Guide to electronic signatures in the legal sector: *"Can electronic signatures also convince Swiss lawyers, attorneys and certifying officers?"*

Last update: February 2023

Due to the high requirements in electronic legal transactions and cumbersome processes with USB sticks and card readers, many Swiss lawyers have refrained from using electronic signatures and continue to hand-sign documents. In the meantime, however, there are lean solutions for signing confidential documents securely and risk-free under Swiss and EU law. Read the comprehensive guide now to answer relevant and critical questions in the legal industry regarding electronic signatures.

Why should I use electronic signatures as a lawyer?
The advantages of electronic signatures are obvious. With digital signature solutions such as eSignR, legal professionals can sign electronically, regardless of location, in a cost-saving and legally binding manner. Especially for lawyers or notary publics, who usually charge for their services on an hourly basis, an increase in efficiency through fast and convenient signature processes and secure electronic transmission via recognized delivery platforms should be particularly attractive.

Are electronic signatures legally binding?
In the field of digital signatures, there is mention of three categories of signatures - the simple (EES), the advanced (FES), and the qualified electronic signature (QES). The EES and FES are not regulated, while the regulation for the QES as per the law in Switzerland: referencing the Swiss law (ZertES) and EU law (eIDAS), which is equivalent to the handwritten signature. Behind the qualified electronic signature is a defined high level of technical security and a defined reliable identification process regarding the holder of the signature or the certified certificate attached to the technical signature.

Are electronically signed documents recognized by authorities?
Yes, if the person signing uses a reliable signature solution such as eSignR with an officially recognized signature service to create a qualified signature, documents signed this way can be submitted online without hesitation. Depending on the office or authority, however, the submission may have to be made via an officially recognized encrypted delivery platform such as Swiss Post's IncaMail or PrivaSphere.

Can electronic signatures be invalid or of poor quality?
The quality of electronic signatures is considered to be of poor-quality signature type if the signing entity opts for EES or FES, the potential for a catastrophic mistake but one that can happen quickly. For this reason, in contrast to our competitors, with the signature solution eSignR, we offer the highest signature regulated type by the Swiss ZertES, the qualified electronic signature (QES) with maximum security.

Where is the qualified electronic signature required?
Whenever the written form is required, as in private law, or wherever the requirement for a qualified electronic signature is in procedural law. Only the qualified electronic signature is legally equivalent to the hand signature. Therefore, it is advisable to use a qualified certificate and a signature solution that only supports qualified electronic signatures from the very beginning as an added measure. In taking this approach, you always sign at the highest quality level.

Where are digitally signed documents stored? What are the risks of cloud-based solutions?
Most e-signing software solutions load the documents onto cloud instances so that, for example, several people can sign a PDF in succession, known as a digital 'signing round.' Although it may sound tempting, the consequence is that you also grant third parties (the cloud providers) access to personal, potentially sensitive data, leading to the loss of sole sovereignty over your data. In addition, it can be problematic for certain professional groups, such as lawyers and notaries, because of the attorney-client privilege or professional

secrecy. With eSignR, the top priority is to protect confidential data. For this reason, your confidential documents never leave your system environment during the signature process.

Are there officially recognized electronic delivery platforms for secure e-mail traffic?
Yes, recognized delivery platforms are available for electronic transmission within the framework of electronic legal transactions. You may find further details comprising a list of recognized delivery platforms can be found at: https://www.bj.admin.ch/bj/de/home/staat/rechtsinformatik/e-uebermittlung.html.

How secure is the electronic signature compared to the handwritten signature?
Those who have yet to deal with electronic signatures may assume they are less secure than handwritten signatures. However, when looked at closely, a qualified electronic signature is much more secure technically and in terms of providing a false or fake identity. To be able to sign electronically at all, a signed certificate is required. After obtaining the signature certificate, the signatory must be personally identified once by an officially recognized trust service provider (e.g., Swisscom Trust Services) upon presentation of a passport or identity card. In addition, a secure signature solution, such as eSignR, is also required. eSignR uses a modern, highly secure asymmetric cryptographic procedure. During the signature process, the identity of the person signing is also confirmed utilizing two-factor authentication via, for example, the Mobile ID or the Mobile ID app from Swisscom.

Can electronically-signed documents or personal signatures be hacked, stolen, or misused?

It is often mistakenly assumed that the electronic signature consists of a purely visual signature. However, it consists of a secure cryptographic part in which the so-called hash value (cryptographically calculated fingerprint of a document) is stored in encrypted form. The special feature is that the private key for encryption is not applied to the document itself but to its hash value. Manipulated documents can thus be detected beyond doubt and also proven.

The electronic signature could be copied from one document and pasted into another, but this would result in the signature becoming invalid and could no longer be validated correctly. For this reason, we recommend always checking the validity of electronically signed documents received. For documents that must comply with Swiss law, we recommend using the free signature validator of the Swiss Confederation and, for the EU area, the signature validator of the Austrian Rundfunk und Telekom Regulierungs-GmbH. In the world, unfortunately, there is always the danger of encountering criminal machinations, which applies to electronic as well as analog processes.

Is the entire process for creating digital signatures DSG/VDSG and DSGVO compliant?
When creating qualified electronic signatures with eSignR, all requirements regarding the protection of personal data are met and carried out in the signature process by obtaining the declaration of intent and through two-factor authentication. Furthermore, the identity of the person signing is secured by the obligatory strict identity check so that the recipient can also rely 100% on the origin of your signed documents. The personal data for subscription management, located on the eSignR online portal, is also handled in compliance with the DSG/VDSG and DSGVO.

Do I need additional hardware for the electronic signature?
Various providers require a USB stick or a card reader for the electronic signature. However, to use the eSignR signature solution, you only need your mobile phone or smartphone for each signature process, required only for two-factor authentication (2FA).

Can electronic signatures be integrated into existing workflow systems?
Connecting the eSignR signature solution to existing industry solutions through APIs is possible. The eSignR team is currently working on connections to relevant applications. We look forward to your feedback on potential software connections at any time so that you can integrate eSignR even better into your everyday work. Of interest to notaries is the integration of the Cygillum functionality into eSignR, which allows electronic copies of notarial deeds to be provided with the confirmation of approval (the regulated seal) of the register of notaries directly in the signature process of eSignR.

What do lawyers say about electronic signatures?

The renowned Zurich business law firm Blum&Grob predominantly uses electronic signatures. We were particularly struck by the article by David Schwaninger and Michelle Merz - lawyers and partners at Blum&Grob: *"The possibility of having contracts legally signed electronically makes it significantly easier to conclude contracts in everyday business - especially in times of home offices. However, before such an electronic signature can be used, it must be checked in each case whether a contract can actually be legally concluded with it. In addition, it must be weighed up in each individual case which type of electronic signature should be used."*

Now read the article "the electronic signature" by the two industry experts for more information. -> Read the article now: https://blumgrob.ch/factsheet/die-elektronische-signatur/

Do you have further questions about electronic signatures in the legal sector?

Contact us and let Igor Metz, CEO of Glue Software Engineering AG, advise you. He already has over 15 years of experience in the Swiss government and is very familiar with the challenges of digitalization in the legal sector.
https://esignr.ch/en/contact/

Can you imagine signing documents electronically in the future?

Then try out the signature solution eSignR for 30 days free of charge and without obligation.
-> Test version: https://esignr.ch/download/