Signature électronique : 3 critères clés pour faire son choix

La signature électronique s'est largement démocratisée depuis l'apparition des restrictions sanitaires et la généralisation du télétravail. Fort d'une très nette augmentation de la demande, ce marché a aiguisé l'appétit de certains prestataires. Pourtant le choix d'un tel service est loin d'être anodin car il exige de ceux-ci une capacité à assumer une responsabilité juridique forte, tout en étant capable d'accompagner les entreprises sur les aspects légaux liés à leurs usages de signature électronique. Seul un Prestataire de Services de Confiance (PSCo) qualifié selon le règlement européen eIDAS peut véritablement maîtriser les enjeux techniques et juridiques d'une telle solution, au profit de la sécurité de ses clients et des signataires.

Maîtriser les risques en garantissant la valeur juridique

Avec le développement des transactions numériques, il est de plus en plus difficile de s'assurer qu'une personne est véritablement celle qu'elle prétend être. Le vol d'identité est en hausse et la France est loin d'être épargnée par l'augmentation du nombre de fraudes en la matière. Selon le cabinet d'audit PwC, 53% des entreprises françaises auraient été victimes de fraudes à l'identité dont le montant est équivalant à 1,4 milliard de dollars de pertes au cours des 24 derniers mois. Les enjeux d'identification et d'authentification, notamment dans les processus de contractualisation dématérialisés, sont centraux et nécessitent donc de comprendre ce qu'ils impliquent pour les utilisateurs.

S'il revient au PSCo de proposer différents niveaux de sécurité de signatures répondant à différents types de risques en matière de signature électronique, les entreprises doivent quant à elles évaluer le niveau de risque lié aux documents qui seront signés. Le règlement eIDAS est à l'origine de trois niveaux de signature : simple, avancée et qualifiée. Ces trois niveaux de signature sont mis en oeuvre grâce à différents moyens d'identification électronique permettant de mieux maîtriser les risques d'usurpation d'identité. Plus le niveau de sécurité d'une signature augmente, plus les points de contrôle (à distance ou en face-à-face) de l'identité du signataire sont renforcés, réduisant ainsi le risque d'usurpation d'identité dans le cadre des transactions réalisées. Dans tous les cas, une signature électronique doit prouver l'identification du signataire et l'intégrité du document signé. L'horodatage qualifié apporte par ailleurs un niveau de sécurité supplémentaire en garantissant l'existence d'un fichier à une date donnée et que celui-ci n'a pas été modifié depuis. Il contribue ainsi à assurer l'intégrité du document signé.

Depuis 2014, le règlement eIDAS a été adopté par le Parlement européen et le Conseil de l'Union européenne. Il permet notamment de qualifier un PSCo dont le rôle est de recueillir le consentement éclairé du signataire, c'est-à-dire le recueil de la preuve du consentement. Selon le niveau d'identification requis, le PSCo est habilité à vérifier l'identité du signataire au moyen de procédés fiables garantissant le lien entre son identité régalienne et l'acte.

Bien qu'il s'agisse avant tout d'une opération à caractère légal comportant une dimension technique complexe entre l'acte de signature et le procédé d'identification du signataire, la signature électronique ne doit pas se faire au détriment de l'expérience utilisateur. C'est notamment pour cette raison que certains PSCo proposent aux signataires disposant déjà d'un certificat de pouvoir le

réutiliser lors de futures signatures. Les Prestataires de Services de Confiance disposant d'une base d'identités numériques suffisamment large simplifient ainsi l'expérience utilisateur. Si la valeur juridique d'une signature électronique est un élément de choix majeur dans le cadre des problématiques d'identification et d'authentification pour limiter les usurpations d'identités, le nombre de certificats qualifiés détenus par un PSCo s'avère également un critère important.

Garantir la sécurité et la confidentialité des données au regard du cadre européen

Un PSCo doit garantir un haut niveau de sécurité sur les données de ses utilisateurs, aspect crucial pour la pérennité d'une organisation. Le vol ou la perte de données, la non-conformité avec les procédures légales telles que le RGPD, ou encore le coût engendré par une interruption de service peuvent effectivement infliger des dommages considérables à une entreprise. Qu'il s'agisse de se protéger contre les piratages externes, la divulgation d'information ou l'erreur humaine, la sécurité doit être au coeur de l'offre de service d'un Prestaire de Services de Confiance.

En raison de la nature juridique de la signature électronique, les PSCo sont étroitement concernés par la question du traitement des données personnelles. La sécurité des données liées à la contractualisation, la vérification de l'identité, la signature et la conservation du document à valeur probante, imposent que la localisation, le stockage et le traitement de ces données soient effectués au sein de l'Union européenne. Il est ainsi important qu'un PSCo qualifié selon le règlement européen eIDAS opère l'intégralité du traitement des données de ses clients en Europe et que ses infrastructures soient également localisées au sein de l'Union européenne. Ce dernier pourra alors garantir que le traitement des données personnelles sera sécurisé et réalisé dans le respect du RGPD. En France, la sécurisation des données et de la valeur juridique inhérentes à l'usage d'un service qualifié eIDAS sont garanties par l'évaluation régulière de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), sur la base d'un audit eIDAS.

Accompagner l'entreprise dans ses besoins spécifiques

Le contexte sanitaire et les exigences globales du marché rendent la signature électronique de plus en plus indispensable et, plus largement, la dématérialisation des processus métier s'impose comme un réel enjeu de compétitivité pour toute entreprise.

Être en mesure de comprendre la stratégie de contractualisation digitale d'une entreprise et l'agrégation des solutions actuelles ou futures au sein d'une organisation nécessite de solides compétences pour offrir des réponses adaptées. Les entreprises ont donc besoin d'un accompagnement pour évaluer et réduire les écueils (juridiques, financiers et business) inhérents pour tirer le meilleur parti d'une solution de signature électronique, tout en limitant les risques possibles selon les métiers ou les activités. A titre d'exemple, lorsqu'un PSCo dispose d'une connaissance pointue d'un marché au regard de ses clients, il bénéficie d'une expertise spécifique forte et sera ainsi à même de formuler des conseils plus pertinents au regard des pratiques métier.

Les entreprises doivent ainsi demander aux experts que sont les PSCo de partager leurs expériences et leurs connaissances juridiques. La prise en compte des risques métier liés à la nature du contrat et aux contraintes réglementaires sont les gages de réussite de leurs projets. C'est en intégrant tous ces paramètres que les entreprises pourront tirer pleinement parti des bénéfices de la signature électronique pour leur activité.