et la résilience des infrastructures et installations physiques, et les futures obligations relatives à la communication et à la gestion de crise font l'objet, à l'identique du reste de ce texte, d'obligations très détaillées.

Qu'est-ce que la résilience numérique opérationnelle ?

Cela concerne (i) la disponibilité et (ii) la qualité des services rendus par les entités financières. Il s'agit pour l'UE de lutter contre les conséquences de tout type d'incidents affectant la production informatique des entreprises du secteur.

L'article 1^{er} du projet DORA est d'ailleurs assez clair sur ce point : il s'agit d'assurer la sécurité des réseaux et des systèmes d'information sous-tendant les processus opérationnels des entités financières, c'est-à-dire la continuité de leurs activités opérationnelles.

Il faudra également pour les entreprises du secteur s'assurer de limiter les dégâts et de redémarrer la production afin de résoudre immédiatement et rapidement tout incident,

notamment en cas de cyber-attaque. Dans ce cas, la priorité doit être donnée à la reprise des activités et aux mesures de rétablissement.

DORA prend néanmoins soin de préciser que le redémarrage de l'activité de l'entité impactée ne devra « en aucun cas compromettre l'intégrité et la sécurité des réseaux et des systèmes d'information ni la confidentialité des données ».

Comment cela se traduit-il concrètement ?

DORA se décompose en un inventaire d'obligations techniques à mettre en œuvre portant notamment sur les politiques, procédures et contrôles de l'identification des utilisateurs et du contrôle d'accès aux systèmes d'information. Il est également question de protection des secrets cryptographiques avec la mise en place de mécanismes d'authentification forte, et des systèmes de contrôle dédiés pour empêcher l'accès aux clés de chiffrement sur la base des résultats des processus approuvés de classification des données.

Les systèmes et applications informatiques essentiels seront soumis au moins une fois par an à l'évaluation de l'état de préparation de leur sécurité numérique. Pour cela, il faudra recenser leurs faiblesses, défaillances ou lacunes pour pouvoir mettre rapidement en œuvre des mesures correctives. A ces fins, il faudra établir, maintenir et réexaminer des programmes complets de tests numériques, à effectuer par des parties indépendantes, internes ou externes qui devront très probablement être labellisées.

DORA imposera enfin d'assurer un suivi et un contrôle permanents des incidents de sécurité. Pour cela, les entreprises du secteur financier devront mettre en place des mécanismes permettant de détecter rapidement les activités anormales, y compris les problèmes de performance.

Quel est l'impact sur les relations avec les prestataires ?

DORA prévoit toute une série de dispositions relatives au suivi rigoureux du risque lié aux prestataires de services informatiques, lors de la conclusion du contrat de fourniture ou de service, de son exécution, de sa résiliation et de la phase post-contractuelle.

En synthèse, il faudra prévoir dans les contrats une description complète des services, l'indication des lieux où les données doivent être traitées, une description complète des niveaux de services accompagnée d'objectifs de performance quantitatifs et qualitatifs, des dispositions sur l'accessibilité, la disponibilité, l'intégrité, la sécurité et la protection des données à caractère personnel, des garanties d'accès, de récupération et de restitution en cas de défaillance des prestataires, les délais de préavis et les obligations d'information (à la charge des prestataires), les droits d'accès, d'inspection et d'audit par les entités financières, des droits de résiliation clairs voire des stratégies de sortie spécifiques. ■



Conclusion

La future organisation de la résilience opérationnelle devra prendre en compte la réalité tant du fonctionnement des systèmes d'information des entreprises du secteur financier que des services rendus à leurs clients, en BtoB comme en BtoC.

Si les grandes banques et assurances sont probablement bien armées pour anticiper l'arrivée de ce nouveau règlement (2024 à confirmer), il n'en est certainement pas de même pour les plus petites structures et les nombreux sous-traitants qui traitent et partagent les données du secteur. Cette obligation de résilience leur imposera un travail de mise en conformité en profondeur pour mettre en œuvre, de manière concrète, pragmatique et évolutive, un grand nombre de mesures techniques destinées à garantir une gestion solide de leurs risques numériques. ■



Le développement de l'assurance du risque cyber

La direction générale du Trésor, dans un rapport remis le 7 septembre, propose un plan d'actions pour développer l'assurance du risque cyber et répondre aux défis croissants qui peuvent menacer la santé économique des entreprises.

