Adobe Sign

Grundlagen für Erfolg mit elektronischen Signaturen.

Entwicklung einer effektiven Richtlinie für elektronische Signaturen.

Elektronische Signaturen verändern Geschäftsabläufe grundlegend. Sie machen die umständliche Handhabung gedruckter Schriftstücke überflüssig und beschleunigen zudem Genehmigungs- und Unterzeichnungsprozesse. Die Einbindung elektronischer Signaturen in eure bestehenden Workflows ist einfacher, als ihr vielleicht denkt. Als sinnvollen ersten Schritt solltet ihr eine generelle Richtlinie für elektronische Signaturen festlegen.

Eine solche Richtlinie regelt den Einsatz von elektronischen Signaturen gemäß regionalen und internationalen Gesetzen und Vorschriften. Zunächst müsst ihr festlegen, was in die Richtlinie aufgenommen werden soll.

Dieser Leitfaden bietet einige Vorschläge, auf deren Grundlage ihr eine für euer Unternehmen geeignete Richtlinie für elektronische Signaturen erstellen könnt. Die folgenden Anregungen helfen euch dabei, sicherzustellen, dass eure elektronischen Verträge rechtsgültig und durchsetzbar sind.

Die Gesetzeslage kennen.

Elektronische Unterschriften sind in fast allen Industrieländern rechtlich anerkannt und durchsetzbar. Da die Gesetzgebung von Land zu Land unterschiedlich ist, solltet ihr eine Richtlinie entwickeln, die in allen Ländern anwendbar ist, in denen ihr geschäftlich tätig seid. Bevor ihr beginnt, solltet ihr euch über die verschiedenen Gesetze und ihre Auswirkung auf die Verwendung elektronischer Unterschriften auf regionaler und internationaler Ebene informieren.

Die internationale Gesetzgebung zu elektronischen Signaturen lässt sich in zwei Kategorien einteilen:

- **Großzügig** – Viele Länder wie die USA, Australien, Neuseeland und Kanada regeln elektronische Unterschriften großzügig. Sie sind mit wenigen Einschränkungen allgemein zulässig und haben denselben Status wie händische Unterschriften.
- **Mehrstufig** – In anderen Ländern ist die Verwendung elektronischer Unterschriften generell zulässig. Einer Signatur mit zertifikatbasierter digitaler ID wird jedoch bei der Authentifizierung des Unterzeichners höhere Beweiskraft zugemessen, u. a. in der EU, China, Indien und Südkorea. In der EU haben beispielsweise nur Signaturen mit einer digitalen ID von einem qualifizierten Anbieter automatisch denselben Status wie eine händische Unterschrift.

Professionelle Lösungen für elektronische Unterschriften wie Adobe Sign ermöglichen die Einhaltung beider Gesetzgebungsarten und vereinfachen damit länderübergreifende Geschäftsprozesse.

Eine geeignete Lösung finden.

Ein wichtiger Schritt bei der Entwicklung einer Richtlinie für elektronische Unterschriften ist die Prüfung eurer Verträge. Die für euer Unternehmen optimale Lösung berücksichtigt die Gesetzgebung und das Risiko, sodass ihr euch mit möglichst geringem Aufwand auf rechtlich einwandfreie und zudem sichere Transaktionen verlassen könnt. Weitere Faktoren hängen von euren Geschäftsprozessen und den vor Ort gültigen Gesetzen und Vorschriften ab. In der Regel kommen bei gut strukturierten Prozessen für elektronische Unterschriften eine oder mehrere der folgenden Methoden zur Automatisierung von Unterzeichnungsprozessen und Sicherstellung höchster Compliance zum Einsatz.

- **Geringes Risiko: standardmäßige elektronische Signaturen** – Sofern kein hohes Geschäftsrisiko besteht und die örtlichen Gesetze dies zulassen, verwenden viele Organisationen standardmäßige elektronische Unterschriften für Vereinbarungen im üblichen Geschäftsverkehr. Das können etwa Verträge, Leistungsbeschreibungen oder Personalformulare sein. Im Rahmen eines abgesicherten Unterzeichnungsprozesses wird eine E-Mail an die Unterzeichner gesendet, die auf den eingebetteten Link klicken, um das betreffende Dokument zu öffnen. Diese Methode wird als erste Stufe der Authentifizierung betrachtet, weil die Mehrheit der Unterzeichner alleinigen Zugriff auf ihr E-Mail-Konto hat. Das Dokument ist

durchgehend geschützt, und jeder Schritt im Prozess – einschließlich der Authentifizierung – wird in einem Prüfprotokoll dokumentiert.

