Adobe Sign

Les clés du succès de la signature électronique

Mettre en place une politique de signature électronique efficace.

Les signatures électroniques transforment les pratiques commerciales des entreprises. Non seulement elles leur épargnent la transmission de contrats imprimés, mais elles accélèrent considérablement les processus de signature et de validation. Et surtout, leur intégration dans les workflows en place est plus simple que vous ne le pensez. La définition d'une politique de signature globale constitue un excellent point de départ.

Une politique de signature électronique efficace définit les consignes d'utilisation des signatures électroniques et vous aide à vous assurer que vos processus de signature sont conformes aux législations locales et internationales, ainsi qu'aux diverses règlementations. L'élaboration d'une politique de signature électronique commence par l'identification des éléments à inclure.

Ce guide fournit des recommandations pour vous aider à créer une politique de signature électronique adaptée à votre entreprise. Les considérations ci-après permettent de définir une politique qui garantit la légalité et la validité juridique de vos contrats électroniques.

Comprendre la législation relative aux signatures électroniques.

Les signatures électroniques ont force exécutoire et sont juridiquement recevables dans la quasi-totalité des pays industrialisés. Toutefois, comme la législation relative aux signatures électroniques varie d'un pays à l'autre, il est judicieux de définir une politique de signature électronique d'entreprise applicable dans tous les pays où vous exercez vos activités. Avant de commencer à définir votre politique, il est important de comprendre la législation relative aux signatures électroniques et son impact au niveau local et international.

Il existe actuellement dans le monde deux types de législation sur les signatures électroniques.

- **Législation minimaliste** : de nombreux pays, tels que les États-Unis, l'Australie, la Nouvelle-Zélande et le Canada, possèdent une législation minimaliste ou permissive, qui permet d'appliquer des signatures électroniques avec un minimum de restrictions légales et accordent aux signatures électroniques la même valeur légale qu'aux signatures manuscrites.
- **Législation à plusieurs niveaux** : les pays qui possèdent une législation à plusieurs niveaux permettent généralement d'utiliser les signatures électroniques, mais accordent une plus grande valeur probante aux signatures qui utilisent différents types d'identifiants numériques basés sur un certificat pour authentifier les signataires. L'Union européenne, la Chine, l'Inde, la Corée du Sud et d'autres zones géographiques et pays ont adopté une législation à plusieurs niveaux. Par exemple, dans l'Union européenne, seules les signatures qui utilisent des identifiants numériques de fournisseurs qualifiés reçoivent automatiquement le même statut que les signatures manuscrites.

Les solutions de signature électronique professionnelles, comme Adobe Sign, permettent de se conformer facilement à la législation minimaliste et à plusieurs niveaux, et de prendre en charge les processus métier internationaux.

Trouver une approche adaptée des signatures.

L'évaluation de vos contrats pour trouver l'approche des signatures adaptée à votre entreprise est une étape importante dans l'élaboration d'une politique de signature électronique. Vous devrez concilier au mieux règlementations et risques, et évaluer les moyens à déployer pour que vos transactions soient légales et sécurisées. Différents facteurs sont à prendre en compte, en fonction de vos processus métier, ainsi que de la législation et de la règlementation locales auxquelles ils sont soumis. Toutefois, une politique de signature électronique correctement structurée utilise généralement une ou plusieurs des méthodes ci-après pour automatiser le processus de signature et garantir la conformité.

- **Risque faible : signatures électroniques standard** : si les risques commerciaux sont faibles et si la législation le permet, de nombreuses entreprises utilisent des signatures électroniques standard pour les accords commerciaux courants, tels que les contrats, déclarations de travaux ou formulaires des employés. Une demande par e-mail est envoyée à chaque signataire via un processus de signature sécurisé. Il suffit au signataire de cliquer sur le lien unique incorporé dans l'e-mail pour accéder au document. Il s'agit là d'une méthode rudimentaire d'authentification des signataires, sachant que la plupart des utilisateurs

disposent d'un accès exclusif à un compte de messagerie. Le document est géré en toute sécurité tout au long du processus et chaque étape, y compris l'authentification, est consignée et stockée dans une piste d'audit.

Une fois que tous les utilisateurs ont signé, le document final est automatiquement envoyé à toutes les parties, avec un sceau infalsifiable pour confirmer son intégrité. Pour améliorer la conformité, les entreprises peuvent également définir des processus imposant l'obtention d'un consentement exprès aux transactions électroniques avant le début du processus de signature.

- **Risque modéré : signatures électroniques avancées** : pour renforcer la sécurité des contrats plus sensibles, de nombreuses entreprises ajoutent une deuxième forme d'authentification des signataires. Les signatures électroniques avancées fonctionnent comme les signatures électroniques standard, mais une étape supplémentaire d'authentification des signataires est ajoutée avant l'ouverture ou la signature d'un document. Les méthodes d'authentification par code PIN de téléphone, identifiant de réseaux sociaux ou mot de passe, ou encore basées sur les connaissances (KBA), offrent de meilleures garanties sur l'identité des signataires.
- **Risque élevé ou exigence règlementaire : signatures numériques** : certaines entreprises choisissent les signatures numériques pour respecter les exigences les plus strictes en matière de conformité légale et règlementaire, et protéger les processus de signature stratégiques, présentant le plus haut niveau de risque.

