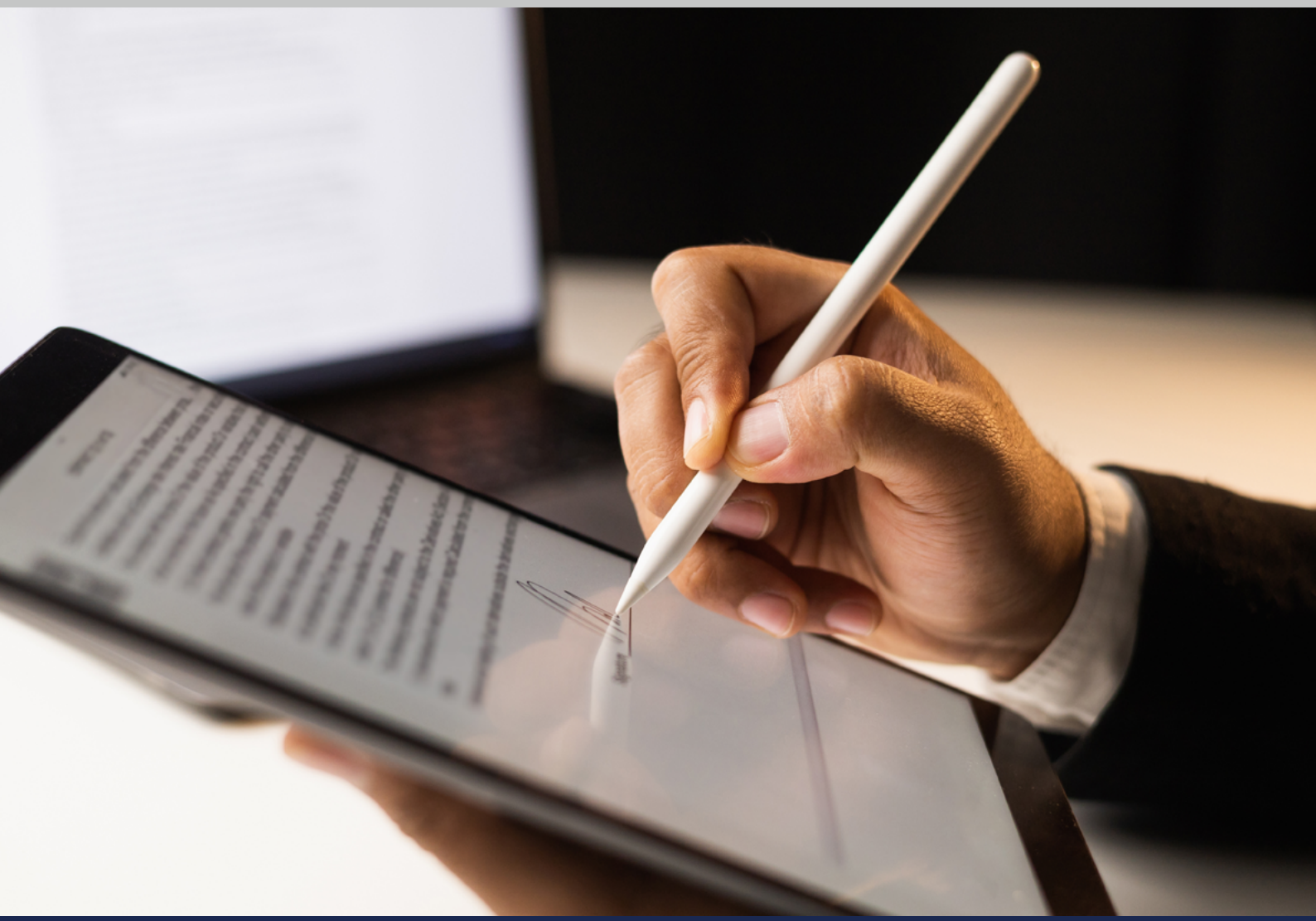
FORUM



Elektronische Signaturen

präsentiert von MORGENSTERN

MORGENSTERN

Whitepaper

Elektronische Signaturen

Inhalt

Wir bei MORGENSTERN legen großen Wert auf inklusive Sprache. Deswegen gendern wir – und zwar gerne! Du sollst dich von unseren Texten angesprochen fühlen, egal wer du bist.

Fachbegriffe gendern wir jedoch nicht, da sie wie Eigennamen feststehende Begriffe sind. Hier geht es nicht um das generische Maskulinum, sondern um fachliches Vokabular, das seine eigene juristische Bedeutung hat.

...dir aber nun **viel Spaß**, liebe*r Leser*in!