Sobald jeder Beteiligte unterschrieben hat, wird das endgültige Dokument automatisch mit einem manipulationssicheren Siegel zur Bestätigung der Integrität versehen und an alle Parteien gesendet. Um gesetzliche Bestimmungen noch zuverlässiger einzuhalten, könnt ihr Prozesse entwickeln, bei denen eine ausdrückliche Zustimmung zur elektronischen Unterschrift erforderlich ist.

- **Moderates Risiko: erweiterte elektronische Signaturen** – Viele Organisationen setzen bei kritischeren Dokumenten einen zweiten Authentifizierungsschritt voraus, bevor ein Unterzeichner ein Dokument öffnen oder unterzeichnen kann. Dazu gehören die Eingabe einer telefonisch übermittelten PIN, einer Social-ID, eines Kennworts oder die wissensbasierte Authentifizierung (Knowledge-Based Authentication, KBA).
- **Hohes Risiko oder gesetzliche Vorschrift: digitale Signaturen** – Einige Unternehmen verwenden digitale Signaturen, weil sie strikten gesetzlichen Vorgaben unterliegen und hochsensible Unterzeichnungsprozesse schützen müssen.

  Digitale Signaturen sind eine spezielle Art von elektronischer Unterschrift, bei der die Unterzeichner ihre Identität mit einer zertifikatbasierten digitalen ID nachweisen müssen. Diese IDs werden von Zertifizierungsstellen und Vertrauensdiensten ausgestellt. Wie bei den ersten beiden genannten Varianten können auch Lösungen für digitale Signaturen Prüfprotokolle, die automatische Zustellung des endgültigen Dokuments sowie Optionen für eine ausdrückliche Zustimmung enthalten. Der Nachweis der Unterschrift erfolgt jedoch anders, weil die Unterschrift selbst im Dokument verschlüsselt wird und auch lange nach der Unterzeichnung von der Zertifizierungsstelle oder dem Vertrauensdienst validiert werden kann.

Zur Auswahl der geeigneten Lösung für euer Unternehmen dienen die folgenden Leitfragen:

- Ist eine bestimmte Unterschriftsart gesetzlich vorgeschrieben?
- Seid ihr bereit, für alle Unterzeichner digitale IDs zu erwerben?
- Wie hoch ist die Wahrscheinlichkeit, dass eine Unterschrift angezweifelt wird – und wie hoch ist das damit verbundene Risiko?
- Wäre die Voraussetzung einer digitalen ID für Durchschnittskunden ein Argument gegen euer Unternehmen?

Best Practices befolgen.

Alle Gesetze für elektronische Unterschriften basieren auf den gleichen Prinzipien. Ob ihr nun in einem oder mehreren Ländern geschäftlich tätig seid: Mit sechs Fragen zur Richtlinie für elektronische Unterschriften könnt ihr sicherstellen, dass eure elektronischen Vereinbarungen rechtsgültig und durchsetzbar sind.

1. **Authentifizierung:** Wer hat unterschrieben?
2. **Absicht zur Unterzeichnung:** Hat der Unterzeichner seine Absicht zur Unterzeichnung dargelegt?
3. **Nachweis der Unterschrift:** Könnt ihr beweisen, dass ein Dokument unterschrieben und danach nicht mehr verändert wurde?
4. **Zustimmung:** Hat der Unterzeichner dem elektronischen Geschäftsverkehr zugestimmt?
5. **Ausnahmen:** Gibt es Ausnahmen für bestimmte Dokumentenarten?
6. **Archivierung:** Wie lange werden Unterlagen gespeichert?

Authentifizierung.

Workflows mit elektronischen Unterschriften müssen Optionen zur Authentifizierung der Unterzeichner umfassen. Je nach Risiko und Compliance-Anforderungen ihrer jeweiligen Geschäftsprozesse verwenden die meisten Unternehmen mindestens eine der oben beschriebenen Methoden. Da Adobe Sign alle Verfahren in einer Lösung vereint, könnt ihr für jeden Prozess die richtige Methode auswählen.

Absicht zur Unterzeichnung.

Prozesse sollten einen Schritt enthalten, in dem Unterzeichner eine eindeutige Aktion als Verpflichtungserklärung ausführen (z. B. ihren Namen eintippen bzw. schreiben oder auf eine Schaltfläche klicken). Unterzeichner sollten auch die Möglichkeit erhalten, sich gegen die elektronische Unterzeichnung zu entscheiden. Beide Funktionen sind in Adobe Sign-Workflows integriert.

