Guide de la signature électronique dans le secteur juridique : "Les signatures électroniques peuvent-elles aussi convaincre les avocats, avocates et officiers publics suisses ?"

Dernière mise à jour : février 2023

En raison des exigences élevées des transactions juridiques électroniques et des processus compliqués concernant la clé USB, le lecteur de cartes & autres, de nombreux avocats suisses ont jusqu'à présent renoncé à la signature électronique et continuent de signer les documents à la main. Entre-temps, il existe toutefois des solutions légères permettant de signer des documents confidentiels de manière sûre et sans risque, conformément au droit suisse et européen. Lisez maintenant le guide complet pour répondre aux questions pertinentes et critiques dans le secteur juridique concernant la signature électronique.

Pourquoi devrais-je utiliser la signature électronique en tant qu'avocat(e) ?
Les avantages de la signature électronique sont évidents. Avec des solutions de signature numérique, comme eSignR, les professionnels du droit peuvent signer électroniquement, indépendamment du lieu, à moindre coût et de manière juridiquement contraignante. L'augmentation de l'efficacité grâce à des processus de signature rapides et confortables, associée à une transmission électronique sécurisée en faisant usage des plateformes de distribution reconnues, devrait être particulièrement intéressante pour les avocats ou les officiers publics qui facturent généralement leurs services à l'heure.

Les signatures électroniques sont-elles juridiquement contraignantes ?
Dans le domaine de la signature numérique, trois types de signatures sont souvent mentionnés - la signature électronique simple (EES), la signature électronique avancée (FES) et la signature électronique qualifiée (QES). En suisse, l'EES et la FES ne sont pas réglementées par la loi. Contrairement, la QES est assimilée à la signature manuscrite selon le droit suisse (SCSE) et le droit européen (eIDAS). Derrière la signature électronique qualifiée se cache une technique de sécurité élevée et un processus d'identification fiable définis, concernant le titulaire de la signature ou du certificat qualifié qui est joint à la signature technique.

Les documents signés électroniquement sont-ils reconnus par les autorités ?
Oui, si la personne qui signe utilise une solution de signature fiable, comme eSignR, en combinaison avec un service de signature officiellement reconnu pour créer une signature qualifiée. Les documents signés peuvent ainsi être déposés en ligne sans crainte. Toutefois, selon le service ou l'autorité, il se peut que le dépôt ne soit pas possible.

Les documents signés électroniquement sont-ils reconnus par les autorités ?
Oui, si la personne qui signe utilise une solution de signature fiable, comme eSignR, en combinaison avec un service de signature officiellement reconnu pour créer une signature qualifiée, les documents ainsi signés peuvent être déposés en ligne sans crainte. Selon le service ou l'autorité, il se peut toutefois que le dépôt se fasse via une plateforme de distribution cryptée officiellement reconnue, comme IncaMail de la Poste ou PrivaSphere.

Les signatures électroniques peuvent-elles être invalides ou non valides du point de vue de la qualité ?
La personne qui signe peut choisir un type de signature de qualité insuffisante, par exemple si l'EES ou le FES sont utilisés lors de l'apposition de la signature numérique, une erreur potentiellement catastrophique peut toutefois se produire rapidement. C'est pourquoi, contrairement à nos concurrents, nous proposons exclusivement le type de signature le plus élevé réglementé par la SCSE suisse, la QES (signature électronique qualifiée), avec toute la sécurité que cela implique, dans le cadre de la solution de signature eSignR.

Où la signature électronique qualifiée est-elle exigée ?
En principe, partout où la forme écrite est exigée dans le droit privé ou dans la mesure où une signature électronique qualifiée est exigée, par exemple dans le droit de procédure. Seule la signature électronique qualifiée est juridiquement équivalente à la signature manuscrite. Pour être sûr de ne pas se tromper, il est recommandé de miser dès le départ sur un certificat qualifié et sur une solution de signature qui ne supporte que la signature électronique qualifiée. Ainsi, vous signerez toujours au niveau de qualité le plus élevé.

Où sont stockés les documents signés numériquement ? Quels sont les risques des solutions basées sur le cloud ?
La plupart des solutions logicielles de signature électronique chargent les documents sur des instances en nuage, afin que plusieurs personnes puissent par exemple signer un PDF, l'une après l'autre lors d'une 'ronde de signature' numérique. Cela peut paraître séduisant, mais cela engendre pour conséquence l'accès à des données personnelles étant potentiellement sensibles, que vous donnez également à des tiers (les fournisseurs de cloud) résultant en la perte exclusive de vos données. Pour certains groupes professionnels, comme les avocats et les notaires, cela pose un problème relatant au secret professionnel ou d'avocat. Avec eSignR, la priorité absolue est la protection des données confidentielles. C'est pourquoi vos documents confidentiels ne quittent à aucun moment l'environnement de votre propre système au cours du processus de signature.

