expertenReport

Quelle: Aukid – stock.adobe.com

Drei Punkte zur E-Signatur

Am 09. Februar ist der alljährliche Safer Internet Day. Das möchten wir zum Anlass nehmen, zu fragen, wie sicher ist eine elektronische Signatur eigentlich ist. Verträge nicht mehr mit der Hand unterzeichnen zu müssen, spart einem eine Menge Umstände, insbesondere dann wenn der Vertrag sowieso im digitalen Raum geschlossen wird.

Doch wie sicher ist das überhaupt? Können notwendige (digitale) Identifikationsprozesse beispielsweise mit Hilfe von Deepfakes ausgetrickst werden?

Drei wichtige Punkte

Qualifizierte elektronische Signatur (QES): Durch die strengen Richtlinien und Kontrollen ist die QES stärker gesichert, als eine händische Signatur. Für die Erstellung der QES sind drei Komponenten nötig: Die Signatur selbst, die ID und ein Schlüssel. Die ID ist die digitale Identität des Unterzeichnenden, während der Schlüssel das Sicherheitswerkzeug ist, um die Willensbekundung zu bestätigen, beispielsweise eine 2-Faktor-Authentisierung via Smartphone. Für die Anwendung stehen eine einfache, fortgeschrittenen und qualifizierte elektronische Signatur zur Verfügung.

Eine einfache, elektronische Unterschrift wird häufig für Unterlagen, die routinemäßig zu unterzeichnen sind verwendet. Das rechtliche und finanzielle Risiko ist dann häufig begrenzt oder überschaubar. Beispielsweise bei einem Übergabeprotokoll oder einer Besichtigungsbestätigung einer Immobilie.

Fortgeschrittene E-Signaturen sind sicherer. Angewendet werden sie zum Beispiel bei Finanztransaktionen oder auch Dokumenten mit erheblich höheren rechtlichen Risiken. Die qualifizierte elektronische Unterschrift basiert auf den identischen Sicherheitskriterien wie die fortgeschrittene Signatur.

Sie unterscheidet sich jedoch im Wesentlichen darin, dass die Identität der unterzeichnenden Person im Vorfeld festgestellt wurde. Der Signaturschlüssel muss in einer qualifizierten elektronischen Signaturerstellungseinheit (QSCD) vorliegen.

Videoidentifikationsverfahren: Bei seriösen Anbietern findet eine Videoidentifikation immer über Unternehmens-eigene Seiten statt und nie über externe Programme. So ist der Nutzer bestmöglich gegen Cyber-Kriminalität abgesichert. Ein Betrug durch Deepfakes während eines Videoidentifikationsverfahrens ist mit großen Hindernissen verbunden, da immer auch der Personalausweis benötigt wird.

Bank Identverfahren: Noch sicherer und unkomplizierter wird Ihre Identifikation für die Signatur, wenn sie durch ein bestehendes Bankkonto stattfindet.

Denn Banken sind durch die Know-Your-Customer-Erfordernis des Geldwäschegesetzes verpflichtet, die Identität ihrer Kunden erfassen zu müssen. Somit bietet es sich an, das Bankkonto als Mittel der Identifizierung zu integrieren.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4921043/wie-sicher-sind-elektronische-signaturen/