  Les signatures numériques sont un type particulier de signature électronique qui utilise des identifiants numériques basés sur des certificats pour authentifier l'identité du signataire. Ces identifiants sont généralement émis par une autorité de certification ou un prestataire de services de confiance. À l'instar des solutions de signature électronique, les solutions de signature numérique peuvent inclure des pistes d'audit, la distribution automatique du document final et des options de consentement explicite. La preuve de la signature est cependant différente, car la signature proprement dite est liée au document par un cryptage et peut être validée par l'autorité de certification ou le prestataire de services de confiance longtemps après la signature du document.

Pour savoir quelle approche répond le mieux aux besoins de votre entreprise en matière de signatures électroniques, posez-vous certaines questions clés sur vos processus métier :

- Une législation applicable impose-t-elle une forme particulière de signature ?
- Suis-je prêt à investir pour équiper tous les signataires d'identifiants numériques ?
- Quelle est la probabilité que cette signature soit contestée et quel est le risque associé ?
- L'obligation de fournir un identifiant numérique peut-elle constituer un obstacle pour les clients ?

Intégrer les bonnes pratiques dans votre politique.

Sachant que toutes les lois relatives aux signatures électroniques partagent les mêmes principes fondamentaux, que vous exerciez votre activité dans un ou plusieurs pays, votre politique de signature doit répondre à six questions clés pour garantir la légalité et la validité juridique de vos contrats électroniques.

1. **Authentification :** Qui a signé ?
2. **Intention de signer :** Le signataire a-t-il montré son intention de signer ?
3. **Preuve de la signature :** Pouvez-vous prouver qu'un document particulier a été signé et n'a pas été modifié depuis sa signature ?
4. **Accord :** Le signataire a-t-il accepté de s'engager par voie électronique ?
5. **Exceptions :** Certains types de document sont-ils exclus ?
6. **Conservation :** Quelle doit être la durée d'archivage de vos documents ?

Authentifier l'identité des signataires.

Votre processus de signature électronique doit permettre d'identifier et d'authentifier les signataires durant le processus de signature. La plupart des entreprises choisissent l'une ou plusieurs des méthodes décrites dans la section précédente, en fonction de leurs exigences en matière de risques et de conformité pour leurs processus métier. Adobe Sign prend en charge toutes ces méthodes dans une seule solution, ce qui simplifie le choix de la bonne approche pour chaque processus.

Démontrer l'intention de signer.

Vos processus doivent inclure une étape où le signataire accomplit une action précise (ex., saisir ou écrire un nom, ou cliquer sur un bouton), afin de signifier son intention de signer. Les signataires doivent également avoir la possibilité de s'opposer à la signature d'un contrat par voie électronique. Ces deux fonctions sont intégrées dans les processus d'Adobe Sign.

Établir une preuve de la signature.

Pour être considérée comme une signature électronique, une signature doit être associée au document qui a été signé.

C'est pourquoi Adobe Sign garantit la sécurité des documents tout au long du processus de signature et certifie leur intégrité avec un sceau infalsifiable. Chaque étape est consignée dans une piste d'audit sécurisée, qui constitue une preuve irréfutable, facile à produire, de la signature de chaque partie. Une fois qu'un document a été signé, tous les signataires reçoivent une copie électronique complète et non modifiée du contrat pour référence et archivage.

Autoriser les transactions électroniques.

De nombreuses lois sur les signatures électroniques exigent une forme de consentement aux transactions par voie électronique. Les solutions de signature électronique telles qu'Adobe Sign intègrent ce consentement sous une forme ou une autre dans le workflow de signature. Il est donc inutile de modifier vos documents. Toutefois, si vous souhaitez insérer une autre langue dans le corps du document lui-même, prévoyez d'ajouter une clause de consentement dans vos contrats. La clause suivante peut par exemple figurer directement au-dessus du bloc de signature :

> **Attention :** En signant ce document, vous attestez avoir pris connaissance des présentes informations destinées au consommateur, et consentez à effectuer des transactions et recevoir des avis et renseignements par voie électronique, ainsi qu'à utiliser des signatures électroniques au lieu de signatures manuscrites. La réception d'avis et publications et la signature de documents par voie électronique ne sont pas obligatoires. Vous pouvez demander à recevoir des exemplaires papier et retirer votre consentement à tout moment.

Gérer les exceptions.

Certains processus ne sont pas exécutables par voie électronique. Si vous envisagez d'exclure ou d'inclure certains contrats, indépendamment de votre politique générale, insérez une rubrique détaillant ces exceptions. Par exemple, certaines lois sur les signatures électroniques excluent les droits de mutation immobilière ou le droit de la famille. De plus, certains secteurs d'activité ultra-règlementés, comme l'industrie biopharmaceutique, acceptent uniquement les signatures numériques pour certains types de processus métier. Votre analyse des risques permet d'identifier les exceptions à inclure dans votre politique.