01. Einführung

Was versteht man unter einer elektronischen Signatur?

Unter einer elektronischen Signatur versteht man Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen. Da diese Prozedur als ein Ersatz der eigenhändigen Unterschrift beim Abschluss von Verträgen anzusehen ist, wird durch den Einsatz elektronischer Signaturen somit der Verzicht auf Dokumente in Papierform ermöglicht.

Dabei fällt immer wieder auch der Begriff „digitale Signatur". Allerdings gibt es aus rechtlicher Sicht keinen Unterschied. Digitale Signatur ist ein technischer bzw. mathematischer Begriff. Die korrekte juristische Bezeichnung lautet „elektronische Signatur".

Brauchst du Rat? Kontaktiere uns! Wir bei MORGENSTERN haben ein erfahrenes und hoch spezialisiertes Team bestehend aus Anwälten, Datenschutz- und IT-Sicherheitsexperten!

contact@morgenstern-legal.com
+49 (0) 6232 - 100119 0

Mehr MORGENSTERN Whitepaper findest du übrigens auch unter:
morgenstern-privacy.com & morgenstern-legal.com

02. Welche Art von elektronischen Signaturen gibt es?

Unterschieden wird zwischen der einfachen elektronischen Signatur (EES), der fortgeschrittenen elektronischen Signatur (FES) und der qualifizierten elektronischen Signatur (QES).

Die **einfache elektronische Signatur (EES)** muss keine Möglichkeit der Identifizierung beinhalten oder eine Veränderung des Dokuments erkennen lassen. Diese Form der Signatur ist sehr einfach und schnell zu leisten, jedoch schlecht beweisbar. Somit kommt auch keine IT-Anwendung zur Fälschungssicherung in Frage. Hierbei handelt es sich einfach um Daten, die in elektronischer Form anderen elektronischen Daten beigefügt werden. Diese werden zum Unterschreiben verwendet. Beispiele für die einfache elektronische Signatur sind z. B. digitalisierte Unterschriften (etwa per Adobe Acrobat DC Signaturfunktion), E-Mail-Signaturen mit Grußformel oder auch Touchscreen-Signaturen.

Die **fortgeschrittene elektronische Signatur (FES)** wird in der Praxis häufig angewandt, da sie beweiskräftig ist und einfach, schnell und unkompliziert geleistet werden kann. Bei Beweisführung ist sie wesentlich aussagekräftiger als die einfache elektronische Signatur, da dem unterzeichneten Dokument ein einmaliger Signaturschlüssel beigefügt wird, mit dem der Unterzeichner eindeutig zu identifizieren ist. Eine IT-Anwendung ist somit möglich hinsichtlich der eindeutigen Zuordnung, der Identifizierung des Unterzeichners, der Kontrolle durch den Unterzeichner sowie der Verknüpfung mit Daten, um nachträgliche Veränderungen dieser erkennen zu lassen. Allerdings bietet auch diese Form der elektronischen Signatur keine vollständige Sicherheit, da das Passwortmanagement in der Hand des Unterzeichners liegt.

Die **qualifizierte elektronische Signatur (QES)** bietet die höchsten rechtsgeschäftlichen, beweisrechtlichen und technischen Standards. Und das ist auch zwingend notwendig, schließlich gewährt diese Form der elektronischen Signatur die gleiche Rechtswirkung wie eine eigenhändige Unterschrift (vgl. Art. 25 Abs. 2 eIDAS-VO). Bei der QES muss deshalb die Identität der Person vor der Unterschrift geprüft werden. Die Identifizierung kann nach den zurzeit gültigen Standards beispielsweise durch das Post-Ident-Verfahren oder das Video-Ident-Verfahren erfolgen. Danach stellt ein zertifiziertes Trust Center ein elektronisches Zertifikat aus, welches den Namen des Unterzeichners trägt. Damit kann der Unterschreiber anschließend (einmalig oder mehrfach, je nach Zertifikatstyp) qualifizierte Signaturen auslösen. Aufgrund dieser zusätzlichen Sicherheitsstufe ist ein Dokument, das mit einer QES signiert wurde, in allen EU-Mitgliedstaaten ebenso rechtlich bindend wie ein Dokument mit handschriftlicher Signatur.

