

# Ratgeber für die elektronische Unterschrift in der Rechtsbranche: «Können elektronische Signaturen auch Schweizer Anwälte, Anwältinnen und Urkundspersonen überzeugen?»

Letzter Stand: Februar 2023

**Aufgrund der hohen Anforderungen im elektronischen Rechtsverkehr und umständlichen Prozessen mit USB-Stick, Card-Reader & Co verzichten bisher viele Schweizer Anwälte auf die elektronische Unterschrift und unterschreiben Dokumente weiterhin von Hand. Mittlerweile gibt es jedoch schlanke Lösungen, um vertrauliche Dokumente sicher und risikofrei gemäss CH und EU-Recht zu signieren. Lesen Sie jetzt den umfassenden Ratgeber, um relevante und kritische Fragestellungen in der Rechtsbranche bezüglich der elektronischen Unterschrift zu beantworten.**

## **Wieso soll ich als Anwalt/Anwältin die elektronische Unterschrift nutzen?**

Die Vorteile der elektronischen Unterschrift liegen auf der Hand. Mit digitalen Signaturlösungen wie eSignR können Rechtsexperten standortunabhängig, kostensparend und rechtlich bindend elektronisch signieren. Speziell bei Anwälten und Anwältinnen oder Urkundspersonen, welche Ihre Dienste meist auf Stundenbasis berechnen, sollte eine Steigerung der Effizienz durch schnelle und komfortable Unterschriftsprozesse zusammen mit einer sicheren elektronischen Übermittlung via anerkannte Zustellplattformen besonders attraktiv sein.

## **Sind elektronische Unterschriften rechtlich bindend?**

Im Bereich der digitalen Signatur werden häufig drei Typen von Signaturen genannt – die einfache (EES), die fortgeschrittene (FES) und die qualifizierte elektronische Signatur (QES). Die EES und FES sind im Schweizer Gesetz nicht geregelt. Nur die QES wird in der Schweiz durch das Gesetz geregelt: diese ist gemäss schweizerischem Recht (ZertES) und EU-Recht (eIDAS) der handschriftlichen Unterschrift gleichgestellt. Hinter der qualifizierten elektronischen Unterschrift steht eine definierte hohe technische Sicherheit und ein definierter zuverlässiger Identifikationsprozess bezüglich des Inhabers der Unterschrift bzw. des qualifizierten Zertifikats, das der technischen Signatur beigelegt wird.

## **Werden elektronisch signierte Dokumente von Behörden anerkannt?**

Ja, wenn die unterzeichnende Person eine zuverlässige Signaturlösung wie eSignR zusammen mit einem offiziell anerkannten Signatur-Service zur Erstellung einer qualifizierten Signatur verwendet, können die so signierten Dokumente bedenkenlos online eingereicht werden. Je nach Stelle oder Behörde kann es jedoch sein, dass die Einreichung via eine offiziell anerkannte verschlüsselte Zustellplattform wie beispielsweise IncaMail der Post oder PrivaSphere erfolgen muss.

## **Können elektronische Unterschriften ungültig bzw. von ihrer Qualität her ungültig sein?**

Die unterzeichnende Person kann einen qualitativ ungenügenden Signaturtyp auswählen, beispielsweise wenn beim Anbringen der digitalen Signatur die EES oder FES verwendet wird, ein potenziell katastrophaler Fehler, der jedoch schnell passieren kann. Aus diesem Grund bieten wir bei der Signaturlösung eSignR im Gegensatz zu unserer Konkurrenz ausschliesslich den höchsten, vom schweizerischen ZertES geregelten Signaturtyp, die QES, die qualifizierte elektronische Signatur) mit der ganzen dahinterstehenden Sicherheit an.

## **Wo wird die qualifizierte elektronische Signatur gefordert?**

Grundsätzlich überall, wo im Privatrecht die schriftliche Form, oder wo beispielsweise im Prozessrecht eine qualifizierte elektronische Unterschrift gefordert wird. Nur die qualifiziertere elektronische Signatur ist rechtlich der Handunterschrift gleichgestellt. Um auf der sicheren Seite zu sein, empfiehlt es sich, von Anfang an auf ein qualifiziertes Zertifikat und auf eine Signaturlösung zu setzen, welche nur die qualifizierte elektronische Signatur unterstützt. So signieren Sie immer auf der höchsten Qualitätsstufe.