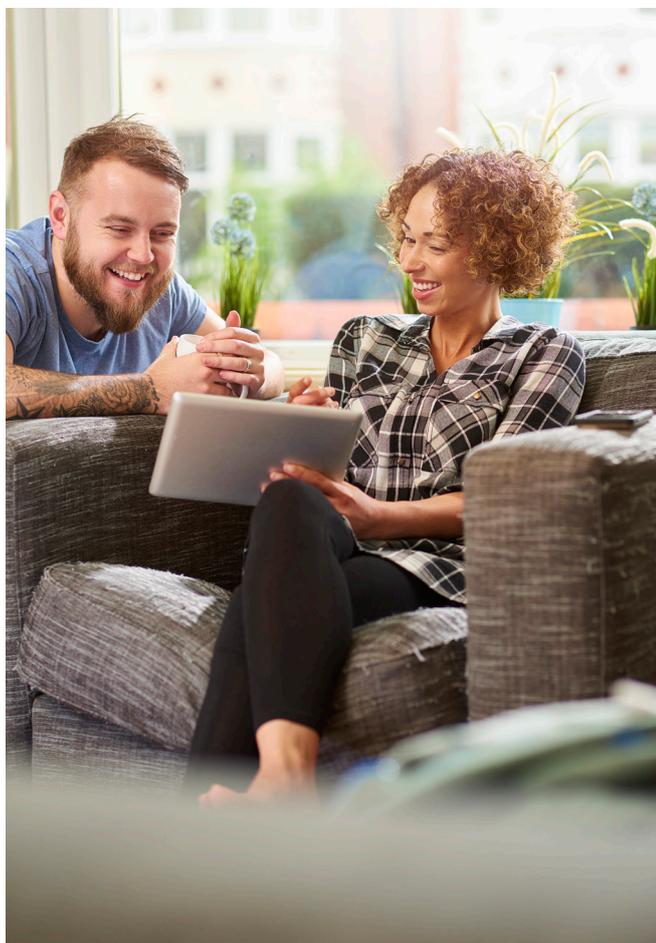
[Consulter le rapport cyber](#)

À la suite d'une concertation avec les acteurs concernés, la direction générale du Trésor propose, dans un rapport dédié, un plan d'actions pour développer l'assurance du risque cyber et répondre aux défis croissants qui peuvent menacer la santé économique des entreprises.

Ce plan s'articule autour de quatre axes :

- clarifier le cadre juridique de l'assurance du risque cyber ;
- favoriser une meilleure mesure du risque cyber ;
- améliorer le partage de risque entre assurés, assureurs et réassureurs ;
- accroître les efforts de sensibilisation des entreprises au risque cyber.

L'une des mesures faisant débat concerne le conditionnement de l'assurabilité au dépôt de plainte de la victime. C'est une mesure législative proposée et prévue à court terme. ■



Amazon arrête son activité de télémédecine

Amazon va stopper son service de télémédecine Amazon Care à la fin de l'année après seulement 3 ans d'activité. Amazon Care connecte en ligne les patients avec des médecins et des infirmières qui peuvent fournir un traitement à n'importe quelle heure. Le service n'a pas d'agence, mais offre des services en personne pour des soins comme les vaccinations et les tests de dépistage de la grippe.

Ce service a été lancé en 2019 pour une partie des employés d'Amazon qui ont servi d'utilisateurs d'essai, il a depuis été étendu à l'ensemble du géant de l'e-commerce dans les 50 états américains, ainsi que pour d'autres entreprises du secteur privé. "Amazon Care n'est pas une offre assez complète pour les grandes entreprises visées et n'aurait pu rencontrer de succès à long terme" a affirmé Neil Lindsay, le responsable de l'activité Services de santé.

Le groupe reste déterminé à investir dans le secteur et imaginer l'avenir de la santé malgré cet arrêt. « La structuration d'Amazon Care a amélioré notre compréhension des besoins en matière de services de santé pour les sociétés et les clients particuliers », a expliqué le dirigeant. ■



20 millions d'euros supplémentaires pour **la cybersécurité des établissements de santé**

Selon l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), 27 hôpitaux ont été ciblés par une cyberattaque en 2020 et en moyenne un incident par semaine a été recensé en 2021 dans un établissement du secteur de la santé.

Dernièrement c'est le centre hospitalier de Corbeil-Essonnes qui a été touché. Son fonctionnement est fortement impacté depuis une attaque survenu dimanche 21 août. Les hackers ont réclamé une rançon de 10 millions de dollars.