Auch gibt es Fälle, bei denen die qualifizierte elektronische Signatur die einzige zulässige Art der digitalen Signatur für bestimmte Vertragsarten darstellt. Gemäß § 39 a Abs. 1 S. 2 BeurkG etwa muss die elektronische notarielle Urkunde eine qualifizierte elektronische Signatur tragen. Ebenfalls erwähnenswert sind in diesem Zusammenhang beispielsweise der Verbraucherdarlehensvertrag (§ 492 Abs. 1 S. 1 BGB) und der Arbeitnehmerüberlassungsvertrag (§ 12 Abs. 1 S. 1 AÜG), deren Abschluss grundsätzlich eigenhändig durch Namensunterschrift (schriftlich i.S.v. § 126 BGB) zu erfolgen hat und ausnahmsweise durch eine elektronische Form ersetzt werden darf, wenn es sich hierbei gemäß §§ 126 Abs. 3 i.V.m. 126 a Abs. 1 BGB um eine qualifizierte elektronische Signatur handelt.

Bedingt durch die erhöhte Sicherheitsstufe geht mit der Nutzung der QES, verglichen mit den anderen elektronischen Signaturen, allerdings auch ein höherer Aufwand bei der Anwendung und ein größerer Kostenaufwand einher. Außerdem existiert bislang lediglich ein nur sehr geringes Angebot hinsichtlich einer flächendeckenden Anwendung des QES.

03. Zielsetzung und Herausforderungen

Da die primäre Zielsetzung im Rahmen der elektronischen Signaturen die digitale Transformation der Kernprozesse darstellt, müssen diverse Herausforderungen in Angriff genommen werden.

Ein Kernprozess für viele Unternehmen ist das Handling von Verträgen, das aus einem scheinbaren Mangel an gangbaren Alternativen oft weiter analog stattfindet – und mit massiven Aufwänden verbunden ist. Dabei hat die digitale Transformation der Kernprozesse ein enormes Potenzial für Zeitersparnisse, Kostensenkung, Nachhaltigkeit und Qualitätsverbesserung, sofern es richtig und rechtskonform umgesetzt wird. Hiermit sind diverse Herausforderungen verbunden.

Die **Wahl der Infrastruktur** ist eine davon. Hier besteht zum einen die Möglichkeit des Einsatzes einer on-premise-Lösung (lokale Server), und zum anderen die einer Cloud-Lösung. Bei der on-premise-Lösung findet die Verwaltung bzw. die Wartung auf internen IT-Systemen statt. Das impliziert viel Hardwaremanagement, da interne Hardware in aller Regel ein Leistungslimit aufweist. Auch ist die Fehleranfälligkeit in der Regel höher, da bei internem Fehler die Dienstverfügbarkeit unter Umständen lange ausfallen kann. Das Risiko von Hardwareausfällen trägt dabei auch alleine der Betreiber. Außerdem ist die lokale Anschaffung oft mit sehr hohen Kosten verbunden. Dafür bietet die on-premise-Lösung bei idealer Umsetzung schließlich viel Transparenz und auch Sicherheit.

Bei der **Cloud-Lösung** wiederum geht die IT-Verwaltung extern vonstatten. Im Gegensatz zur on-premise-Lösung kann hier die Rechenleistung beliebig dazu- oder abgebucht werden. Das heißt, sie ist skalierbar und flexibel, ohne einen hohen Kostenaufwand zu Beginn der Nutzung. Außerdem wird hier eine in der Regel bessere Verfügbarkeit der Dienste und Backup-Lösungen sichergestellt als in der lokalen Lösung, weshalb Risiken von Hardwareausfällen faktisch geringer sind. Nicht zuletzt bieten bei technischen Problemen Experten Support, da der Cloud-Provider in aller Regel eine Expertise für seine Hauptdienstleistung hat. Auch hinsichtlich der Anschaffungskosten ist die Nutzung einer Cloud-Lösung planbarer. Da viele Cloud-Dienstleister allerdings ihren Sitz im Ausland haben, steigt hierbei auch die Gefahr einer Übermittlung personenbezogener Daten in unsichere Drittländer. Egal, welche Variante nun bevorzugt wird: Die Wahl muss in die Gesamtcloudstrategie bzw. die Infrastrukturstrategie des Unternehmens passen, stellt sie doch eine gewichtige Unternehmensentscheidung für alle Geschäftsbereiche dar.