### **Wo werden digital signierte Dokumente gespeichert? Was sind die Risiken von cloudbasierten Lösungen?**

Die meisten Software-Lösungen für das elektronische Signieren laden die Dokumente auf Cloud-Instanzen, damit beispielsweise mehrere Personen ein PDF in einer digitalen 'Signierrunde' nacheinander unterschreiben können. Dies mag verlockend klingen, jedoch hat dies zur Folge, dass Sie so auch Dritten (den Cloud-Anbietern) Zugriff auf persönliche, potenziell sensible Daten gewähren und Sie somit die alleinige Hoheit über Ihre Daten verlieren. Für bestimmte Berufsgruppen, wie beispielsweise bei Anwalts- und Notariatspersonen, ist dies wegen des Anwaltsgeheimnisses, oder des Berufsgeheimnisses problematisch. Beim eSignR ist die oberste Priorität der Schutz von vertraulichen Daten. Aus diesem Grund verlassen Ihre vertraulichen Dokumente im Signatur-Prozess zu keinem Zeitpunkt Ihre eigene System-Umgebung.

### **Gibt es offiziell anerkannte elektronische Zustellplattformen für den sicheren E-Mail-Verkehr?**

Ja, für die elektronische Übermittlung im Rahmen des elektronischen Rechtsverkehrs stehen anerkannte Zustellplattformen zur Verfügung. Detail und eine Liste der anerkannten Zustellplattformen finden Sie unter: <https://www.bj.admin.ch/bj/de/home/staat/rechtsinformatik/e-uebermittlung.html>

### **Wie sicher ist die elektronische Unterschrift im Vergleich zur handschriftlichen Unterschrift?**

Wer sich noch nicht mit der elektronischen Signatur befasst hat, nimmt vielleicht an, dass diese weniger sicher als eine handschriftliche Signatur ist. Genau betrachtet ist eine qualifizierte elektronische Unterschrift jedoch wesentlich sicherer sowohl technisch als auch hinsichtlich der Vortäuschung einer falschen Identität. Um überhaupt qualifiziert elektronisch signieren zu können, wird ein Signatur-Zertifikat vorausgesetzt. Um dieses Signatur-Zertifikat zu erhalten, muss der Signierende von einem offiziell anerkannten Vertrauensdiensteanbieter (beispielsweise Swisscom Trust Services) einmalig persönlich gegen Vorweisung von Pass oder Identitätskarte identifiziert werden. Weiter ist eine sichere Signaturlösung wie eSignR notwendig: eSignR verwendet ein modernes hochsicheres asymmetrisches kryptografisches Verfahren. Beim Signaturvorgang wird zusätzlich die Identität der signierenden Person mittels Zwei-Faktor-Authentifizierung via beispielsweise die Mobile ID oder die Mobile ID App der Swisscom bestätigt.

### **Können elektronisch signierte Dokumente oder die eigene Unterschrift gehackt, entwendet oder missbraucht werden?**

Irrtümlicherweise wird oft angenommen, dass die elektronische Unterschrift aus einer rein visuellen Signatur besteht. Sie besteht jedoch aus einem sicheren kryptographischen Teil, in dem der sogenannte Hash-Wert (kryptografisch errechneter Fingerabdruck eines Dokumentes) verschlüsselt gespeichert wird. Die Besonderheit ist, dass der private Schlüssel zur Verschlüsselung nicht auf das Dokument selbst, sondern auf dessen Hash-Wert angewendet wird. Manipulierte Dokumente können so zweifelsfrei erkannt und auch nachgewiesen werden.

Die elektronische Signatur könnte zwar aus einem Dokument kopiert und in ein anderes eingefügt werden, was aber zur Folge hätte, dass die Signatur damit ungültig wird und nicht mehr korrekt validiert werden kann. Aus diesem Grund empfehlen wir, erhaltene elektronisch signierte Dokumente immer auf ihre Gültigkeit zu prüfen. Für Dokumente, die dem schweizerischen Recht entsprechen müssen, empfehlen wir Ihnen, den kostenlosen Signaturvalidator der Schweizerischen Eidgenossenschaft und für den EU-Raum die Signaturprüfung der österreichischen Rundfunk und Telekom Regulierungs-GmbH zu nutzen. In der Welt besteht leider immer die Gefahr auf kriminelle Machenschaften zu stossen, dies gilt leider für elektronische sowie analoge Prozesse.

