MANDANTEN
INFORMATION

SZA
SCHILLING, ZUTT & ANSCHÜTZ

April 2021

ELEKTRONISCHE SIGNATUREN – RECHTLICHER RAHMEN UND ANWENDUNG

Digitalisierung – ein Schlagwort, das sowohl im privaten wie auch geschäftlichen Alltag kontinuierlich mehr Raum einnimmt. Schnell, bequem, papierlos. So soll die Kommunikation besonders auch im geschäftlichen Bereich stattfinden. Dies gilt insbesondere in Zeiten der Pandemie, in denen die Verlagerung rechtsgeschäftlicher Handlungen ins Digitale besondere Bedeutung erlangt.

Daher wird für viele Unternehmen die Frage immer drängender, wie handschriftliche Signaturen eines Vertrages in Papierform rechtssicher durch elektronische Signaturen digitaler Vertragsdokumente ersetzt werden können: Welche Anforderungen müssen zur Rechtsgültigkeit einer elektronischen Signatur erfüllt sein und wie können diese konkret umgesetzt werden? Nachfolgend wird ein Überblick zu diesen Fragen gegeben.

Einleitend werden zunächst einige wesentliche Punkte zu Formzwang und der Formfreiheit im deutschen Recht skizziert, die für das Verständnis wichtig sind (I). Im Nachgang wird der rechtliche Rahmen für elektronische Signaturen erläutert (II). Es folgt ein Überblick zu den rechtlichen Konsequenzen und Wirkungen der elektronischen Signatur (III). Abschließend folgt eine Gegenüberstellung von Vor- und Nachteile (IV).

I. Formfreiheit und Formzwang

In Deutschland gilt das Prinzip der Formfreiheit von privatrechtlichen Rechtsgeschäften. Nur für ausgewählte Rechtsgeschäfte schreibt das deutsche Recht die Wahrung bestimmte Formen vor. Beispielsweise muss die Bürgschaftserklärung die Schriftform (§ 126 BGB) erfüllen (§ 766 S. 1 BGB) und ein Grundstückskaufvertrag bedarf der notariellen Beurkundung (§§ 311b Abs. 1, 128 BGB). Erfüllen Rechtsgeschäfte die gesetzlich vorgeschriebene Form nicht, sind sie nichtig (§ 125 BGB). Auch steht es den Parteien eines Vertrags im Rahmen ihrer Privatautonomie frei, auch jenseits dieser Fälle vertraglich Formzwänge zu vereinbaren (§ 127 BGB).

Solche Formvorschriften erfüllen u.a. den Zweck, den Inhalt eines Vertrags zu fixieren, um so den Beweis für dessen Inhalt zu erleichtern.

Das deutsche Recht kennt eine Reihe von unterschiedlichen Formerfordernissen. Neben den bereits erwähnten Varianten Schriftform und notarielle Beurkundung sind dies noch die Textform (§ 126b BGB) und die elektronische Form (§ 126a BGB). Die Textform, das einfachste Formerfordernis, verlangt neben einer lesbaren Erklärung auf einem dauerhaften Datenträger lediglich noch die Nennung der Person des Erklärenden. Im Unterschied dazu reicht bei der Schriftform die bloße Nennung des Unterzeichners nicht aus, vielmehr bedarf es einer eigenhändigen Unterschrift.

> Das Unterzeichnen mit dem Namen in einer Mail oder sonstigen elektronischen Dokument erfüllt daher ebenso wenig die Schriftform wie das Einfügen einer eingescannten Unterschrift.

Bei der elektronischen Form[1] hat der Aussteller einem elektronischen Dokument seinen Namen hinzuzufügen und es mit einer qualifizierten elektronischen Signatur (nachfolgend: eSignatur) zu versehen. Durch diese kann die Schriftform grundsätzlich ersetzt werden (näheres hierzu unter Ziff. III).

II. Rechtliche Anforderungen an die eSignatur[2]

Die Anforderungen und Rechtsfolgen der eSignatur sind für die gesamte EU einheitlich in der eIDAS-Verordnung[3] (im Folgenden eIDAS-VO) geregelt. Diese definiert drei unterschiedliche Formen elektronischer Signaturen, die ein jeweils abgestuftes Anforderungsprofil voraussetzen und unterschiedliche rechtliche Wirkungen erzeugen: einfache, fortgeschrittene und qualifizierte elektronische Signatur.