Existe-t-il des plates-formes de distribution électronique officiellement reconnues pour l'échange sécurisé de courriers électroniques ?
Oui, il existe des plateformes de distribution reconnues pour la transmission électronique dans le cadre des transactions juridiques électroniques. Vous trouverez des détails et une liste des plates-formes de distribution reconnues sur le site : https://www.bj.admin.ch/bj/de/home/staat/rechtsinformatik/e-uebermittlung.html

Quel est le degré de sécurité de la signature électronique par rapport à la signature manuscrite ?
Ceux qui ne se sont pas encore penchés sur la signature électronique assument qu'elle est moins sûre qu'une signature manuscrite. Pourtant, en regardant de plus près, une signature électronique qualifiée est bien plus sûre, tant sur le plan technique que sur celui de l'usurpation d'identité. Pour pouvoir signer électroniquement de manière qualifiée, il faut disposer d'un certificat de signature. Pour obtenir ce certificat de signature, le signataire doit être identifié personnellement et une seule fois par un fournisseur de services de confiance officiellement reconnu (par exemple Swisscom Trust Services) sur présentation de son passeport ou de sa carte d'identité. Une solution de signature sécurisée telle qu'eSignR est également nécessaire : eSignR utilise un procédé cryptographique asymétrique moderne et hautement sécurisé. Lors du processus de signature, l'identité de la personne signataire est en outre confirmée par une authentification à deux facteurs via, par exemple, le Mobile ID ou l'application Mobile ID de Swisscom.

Les documents signés électroniquement ou la propre signature peuvent-ils être piratés, dérobés ou utilisés abusivement ?
On pense souvent, à tort, que la signature électronique est une signature purement visuelle. Or, elle se compose d'une partie cryptographique sécurisée dans laquelle la valeur dite de hachage (empreinte digitale d'un document calculée de manière cryptographique) est enregistrée sous forme cryptée. La particularité est que la clé privée de cryptage n'est pas appliquée au document lui-même, mais à sa valeur de hachage. Les documents manipulés peuvent ainsi être reconnus sans aucun doute et même prouvés.

La signature électronique pourrait certes être copiée d'un document et insérée dans un autre, mais cela aurait pour conséquence d'invalider la signature et de l'empêcher d'être validée correctement. C'est pourquoi nous recommandons de toujours vérifier la validité des documents signés électroniquement que vous recevez. Pour les documents qui doivent être conformes au droit suisse, nous vous recommandons d'utiliser le validateur de signature gratuit de la Confédération suisse et, pour l'espace de l'UE, la vérification de signature de la société autrichienne Rundfunk und Telekom Regulierungs-GmbH. Dans le

monde, il y a malheureusement toujours le risque de tomber sur des agissements criminels, et cela vaut malheureusement aussi bien pour les processus électroniques qu'analogiques.

L'ensemble du processus de création de signatures numériques est-il conforme à la DSG/VDSG et au RGPD ?

Lors de la création de signatures électroniques qualifiées avec eSignR, toutes les exigences relatives à la protection des données personnelles sont respectées. Cela se fait dans le processus de signature par l'obtention de la déclaration de volonté et par l'authentification à deux facteurs. L'identité de la personne qui signe est garantie par un contrôle d'identité strict obligatoire, de sorte que le destinataire peut lui aussi se fier à 100% à l'origine de vos documents signés. Les données personnelles pour la gestion des abonnements, qui se trouvent sur le portail en ligne d'eSignR, sont également traitées conformément à la LPD/VDSG et au RGPD.

La signature électronique nécessite-t-elle du matériel supplémentaire ?

Il existe divers fournisseurs qui exigent une clé USB ou un lecteur de carte pour la signature électronique. Pour utiliser la solution de signature eSignR, il suffit d'avoir un téléphone portable ou un smartphone, qui n'est nécessaire que pour l'authentification à deux facteurs lors de chaque processus de signature.

Les signatures électroniques peuvent-elles être intégrées dans des systèmes de flux de travail existants ?

Il est possible de connecter la solution de signature eSignR à des solutions sectorielles existantes grâce à des APIs. L'équipe eSignR travaille actuellement sur des connexions avec des applications pertinentes. Nous serions heureux de recevoir votre feed-back sur les connexions logicielles potentielles, afin que vous puissiez encore mieux intégrer eSignR dans votre travail quotidien. L'intégration de la fonctionnalité Cygillum dans eSignR, qui permet de munir les copies électroniques d'actes notariés de la confirmation d'admission (le sceau réglementé) du registre des officiers publics directement dans le processus de signature d'eSignR, est intéressante pour les officiers publics.

Que disent les avocats à propos de la signature électronique ?

Le célèbre cabinet d'avocats d'affaires zurichois Blum&Grob, utilise principalement des signatures électroniques. L'article de David Schwaninger et Michelle Merz - avocats et partenaires chez Blum&Grob - a particulièrement retenu notre attention : *"La possibilité de faire signer des contrats de manière juridiquement valable par voie électronique facilite considérablement la conclusion de contrats dans le quotidien des affaires - surtout à l'époque du home office. Avant de pouvoir utiliser une telle signature électronique, il convient toutefois de vérifier si elle permet effectivement de conclure un contrat de manière juridiquement valable. En outre, il convient d'évaluer au cas par cas, le type de signature électronique doit être utilisée".*

Lisez maintenant l'article complet "la signature électronique" des deux experts du secteur pour plus d'informations. -> Lire l'article maintenant : https://blumgrob.ch/factsheet/die-elektronische-signatur/

Vous avez d'autres questions sur la signature électronique dans le domaine juridique ?

Prenez contact avec nous et laissez-vous conseiller par Igor Metz, CEO de Glue Software Engineering AG. Ayant déjà plus de 15 ans d'expérience dans le domaine du gouvernement suisse, il connaît parfaitement les défis de la numérisation dans le secteur juridique. -> https://esignr.ch/kontakt/

Vous imaginez-vous signer des documents électroniquement à l'avenir ?

Alors testez la solution de signature eSignR gratuitement et sans engagement pendant 30 jours.
-> Version d'essai : https://esignr.ch/download/