Eine weitere Herausforderung im Zuge der digitalen Transformation der Kernprozesse stellt das **Etablieren eines internen Workflows** dar. Hier ist auf den richtigen Umgang mit elektronischen Signaturen zu achten, und zwar ab dem Moment, in dem dem Unterzeichner das jeweilige Dokument präsentiert wird. Grob kann man diesen Workflow in die folgenden Überlegungen gliedern: In einem ersten Schritt wird das zu signierende Dokument identifiziert. Hier muss bereits die Frage gestellt werden, ob elektronische Signaturen überhaupt zulässig oder potenziell sogar gemäß §§ 128, 129 BGB beschränkt sind. Im Anschluss ist dann darüber nachzudenken, welche Art der elektronischen Signatur angewandt werden soll. Falls ein gesetzliches Schriftformerfordernis einschlägig ist, muss mit der qualifizierten elektronischen Signatur unterzeichnet werden. Ansonsten muss geprüft werden, ob die fortgeschrittene oder sogar die einfache elektronische Signatur angewandt werden kann. Sobald schließlich alle Dokumente signiert wurden, sollten sichere elektronische Kopien zum Herunterladen angeboten oder alternativ sicher gedruckte Kopien per Post versendet werden. Außerdem sollten die Dokumente in einer sicheren (Cloud-)Umgebung abgelegt werden. Hier sollten außerdem auch die internen Richtlinien zur Aufbewahrung von Dokumenten berücksichtigt werden. Es wird empfohlen, elektronisch signierte Datensätze gemäß Datenaufbewahrungsrichtlinie zu speichern und zu verwalten.

> **Tipp:** Der unternehmensinterne Umgang mit elektronischen Signaturen sollte in einer Richtlinie festgehalten werden.

MORGENSTERN
Microsoft 365 - Einführung

Bei der Einführung von Microsoft 365 sind vielfältige Faktoren zu beachten:
IT-Recht, Datenschutz(recht) und Arbeitsrecht sowie IT-Sicherheitsaspekte müssen sorgfältig berücksichtigt werden.

MORGENSTERN bietet einen One-Stop-Shopping-Ansatz.

Legal Review	Security Check Up
über MORGENSTERN Rechtsanwaltsgesellschaft mbH	über MORGENSTERN consecom GmbH

Special für KRITIS Unternehmen

Individuelle Beratung erforderlich?
Dann schreib uns einfach an: contact@morgenstern-privacy.com

Hier gehts zum Whitepaper:
Rechtssicherer Umgang mit Microsoft 365

Da elektronische Signaturen auch aus Sicht des Datenschutzes interessant sind, müssen als eine weitere Herausforderung schließlich die **datenschutzrechtlichen Erwägungen** berücksichtigt werden. Diese variieren sogar je nach Art der Signatur.

Bei der einfachen elektronischen Signatur ist der Verwender der datenschutzrechtlich Verantwortliche i.S.d. Art. 4 Nr. 7 DS-GVO. Die Verantwortung des Verantwortlichen umfasst die Einhaltung der Vorschriften der DS-GVO, das Festlegen geeigneter Schutzmaßnahmen sowie den Nachweis dafür. Das heißt, der Verwender ist in der Beweispflicht. Als Rechtsgrundlage dient hier primär Art. 6 Abs. 1 b) DS-GVO (vertragliche Maßnahme).

Bei der fortgeschrittenen elektronischen Signatur bleibt der Verwender Verantwortlicher. Allerdings ist der Diensteanbieter hier als Auftragsverarbeiter anzusehen. Das hat zur Folge, dass mit ihm ein Vertrag zur Auftragsverarbeitung (AV-Vertrag) gemäß Art. 28 DS-GVO abgeschlossen werden muss.

Bei der qualifizierten elektronischen Signatur indes ist der Diensteanbieter selbst Verantwortlicher. Das ergibt sich aus den gesetzlichen Pflichten des Art. 24 Abs. 2 eIDAS-VO. Der Verwender bleibt allerdings ebenfalls verantwortlich. Das hat zur Folge, dass eine sogenannte „Gemeinsame Verantwortlichkeit" vorliegt und infolgedessen eine Vereinbarung nach Art. 26 DS-GVO geschlossen werden muss.

Unabhängig davon, welche elektronische Signatur eingesetzt werden soll, besteht grundsätzlich immer Handlungsbedarf hinsichtlich der folgenden Punkte:

- Die betroffenen Personen müssen gemäß Art. 13 DS-GVO über die stattfindende Datenverarbeitung informiert werden (Pflichtinformationen)
- Das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO ist entsprechend zu pflegen
- Für einen effektiven Workflow müssen die Mitarbeiter*innen im Rahmen von regelmäßigen Schulungen entsprechend sensibilisiert werden. Dies dient auch dem Nachweis der Rechenschaftspflicht des/ der Verantwortlichen gemäß Art. 5 Abs. 2 DS-GVO
- Auf ein entsprechendes Vertragsmanagement mit dem Diensteanbieter ist zu achten

Worauf ist bei der **Markterkundung und Anbieterauswahl** zu achten?