1. Einfache eSignatur

a. Voraussetzungen

Bei der einfachen eSignatur handelt es sich um Daten in elektronischer Form, die zum Unterzeichnen verwendet und die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden. Beispielsweise gelten eingescannte Unterschriften oder eine mit Namen unterzeichnete Mail als einfache eSignaturen. Die einfache eSignatur ähnelt also konzeptionell der Textform (§ 126 BGB) und stellt die "schwächste" eSignatur dar.

b. Bewertung

Aus der Einfachheit dieser Signaturform folgt, dass sie keinen hohen Sicherheitswert aufweist, weil sie ohne Weiteres kopierbar und entfernbar ist. Mangels eines technischen Manipulationsschutzes ist nicht ersichtlich, ob die Erklärung tatsächlich von dem als Unterzeichner ausgewiesenen Erklärenden stammt. Ferner lässt sich nicht feststellen, ob das Dokument im Nachhinein verändert wurde. Einfache eSignaturen haben also keinen hohen Sicherheits- und Beweiswert.

2. Fortgeschrittene eSignatur

a. Voraussetzungen

Die fortgeschrittene eSignatur zeichnet sich durch vier spezifische Merkmale aus: Erstens wird grundlegend eine einfache eSignatur verlangt, die dem Unterzeichner eindeutig zugeordnet werden kann. Zweitens muss die Signatur die Identifizierung des Unterzeichners ermöglichen. Drittens muss die Signatur unter Verwendung elektronischer Signaturerstellungsdaten erstellt werden, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann. Schließlich ist viertens erforderlich, dass die Signatur mit den von ihr unterzeichneten Daten in einer Weise verbunden ist, dass eine nachträgliche Veränderung der Daten erkannt werden kann. Was bedeuten diese Anforderungen konkret?

1 Die das BGB im Übrigen bereits seit 2001 kennt.

2 Wichtig für das Verständnis: Die eIDAS-VO unterscheidet konzeptionell zwischen "Signaturen" (die nur natürlichen Personen zugeordnet werden können) und "Siegeln" (für juristische Personen etc.), s. auch unten Ziff. II.3.a.

3 Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates v. 23.7.2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

Im Wesentlichen basiert die fortgeschrittene e-Signatur auf zwei sog. "Schlüsseln" in elektronischer Form: Dem Unterzeichner ist ein geheimer, privater Schlüssel zugeordnet und dem Empfänger des Dokuments ein für jedermann zugänglicher, öffentlicher Schlüssel. Der öffentliche Schlüssel stellt eine Art Gegenstück zum privaten Schlüssel dar. Mittels eines Algorithmus wird aus dem Text des zu verschlüsselnden Dokuments der sogenannte Hash-Wert (anschaulich: ein "elektronischer Fingerabdruck") errechnet. Dieser Hash-Wert wird anschließend mit dem oben benannten privaten Schlüssel des Signierenden verschlüsselt. Der verschlüsselte Hash-Wert wird sodann zusammen mit dem unverschlüsselten Dokument dem Empfänger übermittelt. Mit dem öffentlichen Signaturprüfschlüssel kann der verschlüsselte Hash-Wert decodiert werden. Wenn der Empfänger schließlich mittels Algorithmus den Hash-Wert des übermittelten unverschlüsselten Dokuments errechnet, kann er diesen mit dem entschlüsselten Hash-Wert, der vom Unterzeichner übersendeten wurde, vergleichen. Stimmen die Werte überein, dann wurde das übermittelte Dokument auch nicht nachträglich verändert.

In a nutshell: Die fortgeschrittenen eSignatur erfordert die verschlüsselte Übermittlung eines auf dem signierten Dokument basierenden Wertes, der mit dem auf Grundlage des übersendeten Dokuments errechneten Wertes verglichen werden kann. Weichen diese Werte voneinander ab, dann wurde das übersendete Dokument nachträglich verändert. Dadurch können nach der Signierung vorgenommene Manipulationen des Dokuments identifiziert werden.

