Se faire certifier, bonne ou mauvaise idée ? Le retour d'expérience d'Hyperlex

La startup Legaltech vient d'obtenir la norme ISO relative à la sécurisation des données et à la protection de la vie privée. Une étape importante qui vient couronner une année de dur labeur.

Temps de lecture : minute

6 octobre 2021

Les normes ISO, cet univers impitoyable. Autant pour ceux qui les lisent - mais qu'est-ce donc que les normes ISO26000 ou ISO37001 ? - que pour ceux qui doivent s'y conformer. Pourtant, obtenir le fameux sésame est une grande étape dans la vie d'une startup, comme en témoignent les certifications ISO/IEC 27001:2013 et ISO27701:2019 obtenues par Hyperlex. Pour les non-initiés, il s'agit de deux certifications relatives à la sécurité des informations et à la protection de la vie privée.

Pour la startup spécialisée dans la gestion de contrats, se conformer à cette norme n'était pas un passage obligé mais permet de faciliter les discussions avec certains clients, notamment les grands groupes. " *Depuis le Covid, avec l'essor du télétravail notamment, les sujets cybersécurité ont pris de plus en plus d'importance en entreprise*, observe Christophe Henner, COO d'Hyperlex. *Il y a aujourd'hui une prime à être certifié pour travailler avec les grands groupes mais aussi avec de plus en plus d'ETI.* "

Une opération chronophage

Gare cependant à ceux qui se rueraient déjà sur les catalogues de normes

pour y trouver leur bonheur. Le chemin est long, fastidieux et mieux vaut savoir dans quoi l'on s'engage. " *En regardant les dispositifs requis, nous avions évalué que la certification nécessiterait un équivalent temps plein durant une année et un peu moins d'un mi-temps pour la gestion de projet* ", calcule Christophe Henner, qui a eu le compas dans l'oeil puisque cette première estimation s'est avérée cohérente. Même si la startup avait sous-estimé " *la phase de pré-audit* ", très chronophage.

D'autant que malgré la désignation de personnes référentes, presque toutes les équipes de la startup ont été mobilisées à un moment ou un autre de la certification. " *Afin de vérifier que les process sont bien en place, les personnes chargées de l'audit interagissent avec tous les services pour vérifier que tout le monde comprend bien les enjeux et la méthodologie mise en place.* " Impossible donc pour des startups dont les équipes ne comptent que quelques personnes de pouvoir se lancer dans un tel défi. " *Sauf si cela est absolument nécessaire d'un point de vue business, je ne le conseille pas à des startups qui comptent moins d'une vingtaine de personnes dans leur équipe* ", tranche Christophe Henner.

Il faut aussi garder en tête que la certification, une fois obtenue, est vérifiée tous les ans. Ce qui signifie autant de visites de contrôle, avec l'obligation de s'améliorer chaque année car, en matière de sécurité, " *faire aussi bien que l'année précédente n'est pas suffisant* ", rappelle le COO. De quoi décourager les touristes de la certif.

Bien se préparer

Pour gagner du temps, Hyperlex a eu recours à deux astuces. D'abord, la startup a pris le temps de se familiariser avec les pré-requis des normes ISO concernées avant même d'engager le processus de certification. " *Acheter la norme, la lire et regarder ce qui est attendu permet de mettre en place des bonnes pratiques*, confirme le COO. *Certaines actions ne pourront pas être faites dans l'immédiat mais d'autres peuvent être mises*

en place dès le début. Une fois la certification engagée, nous répondions déjà à environ un tiers du référentiel. " Cela permet de lisser la procédure sur plusieurs mois, voire années, et de prendre dès le départ de bonnes habitudes plutôt que d'avoir à en changer.

Ensuite, l'entreprise a tenu à se faire accompagner par un cabinet extérieur, notamment pour " *s'approprier la norme* ". En-dehors du fait que la documentation fournie présente un jargon parfois peu explicite pour ceux qui n'y sont pas rompus, il s'agit surtout de " *traduire le côté normatif dans ce que ça voulait dire concrètement pour nous* ", explique Christophe Henner. " *La certification consiste en un mélange entre l'esprit de la norme, qui explicite la raison pour laquelle la norme existe, et des points contrôlés pour vérifier son respect. Mais ce qui prime, c'est l'intention de la norme et c'est une sacrée gymnastique intellectuelle* ", reconnaît le COO.

Cela vaut d'autant plus le coup de se pencher sur la différence qu'il y a parfois des bonnes surprises : comme la norme doit pouvoir s'adapter à n'importe quel type d'entreprise, elle présente des pré-requis qu'une startup SaaS n'est pas obligée de remplir. Alors que certaines entreprises devront se conformer à des dispositifs de sécurisation de la production en cas de catastrophe naturelle. Par exemple, Hyperlex n'a eu qu'à prouver qu'une inondation de ses bureaux n'affecterait en rien son activité...

Malgré l'investissement conséquent, autant en temps qu'en argent - environ 30 000 euros pour l'accompagnement extérieur - Hyperlex voit aujourd'hui les bénéfices de ce qui s'est apparenté pendant de longs mois à un chemin de croix. La norme ISO lui permet paradoxalement de gagner du temps lorsqu'il s'agit de passer les fourches caudines des grands comptes en matière de sécurité des données.

Article écrit par Geraldine Russell