Archiver les documents.

Gérez vos documents signés par voie électronique, comme n'importe quel autre document. Déterminez notamment la durée d'archivage de vos documents. Les transactions par signature électronique doivent généralement être archivées aussi longtemps que les documents signés sur papier. Veillez à lire et accepter toutes les lois applicables à la politique d'archivage de votre entreprise. Les documents archivés doivent rester accessibles dans un format reproductible par toute personne autorisée à y accéder (ex., le signataire). Adobe Sign archive les document en toute sécurité dans Adobe Document Cloud. Si vous avez des documents sensibles, vous pouvez également les archiver dans un système de gestion d'archives formel ou un coffre-fort électronique.

Élaborer une politique claire.

Une fois que vous avez défini la teneur de votre politique, il est important de la rendre explicite pour les utilisateurs. Suivez les trois conseils ci-après pour rédiger une politique qui sera véritablement lue.

Déclarer l'objectif de la politique.

Définissez l'objectif de votre politique. Par exemple : « Cette politique fournit des consignes sur l'adoption des signatures électroniques, y compris sur la définition des circonstances dans lesquelles les signatures et enregistrements électroniques seront utilisés et acceptés. »

Résumer la politique.

Fournissez un résumé de votre politique. Il peut s'agir d'une courte déclaration reconnaissant la décision de votre entreprise d'accepter les signatures, validations ou autorisations électroniques nécessaires dans le cadre de ses activités comme juridiquement recevables et équivalentes aux signatures manuscrites. Si la validité des signatures électroniques est soumise à certaines conditions (ex., contrats que vous souhaitez exclure ou inclure, départements non autorisés à utiliser les signatures électroniques, etc.), spécifiez ces exceptions dans votre politique.

Définir les termes utilisés dans la politique.

Définissez les termes les plus employés pour que tous les utilisateurs sachent ce que vous voulez dire dans la langue ayant servi à rédiger votre politique. Vous trouverez quelques définitions courantes dans l'Annexe.

Publier la politique.

Une fois l'ensemble finalisé, veillez à communiquer votre politique dans toute l'entreprise afin que chacun sache quand et comment utiliser les signatures électroniques dans son workflow. Publiez votre politique à un endroit facile d'accès. Envisagez d'annoncer son déploiement lors d'une réunion ou d'un évènement afin de pouvoir fournir toutes les explications nécessaires et répondre aux questions. Enfin, vérifiez que l'implémentation au niveau de l'entreprise, y compris les modèles de document ou de workflow standard, est conforme à votre nouvelle politique.

En savoir plus.

Pour en savoir plus sur les signatures électroniques, consultez les ressources suivantes :

- Guide mondial sur la législation en matière de signatures électroniques : synthèse par pays.
- Transformer les processus métier grâce aux signatures électroniques et numériques
- Loi sur les signatures électroniques

Annexe : terminologie des signatures électroniques.

Les **signatures électroniques** désignent tout procédé électronique permettant de faire valoir l'acceptation d'un contrat ou d'un dossier. Les signatures électroniques peuvent utiliser différentes méthodes pour authentifier l'identité du signataire.

Les **systèmes de signature électronique standard** combinent une méthode d'authentification électronique unique (accès à un compte de messagerie, par exemple) et un processus sécurisé qui fournit une piste d'audit avec le document final.

Les **signatures électroniques avancées** ajoutent l'authentification à plusieurs facteurs pour vérifier l'identité du signataire. Les signataires accèdent d'abord à une URL unique envoyée à leur compte de messagerie, puis répondent à une demande d'authentification avant d'ouvrir le document. Les méthodes d'authentification les plus courantes sont les codes PIN de téléphone, les identifiants de réseaux sociaux, les mots de passe ou encore l'authentification basée sur les connaissances (KBA).

Les **signatures numériques** sont un type particulier de signature électronique qui utilise des identifiants numériques basés sur des certificats pour authentifier l'identité du signataire. Les signatures numériques fournissent une preuve de la signature en liant chaque signature au document via un système de cryptage. La validation est généralement assurée par des autorités de certification agréées ou des prestataires de services de confiance.

Les **autorités de certification** sont des sociétés ou des prestataires de services IT agréés qui délivrent des identités numériques et les gèrent. Les autorités de certification confirment d'abord l'identité d'un signataire, puis délivrent l'identifiant numérique, le code PIN privé et/ou le dispositif de sécurité (tel qu'un jeton USB ou une carte à puce) utilisé pour créer des signatures numériques.

Les **prestataires de services de confiance** sont des sociétés qui proposent une large gamme de services d'identité et de transaction sécurisés, y compris les services des autorités de certification. Par exemple, le règlement eIDAS de l'Union européenne définit une classe de prestataires de services de confiance accrédités pour délivrer des identifiants numériques dans chacun des États membres de l'UE. Les documents signés avec ces identifiants sont conformes à la norme la plus stricte, appelée « signature électronique qualifiée », qui a la même valeur légale que les signatures manuscrites.