En visite dans le centre hospitalier, François Braun, Ministre de la Santé et de la Prévention, a exprimé son soutien à l'ensemble du personnel et a annoncé un investissement de « 20 millions d'euros supplémentaires pour la cybersécurité de nos hôpitaux ». Pour le ministre, « la santé des Français » ne doit pas être « prise en otage ».

Comme indiqué par Jean-Noël Barrot, Ministre délégué chargé de la Transition numérique et des Télécommunications, ces 20 millions d'euros seront alloués à l'ANSSI pour qu'elle « renforce son accompagnement auprès des établissements de santé. »

Ces 20 millions viennent s'ajouter aux 25 millions d'euros déjà alloués sur le sujet pour 2021 et 2022. ■

Le secteur de l'assurance concerné par la **“Loi pouvoir d'achat”**

Résiliation en 3 clics

L'article 17 de la Loi pouvoir d'achat du 16 Août 2022 oblige les assureurs à proposer de manière permanente une fonctionnalité gratuite de résiliation par voie électronique, d'accès simple et direct. Cette disposition s'applique dès lors que l'assureur offre la possibilité de conclure des contrats par voie électronique, et ce même si le contrat à résilier n'a pas été conclu en ligne. Un décret à paraître doit fixer les modalités d'accès et d'affichage de la fonctionnalité, les données à fournir par le souscripteur et les modalités techniques qui garantiront l'identification de ce souscripteur.

En outre, l'assureur doit confirmer la bonne réception de la notification de résiliation et communiquer à l'assuré, « sur support durable » et « dans un délai raisonnable », la date à laquelle le contrat prend fin et les effets de la résiliation.

Cette mesure entrera en vigueur au plus tard le 1^{er} juin 2023. La date d'application définitive sera fixée par décret.

Assurance affinitaire

Concernant les assurances dites affinitaires, les assurés bénéficieront d'un droit de renonciation de 30 jours contre 14 aujourd'hui, et ce sans aucune condition. Cette mesure s'appliquera à partir du 1^{er} janvier 2023 (article 18 de la loi Pouvoir d'achat du 16 août 2022). ■

light up

L'ACTUALITÉ DE LA TRANSFORMATION
ET DE L'INNOVATION ASSURANCE

INSURANCE & FINANCIAL SERVICES BY HARDIS GROUP

ifs.hardis-group.com

LIGHT UP
YOUR FUTURE _

HARDIS GROUP

hardis-group.com

Société de conseil, ESN et éditeur de logiciels, Hardis Group s'est donné pour mission d'accélérer la transformation de la chaîne de valeur de ses clients par et avec les nouvelles technologies. Ses équipes accompagnent les transformations stratégiques, organisationnelles et technologiques des entreprises afin de développer leur compétitivité et leur productivité.

Au sein d'Hardis Group, la business unit Insurance & Financial Services compte plus de 60 consultants experts du secteur de l'assurance, des mutuelles, des banques et organismes financiers. Cette entité accompagne les entreprises dans leurs transformations grâce à la technologie afin qu'elles puissent relever leurs défis stratégiques de création de valeur, de différenciation et d'efficacité opérationnelle, et répondre à leurs enjeux de transformation organisationnelle et IT.

Créée en 1984, Hardis Group compte 1 200 collaborateurs. La société a réalisé un chiffre d'affaires de 119,4 millions d'euros en 2020. Elle est implantée à Grenoble (siège social), Paris, Lyon, Lille, Nantes, Bordeaux, Madrid, Utrecht et Varsovie.

REMERCIEMENTS_

Nous remercions tous les intervenants de ce numéro pour le temps qu'ils nous ont accordé.

Propos recueillis entre mai et septembre 2022



**Abonnez-vous et accédez
aux anciens numéros**

ÉQUIPE LIGHT UP #4

RÉDACTION_

Marika Talbi
Laurent Chaillou
Guillaume Frison
Mickaël Chabert
Vincent Bonnabaud
Johan Cote

Consultante Senior Assurance
Consultant Senior Assurance
Consultant Assurance
Consultant Assurance
Consultant Senior Manager
Directeur BU Assurance & Services Financiers

MISE EN PAGE_

Clara Cartier Millon
Fleur Gimond
Nicolas Chavan
Responsable marketing
Designer Graphique
Webmaster