Nachweis der Unterschrift.

Elektronische Unterschriften müssen mit dem unterzeichneten Dokument verknüpft sein, um als solche anerkannt zu werden.

Daher verfolgt Adobe Sign Dokumente zuverlässig während des gesamten Unterzeichnungsprozesses und zertifiziert die Integrität unterzeichneter Dokumente mit einem manipulationssicheren Siegel. Jeder Schritt wird in einem abgesicherten Prüfprotokoll erfasst, das als eindeutiger, leicht vorlegbarer Nachweis über die jeweiligen Unterschriften dient. Sobald ein Dokument unterzeichnet wurde, erhalten alle Unterzeichner eine unveränderte, vollständige Kopie des Dokuments in elektronischer Form.

Zustimmung zum elektronischen Geschäftsverkehr.

Viele Gesetze zu elektronischen Unterschriften setzen irgendeine Form der Zustimmung zur elektronischen Abwicklung von geschäftlichen Transaktionen voraus. Bei Lösungen wie Adobe Sign sind entsprechende Optionen im Unterzeichnungs-Workflow integriert, sodass keine entsprechende Anpassung der Dokumente nötig ist. Unter Umständen möchtet ihr jedoch zusätzliche Hinweise aufnehmen, z. B. eine Zustimmungsklausel. Über dem Unterschriftsfeld kann beispielsweise folgender Text eingefügt werden:

> **Wichtige Information – bitte lesen:** Mit deiner Unterschrift bestätigst du, dass du diese Kundeninformation gelesen hast und mit der Abwicklung mittels elektronischer Medien, dem Erhalt von Informationen und Offenlegungen auf elektronischem Weg und dem Einsatz von elektronischen Signaturen anstelle von Unterlagen in Papierform bzw. Unterschriften auf Papierdokumenten einverstanden bist. Du bist nicht verpflichtet, dem Erhalt von Kundeninformationen und Offenlegungen auf elektronischem Wege zuzustimmen oder Dokumente elektronisch zu unterschreiben. Auf Wunsch erhältst du Unterlagen in Papierform. Du kannst deine Zustimmung zum elektronischen Geschäftsverkehr jederzeit widerrufen.

Ausnahmen.

Manche Abläufe können nicht elektronisch durchgeführt werden. Es mag Vertragsarten geben, bei denen ungeachtet der generellen Richtlinie elektronische Signaturen grundsätzlich verwendet oder grundsätzlich nicht verwendet werden sollen. Dokumentiert solche Ausnahmen in der Richtlinie. Einige Gesetze zu elektronischen Unterschriften schließen beispielsweise Immobilienübertragungen und familienrechtliche Vereinbarungen aus. Dasselbe trifft auf stark reglementierte Branchen zu, etwa die Pharmaindustrie. Hier werden bei bestimmten Geschäftsprozessen nur digitale Signaturen akzeptiert. Die Risikoanalyse hilft bei der Bestimmung, welche Ausnahmen in die Richtlinie aufgenommen werden müssen.

Archivierung.

Behandelt elektronisch unterzeichnete Dokumente wie jedes andere Dokument. Dazu gehören auch Aufbewahrungsfristen. Unterlagen mit elektronischen Unterschriften müssen in der Regel genauso lange wie handschriftlich unterzeichnete Dokumente aufbewahrt werden. In jedem Fall müsst ihr die gesetzlichen Vorschriften befolgen, die die Aufbewahrungsregeln in eurem Unternehmen betreffen. Beachtet, dass Unterlagen in einem Format gespeichert werden müssen, auf die jede berechtigte Person zugreifen kann (z. B. der Unterzeichner). Adobe Sign speichert Dokumente bei Adobe Document Cloud. Wenn ihr Dokumente mit hohem Risiko hat, wäre auch ein ERM- oder E-Vault-System möglich.

Die Richtlinie formulieren.

Wenn ihr euch über den Inhalt eurer Richtlinie im Klaren sind, müsst ihr ihn für eure Mitarbeiter verständlich formulieren. Nachfolgend findet ihr drei hilfreiche Tipps:

Ziel.

Definiert den Zweck oder das Ziel der Richtlinie. Beispiel: „Diese Richtlinie betrifft die Einführung elektronischer Unterschriften und beschreibt Situationen, in denen elektronische Unterschriften und Unterlagen verwendet und akzeptiert werden."

Zusammenfassung.