### **Ist der gesamte Prozess beim Erstellen von digitalen Unterschriften DSG/VDSG und DSGVO-konform?**

Beim Erstellen von qualifizierten elektronischen Signaturen mit eSignR werden sämtliche Anforderungen, welche den Schutz von personenbezogenen Daten beinhaltet, eingehalten. Dies geschieht im Signatur-Prozess über die Einholung der Willensbekundung und durch die Zwei-Faktor-Authentifizierung. Die Identität der signierenden Person ist durch die obligatorische strenge Identitätsprüfung gesichert, so dass sich auch der Empfänger auf die Herkunft Ihrer signierten Dokumente zu 100% verlassen kann. Auch die Personendaten für das *Abonnement-Management*, welche sich auf dem Online-Portal von eSignR befinden, werden konform zu DSG/VDSG und DSGVO behandelt.

### **Braucht es für die elektronische Unterschrift zusätzliche Hardware?**

Es gibt diverse Anbieter, welche einen USB-Stick oder ein Kartenlesegerät für die elektronische Signatur voraussetzen. Um die Signaturlösung eSignR zu nutzen, genügt Ihr Handy oder Smartphone, welches lediglich für die Zwei-Faktor-Authentifizierung bei jedem Signatur-Prozess benötigt wird.

### **Können elektronische Unterschriften in bestehende Workflow-Systeme integriert werden?**

Es gibt die Möglichkeit durch APIs die Signaturlösung eSignR an bestehende Branchenlösungen anzuschliessen. Das eSignR-Team arbeitet zurzeit an Anbindungen zu relevanten Applikationen. Wir freuen uns jederzeit auf Ihr Feedback zu potenziellen Software-Anbindungen, damit Sie eSignR noch besser in Ihren Arbeitsalltag integrieren können. Für Urkundspersonen interessant ist die bereits erfolgte Integration der Cygillum-Funktionalität in eSignR, die es erlaubt elektronische Ausfertigungen notarieller Urkunden direkt im Signatur-Prozess von eSignR mit der Zulassungsbestätigung (dem geregelten Siegel) des Urkundspersonenregisters zu versehen.

### **Was sagen Rechtsanwälte zur elektronischen Unterschrift?**

Die renommierte Zürcher Wirtschaftskanzlei Blum&Grob, verwendet vorwiegend elektronische Unterschriften. Besonders der Artikel von David Schwaninger und Michelle Merz – Rechtsanwälte und Partner bei Blum&Grob ist uns aufgefallen: *«Die Möglichkeit, Verträge auch elektronisch rechtsgültig unterzeichnen zu lassen, erleichtert im Geschäftsalltag – v.a. in Zeiten des Homeoffice – den Abschluss von Verträgen massgeblich. Bevor eine solche elektronische Unterschrift jedoch eingesetzt werden kann, ist jeweils zu prüfen, ob damit ein Vertrag auch tatsächlich rechtsgültig abgeschlossen werden kann. Zudem ist im Einzelfall abzuwägen, welche Art der elektronischen Unterschrift eingesetzt werden soll.»*

Lesen Sie jetzt den gesamten Artikel **«die elektronische Signatur»** der beiden Branchenexperten für mehr Informationen. -> Jetzt Artikel lesen: <https://blumgrob.ch/factsheet/die-elektronische-signatur/>

**Haben Sie weitere Fragen zur elektronischen Unterschrift im Rechtsbereich?** Nehmen Sie mit uns Kontakt auf und lassen Sie sich von Igor Metz, CEO Glue Software Engineering AG, beraten. Er hat bereits über 15 Jahre Erfahrung im Bereich Schweizer Government und ist mit den Herausforderungen der Digitalisierung in der Rechtsbranche bestens vertraut. -> <https://esignr.ch/kontakt/>

### **Können Sie sich vorstellen in Zukunft Dokumente elektronisch zu signieren?**

Dann testen Sie die Signaturlösung eSignR für 30 Tage kostenlos und unverbindlich aus. -> [Testversion](https://esignr.ch/download/): <https://esignr.ch/download/>