Grundsätzlich sind Anbieter, die keine qualifizierten elektronischen Signaturen anbieten, nicht zu empfehlen. Das hat den Hintergrund, dass Diensteanbieter von qualifizierten elektronischen Signaturen mindestens alle 24 Monate von der Bundesnetzagentur kontrolliert werden und entsprechend zukunftssicher sind. Allerdings reicht für normale „Alltagsgeschäfte" die Nutzung einer einfachen elektronischen Signatur in aller Regel auch aus. Problematisch ist nach wie vor die Drittstaatenübermittlung, weshalb der Diensteanbieter bestenfalls in der EU sitzen sollte und nicht in einem unsicheren Drittstaat (wie etwa den USA). Potenziell ist auch auf die Bereitstellung individueller Schnittstellen zu achten. Wenn individuelle Schnittstellen verfügbar sind, kann bei Veränderung des Workflows (z.B. bei dem Einsatz neuer Software) nämlich besser intern auf die neue Begebenheit umgestellt werden. Empfehlenswert sind die nachfolgend aufgeführten Anbieter, da diese die oben genannten Kriterien bereits alle erfüllen. Wichtig: Diese Liste erhebt keinen Anspruch auf eine vollständige Erfassung des Marktes.

- Intarsys GmbH
  - Stapelsignaturen (mit einem Vorgang werden alle abgelegten Dokumente signiert)
  - On-premise und Cloud-Lösungen

- Skribble AG
  - Umfangreicher Schnittstellenkatalog verfügbar
  - Mehrere Prozesse für fortgeschrittene elektronische Signaturen verfügbar

- FP Digital Business Solutions GmbH (FP Sign)
  - Kapazität für großen Bedarf
  - Erfahrung mit Kund*innen aus Energiewirtschaft

- d.velop AG
  - Umfangreicher Schnittstellenkatalog verfügbar
  - Webseiteneintrag speziell für Versorgungsindustrie

- iS2 Intelligent Solution Services AG (inSign)
  - Erfahrung mit Kund*innen aus Energiewirtschaft
  - Identifizierungssystem für Touchscreen-Signaturen („Biometrische Unterschriftendaten“)
    -> Programm erkennt Schreibgeschwindigkeit, Druck, Pausen und erkennt so Fälschung durch andere Person

- Yousign SAS
  - Preis-Leistungs-Verhältnis (nach erstem Eindruck)
  - Fokus auf Anwenderfreundlichkeit

MORGENSTERN

Einführung und Betrieb eines ...

... Hinweisgebersystems

Hinweisgeber-Compliance-Paket

morgenstern-privacy.com

» Jetzt Angebot anfordern

Datenschutz-Paket I

Datenschutz-Paket II

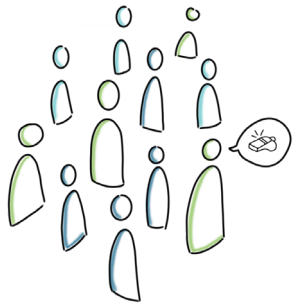
Mitbestimmungspaket

Optional

Betroffenenanfragenpaket

morgenstern-legal.com

» Jetzt Angebot anfordern



the future is yours.

MORGENSTERN Rechtsanwaltsgesellschaft mbH
Große Himmelsgasse 1
DE - 67346 Speyer

Telefon
+49 (0) 6232 - 100119 0

E-Mail
contact@morgenstern-legal.com

Passende Weiterbildungen finden Sie hier:

Weiterbildung zum Thema Recht

Finden Sie aus unserem breiten, erstklassigen Weiterbildungsangebot die für Ihre Bedürfnisse passende Fortbildung. Profitieren Sie von unseren maßgeschneiderten Seminaren und Lehrgängen mit erfahrenen, hochkarätigen Experten rund um das Thema Recht. Jetzt informieren.

e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen.
Jetzt testen.

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als Inhouse-Training.
Jetzt individuelles Angebot anfordern.

Dieses Whitepaper wurde Ihnen von unserem Content-Partner präsentiert.
sichern Sie sich jetzt eine individuelle und zielgenaue Beratung.

MORGENSTERN legal | Dein Partner in Sachen IT-Recht & Digitalisierung
morgenstern-legal.com

MORGENSTERN privacy | Dein Partner in Sachen Datenschutz & IT-Sicherheit
morgenstern-privacy.com

FORUM · Institut für Management GmbH · Postfach 10 50 60 · 69040 Heidelberg · Germany
Tel. +49 6221 500-500 · Fax +49 6221 500-555 · www.forum-institut.de