Fügt eine Zusammenfassung der Richtlinie hinzu. Das kann ein kurzes Statement zur Entscheidung eures Unternehmens sein, elektronische Unterschriften, Genehmigungen oder Autorisierungen bei der Abwicklung von Geschäftsvorgängen als genauso rechtsverbindlich wie händische Unterschriften anzusehen. Falls elektronische Unterschriften in bestimmten Situationen nicht akzeptiert werden (etwa bei speziellen Vertragsarten oder in bestimmten Abteilungen), solltet ihr diese Ausnahmen in eurer Richtlinie aufführen.

Glossar.

Definiert häufig verwendete Begriffe, sodass jeder Leser weiß, wie bestimmte Ausdrücke in eurer Richtlinie zu verstehen sind. Im Anhang findet ihr einige Definitionen zu typischen Termini.

Die Richtlinie bekanntgeben.

Kommuniziert die Richtlinie anschließend unbedingt in eurem Unternehmen, damit jeder Mitarbeiter weiß, wie und in welchen Fällen elektronische Unterschriften in den Arbeitsablauf integriert werden müssen. Veröffentlicht die Richtlinie dort, wo Mitarbeiter bequem darauf zugreifen können. Erwägt auch eine Einführung im Rahmen einer Versammlung, die die Beantwortung von Fragen ermöglicht. Prüft abschließend die Implementierung im Unternehmen – inklusive Vorlagen für Standarddokumente und Workflows –, um sicherzustellen, dass sie mit der neuen Richtlinie übereinstimmt.

Weitere Informationen.

Unter den folgenden Links findet ihr weitere Informationen über elektronische Signaturen:

- Elektronische Signaturen weltweit: Leitfaden zu Gesetzgebung und Durchsetzbarkeit
- Vollständig digitale Geschäftsprozesse mit Adobe-Lösungen für elektronische und digitale Signaturen
- Gesetze zu elektronischen Signaturen

Anhang: Terminologie zu elektronischen Unterschriften bzw. Signaturen.

Eine **elektronische Signatur** (bzw. elektronische Unterschrift) ist ein elektronischer Prozess zum Bekunden der Zustimmung zu einem Vertrag oder Formular. Es gibt mehrere Methoden zur Authentifizierung der Identität des Unterzeichners bei elektronischen Signaturen.

Standardmäßige elektronische Signaturen kombinieren ein Authentifizierungsverfahren – wie den Zugriff auf ein E-Mail-Konto – mit einem abgesicherten Prozess, der ein Prüfprotokoll und die endgültige Fassung des Dokuments umfasst.

Erweiterte elektronische Signaturen prüfen die Identität des Unterzeichners per Multi-Faktor-Authentifizierung. Bevor die Unterzeichner ein Dokument öffnen können, müssen sie zuerst auf eine URL zugreifen, die an ihre E-Mail-Adresse gesendet wurde. Anschließend müssen sie einen bestimmten Vorgang ausführen, etwa eine telefonisch übermittelte PIN, eine Social-ID oder ein Kennwort eingeben oder eine Frage beantworten (Knowledge-Based Authentication, KBA).

Digitale Signaturen sind eine spezielle Art von elektronischer Unterschrift, bei der die Unterzeichner ihre Identität mit einer zertifikatbasierten digitalen ID nachweisen müssen. Als Nachweis der Unterschrift wird die Signatur im Dokument verschlüsselt. Die Prüfung erfolgt normalerweise durch Zertifizierungsstellen oder Vertrauensdienste.

Zertifizierungsstellen sind akkreditierte Firmen oder IT-Services, die digitale Identitäten ausstellen. Sie bestätigen vorab die Identität eines Unterzeichners und stellen dann die digitale ID, persönliche PIN und/oder das Hardware-Sicherheitsmodul (z. B. ein USB-Token oder eine Chip-Karte) zum Erstellen von digitalen Signaturen aus.

Vertrauensdienste sind Firmen, die verschiedene Services für sichere Identitäten und Transaktionen anbieten, darunter auch Zertifizierungsdienste. Beispielsweise definiert die eIDAS-Verordnung der EU eine Klasse von Vertrauensdiensten, die zur Ausstellung von digitalen IDs in jedem EU-Mitgliedsstaat berechtigt sind. Mit diesen IDs unterzeichnete Dokumente erfüllen den höchsten Sicherheitsstandard mit sogenannten „qualifizierten elektronischen Signaturen“, die denselben rechtlichen Status haben wie händische Unterschriften.