Das beschriebene Verfahren lässt sich durch entsprechende Software verschiedener Anbieter durchführen. Möglich ist auch ein dezentrales Verfahren (ohne lokale Software) über die Nutzung eines sog. Vertrauensdienstanbieters. Hierbei handelt es sich um spezielle Dienstleister, die einfache eSignaturen "as a service" anbieten. Solche Vertrauensdienstanbieter müssen nach der eIDAS-VO bestimmte technische und organisatorische Sicherheitsmaßnahmen ergreifen.[4] Die eIDAS-VO verfolgt das Ziel, solche Fernsignaturverfahren, die insbesondere für Verbraucher technische Hürden einebnen, vermehrt zuzulassen. Möchte man dem Vertragspartner, der über eine solche Software nicht verfügt (regelmäßig wird das bei Verbrauchern der Fall sein), einen möglichst einfachen digitalen Vertragsschluss ermöglichen, bietet sich ein solches Fernsignaturverfahren besonders an.

b. Bewertung

Die fortgeschrittene eSignatur bietet gegenüber der einfachen eSignatur den Vorteil, dass eine nachträgliche Manipulation des signierten Dokuments identifiziert werden kann. Außerdem kann sich der Empfänger sicher sein, dass die Person, die über den privaten Schlüssel verfügt, auch der Signierende ist.

Dagegen ermöglicht dieses Verfahren nicht die Verifizierung der Identität des Signaturerstellers, so dass diese aus Empfängersicht unge-

4 Die behördliche Kontrolle der Vertrauendiensteanbieter ist in Deutschland in einem eigenem Stammgesetz, dem Vertrauensdienstegesetz, geregelt; s. zur Aufsichtspflicht auch Art. 17 eIDAS-VO.

wiss bleibt. Zudem stellt die fortgeschrittene e-Signatur noch keine bestimmten Sicherheitsanforderungen an die Schlüsselverwaltung und an die Software- und Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels. Somit bestehen Manipulationsrisiken, insbesondere bei nicht hinreichend sicherer Schlüsselverwaltung durch den Unterzeichner. Aus diesen Gründen vermag auch die fortgeschrittene eSignatur die Schriftform (§ 126 BGB) nicht zu ersetzen (dazu sogleich Ziff. III).

3. Qualifizierte eSignatur

a. Voraussetzungen

Die qualifizierte eSignatur wird in der Praxis beispielsweise bei der digitalen Steuererklärung über das Programm ELSTER oder auch bei der elektronischen Handelsregisteranmeldung (§ 12 HGB) eingesetzt und stellt die höchste Stufe der elektronischen Signaturen dar. Sie muss an eine fortgeschrittene eSignatur noch zwei weitere Anforderungen erfüllen: Erstens muss die Signatur von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt worden sein (dazu sogleich Ziff. II.3.b) und zweitens auf einem qualifizierten Zertifikat für eSignaturen beruhen (dazu sogleich Ziff. II.3.c).

Um für die elektronische Form äquivalente Voraussetzungen zur Schriftform zu schaffen, dürfen qualifizierte Zertifikate nur für natürliche Personen ausgestellt werden. Juristischen Personen können über sog. elektronische Siegel zugeordnet werden. Die eIDAS-VO unterscheidet zwischen elektronischen, fortgeschrittenen und qualifizierten Siegeln nach denselben Kriterien, die für Signaturen verwendet werden.

b. Qualifizierte elektronische Signaturerstellungseinheit

Software- oder Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels müssen spezielle Sicherheitsanforderungen erfüllen, die von der eIDAS-VO näher konkretisiert werden. Im Wesentlichen muss sichergestellt sein, dass die für die eSignatur verwendeten Daten vom rechtmäßigen Unterzeichner gegen eine Verwendung durch andere verlässlich geschützt werden können. Außerdem muss die Signaturerstellungseinheit einen verlässlichen Fälschungsschutz gewährleisten. In der Praxis sind aktuell Signaturkarten mit entsprechenden Lesegeräten, die der Unterzeichnende anschaffen muss, am geläufigsten.

c. Qualifiziertes Zertifikat

Qualifizierte Zertifikate sind elektronische Identitätsnachweise. Dieses Zertifikat lässt sich etwa mit dem elektronischen Personalausweis vergleichen, der nach einer Identitätsprüfung (z.B. Postident-Verfahren) ausgestellt wird. Das Zertifikat enthält insbesondere den öffentlichen Signaturschlüssel für den Empfänger, den Namen des Signierenden und die Gültigkeitsdauer des Zertifikats.

