Politique de signature électronique de SSQ Assurance

Chez SSQ Assurance, nous sommes fiers de nos normes élevées en matière de conformité des documents. En raison de notre alliance avec La Capitale, nous procédons à la révision de toutes nos procédures internes pour simplifier vos affaires avec nous et assurer la protection juridique de toutes les parties concernées.

Ce niveau de conformité sert à assurer une sécurité maximale et à réduire les risques de litige et de non-conformité, tant pour nous que pour nos réseaux de distribution. Essentiellement, la politique de conformité des documents est en place pour protéger nos clients, nos courtiers, nos AGG partenaires et SSQ Assurance.

SSQ Assurance a évalué les solutions de signature électronique énumérées ci-dessous et les a approuvées à condition qu'elles soient utilisées correctement. Il convient de noter que plusieurs de ces solutions comportent divers paramètres qui peuvent avoir une incidence sur la conformité du document et des signatures. Par conséquent, l'utilisation de l'une de ces solutions ne garantit pas à elle seule l'acceptation du document par SSQ Assurance.

– Adobe Sign	– DocuSign	– Formstack sign	– InsureSign
– Authentisign	– Esign	– HelloSign	– OneSpan
– DocHub	– eZsign	– iGeny	– Zoho

Veuillez noter que l'utilisation de toute autre plateforme de signature électronique ne répondant pas à nos critères de sécurité peut entraîner le refus d'un document.

Lorsque SSQ Assurance évalue la conformité d'une signature électronique, les éléments suivants sont vérifiés :

- **Authenticité de la signature**

  La signature est-elle authentique ? Comment pouvons-nous démontrer que le document a réellement été signé par le signataire ?

  En démontrant que seul le client peut avoir signé le document, comme au moyen de l'adresse de courriel fournie par le client sur le formulaire ou d'une authentification à deux facteurs par SMS.

- **Intégrité du document/verrouillage du document**

  Le document a-t-il été modifié, soit avant l'une des signatures ou après avoir été signé ? Le document peut-il être modifié après sa signature ? Le format du document a-t-il été modifié ?

  Cet aspect peut être vérifié lorsque la solution de signature électronique appose un **sceau de sécurité** sur le document après la réception de toutes les signatures, afin de démontrer que le document n'a pas été modifié par le processus.

- **Preuve d'authenticité et d'intégrité**

  Le document signé électroniquement contient-il toutes les **métadonnées** (adresse IP, marquage de la date et de l'heure et renseignements d'identification) requises nous permettant, au besoin, de prouver l'authenticité des signatures ou l'intégrité des documents ? Les métadonnées ont-elles été modifiées ? Un document de preuve distinct contenant les métadonnées doit-il accompagner le document ?

- **Sécurité**

  La solution de signature électronique garantit-elle la sécurité de l'information ?

  Vérifiez que la plateforme de signature électronique utilise un chiffrement fort des données en transit et inactives, en plus de stocker les données dans un volume de base de données chiffré pour assurer l'utilisation d'un canal chiffré pour toutes les communications.

Assurez-vous de consulter ce document au besoin, car nous l'actualiserons en fonction de l'évolution et du renforcement de notre politique de signature électronique d'entreprise.

Nous vous remercions de votre partenariat et de votre soutien continu.

Pour de plus amples renseignements, lisez l'article de blogue La liste de contrôle de sécurité E-Signature ultime.

22423 (2022-03)