Im Unterschied zur fortgeschrittenen eSignatur kann das Zertifikat nach einer Identitätsprüfung nur von staatlich anerkannten Anbietern ausgestellt werden, nämlich von qualifizierten Vertrauensdienstanbietern. Dies sind Anbieter, die die weitreichenden technischen Sicherheitsvorgaben der eIDAS-VO erfüllen und von der zuständigen Aufsichtsstelle einen entsprechenden Qualifikationsstatus verliehen bekommen haben.

Eine Liste der in Deutschland anerkannten Anbietern lässt sich mit folgendem Link abrufen:

https://www.elektronische-vertrauensdienste.de/cln_131/EVD/DE/Verbrauche

r/Vertrauensdienste/Signatur/Signatur-start.html

Eine Liste für die in Europa anerkannten Anbieter findet sich unter:

https://webgate.ec.europa.eu/tl-browser/#/

Die eIDAS-VO lässt auch Fernsignaturverfahren zu, so dass die Vertragsparteien keine eigene Hardware anschaffen müssen, um Zugriff auf eine Signaturerstellungseinheit zu erhalten. Bisher wurden in Deutschland wurde bislang lediglich das sog. "sign-me"-Verfahren der Bundesdruckerei (das sich für die Identifikation eines Video-Chats oder der Online-Funktion des Personalausweises bedient) und das "PostIdent"-Verfahren der Deutsche Post AG als hinreichend sicher anerkannt. Diese arbeiten allerdings ggf. mit anderen Anbietern zusammen, die für ihre eigenen Dienste auf diese Verfahren zurückgreifen.

d. Bewertung

Weil qualifizierte eSignatur nicht nur eine, sondern zwei technische Signaturkomponenten aufseiten des Unterzeichnenden und eine Identifikation der Vertragsparteien erfordert, gilt sie als besonders sicher und ist der Schriftform gleichgestellt (näher unter Ziff. III). Ein weiterer Vorteil ist, dass die qualifizierte eSignatur in allen Mitgliedstaaten der EU anerkannt wird, gleich, in welchem EU-Land der qualifizierte Vertrauensdiensteanbieter ansässig ist. Eine Vorschrift über die Anerkennung von solchen Signaturen aus Drittstaaten gibt es allerdings nicht, so dass (Papier-)Unterschriften weiterhin eine weitaus höhere internationale Anerkennung genießen als qualifizierte eSignaturen. Zudem ist zu bedenken, dass die Anschaffung der erforderlichen Hard- und Software bzw. die Inanspruchnahme von Vertrauensdienstanbietern kostenintensiv sein können.

III. Die eSignatur in der Rechtsanwendung

1. Vertragsrecht

Nach den §§ 126 Abs. 3, 126a Abs. 1 BGB kann die gesetzlich vorgeschriebene Schriftform durch die qualifizierte eSignatur ersetzt werden. Dieser Form der Signatur kommt also eine Ersatzfunktion für die Fälle zu, in denen das Gesetz die Schriftform vorschreibt. Diese Ersetzungsmöglichkeit gewährt das Gesetz aber dann nicht, wenn die qualifizierte eSignatur gesetzlich ausgeschlossen ist, beispielsweise bei der Beendigung des Arbeitsverhältnisses (§ 623 HS. 2 BGB) oder der Erteilung von Bürgschaftserklärungen (§ 766 S. 2 BGB). Die einfache und fortgeschrittene eSignatur erfüllen lediglich die Textform nach § 126b BGB, sie können die Schriftform daher nicht ersetzen.

Einfache eSignatur = Textform

Fortgeschrittene eSignatur = Textform

Qualifizierte eSignatur = elektronische Form = Schriftform (soweit keine gesetzliche Ausnahme greift)

Nach § 127 Abs. 1 BGB kann die elektronische Form auch durch Rechtsgeschäft vereinbart werden. Die Vertragsparteien können jegliche eSignaturen vereinbaren, also auch solche, die

die oben erläuterten Definitionen der eIDAS-VO nicht erfüllen.[5]

2. Beweisrechtliche Aspekte

Dokumente, die mit einer eSignatur versehen wurden gelten bei der gerichtlichen Beweiswürdigung als Augenscheinsobjekte, die der freien richterlichen Beweiswürdigung unterliegen (§§ 286, 371 Abs. 1 ZPO). Eine Ausnahme davon gilt für private elektronische Dokumente, die mit einer qualifizierte eSignatur versehen sind (§ 371a Abs. 1 ZPO). Ein dementsprechend signierter Vertrag erbringt den vollen Beweis für die Abgabe der darin enthaltenen Erklärungen und zugleich wird die Richtigkeit und Vollständigkeit der entsprechend elektronisch signierten Urkunde vermutet (vgl. § 416 ZPO).

Fazit: Der Beweiswert der einfachen und fortgeschrittenen eSignatur bleibt weit hinter dem der qualifizierten eSignatur zurück, die daher immer dann vorzugswürdig ist, wenn es um einen möglichst hohen Beweiswert geht – dies teilt sie allerdings mit der traditionellen Schriftform.

3. Datenschutzrechtliche Aspekte

Die Nutzung von eSignaturen wirft auch datenschutzrechtliche Fragen auf: Fraglich ist wann und in welchem Umfang beim Einsatz von eSignaturen die Bestimmungen des Datenschutzrechts zu beachten sind. Dies richtet sich im Wesentlichen danach, wer im Einzelfall datenschutzrechtlich für die Nutzung der eSignatur verantwortlich ist.

a. Datenschutzrechtliche Verantwortlichkeit

Datenschutzrechtlich verantwortlich ist grundsätzlich, wer über die Zwecke und Mittel der Datenverarbeitung entscheidet (Art. 4 Nr. 7 DS-GVO). Die datenrechtlich Verantwortlichen haben für die Einhaltung des Datenschutzes Sorge zu tragen.

Das Verfahren der einfachen eSignatur wird regelmäßig von den Erklärenden selbst durchgeführt, so dass diese (bzw. deren Arbeitgeber) datenschutzrechtlich verantwortlich sind.

Wie zuvor dargestellt, bedienen sich die Erklärenden bei der Erstellung fortgeschrittener e-Signaturen externer Vertrauensdienstanbieter. Diese Vertrauensdienstanbieter dürften dabei zumeist als Auftragsverarbeiter gelten (Art. 4 Nr. 7, 8 DS-GVO). Folglich müssen diese Dienste anhand bestimmter Sorgfaltskriterien ausgewählt werden (Art. 28 Abs. 1 DS-GVO). Zudem muss mit dem Vertrauensdienstanbieter ein Auftragsverarbeitungsvertrag abgeschlossen werden (Art. 28 Abs. 3 DS-GVO).

Bezüglich der qualifizierten eSignatur ist die datenschutzrechtliche Verantwortung umstritten und noch nicht rechtssicher geklärt. Unklar ist, ob die Vertrauensdienstanbieter auch bei dieser Signaturvariante als Auftragsverarbeiter gelten oder eine gemeinsame datenrechtliche Verantwortlichkeit von Signierendem und Vertrauensdienstanbieter anzunehmen ist, die ebenfalls den Abschluss eines Vertrags über die Bedingungen der Datenverarbeitung erforderlich

5 Zudem enthält § 127 Abs. 2 S. 1 BGB eine Regelung, wonach bei vertraglicher Vereinbarung (selbst) der Schriftform für einseitige Erklärungen die telekommunikative Übermittlung genügt, wenn nicht ein anderer Parteiwille anzunehmen ist. Hier kann also auch die einfache Textform (ob elektronisch oder nicht) der Wahrung der Schriftform genügen.

macht (Art. 26 DS-GVO). Aufgrund dieser ungeklärten Rechtslage empfiehlt sich die enge anwaltliche Begleitung bei der Implementierung der qualifizierten eSignatur in einem Unternehmen.

b. Datenschutzrechtliche Pflichten der Verantwortlichen

Die jeweils Verantwortlichen müssen sicherstellen, dass die Vorgaben der DS-GVO eingehalten werden. In einer nicht abschließenden Aufzählung sind u.a. folgende wesentlichen Pflichten festzuhalten: Die Vertragspartner der Signierenden müssen über die Verarbeitung ihrer Daten vor Durchführung des Signaturverfahrens informiert werden. Bereits oben wurden auf die Verträge hingewiesen, die der Signierende in den einschlägigen Fällen mit dem Vertrauensdienstanbieter abzuschließen hat. Ferner ist die Datenverarbeitung in das Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO) aufzunehmen. Die Mitarbeiter des Unternehmens sind hinsichtlich eines datenschutzkonformen Umgangs mit den Daten und des Ablaufs des digitalen Vertragsschlusses zu schulen.

> Wegen der mitunter hohen Komplexität zwangsläufig aufkommender datenschutzrechtlicher Fragen bei der Verwendung von fortgeschrittenen und qualifizierten eSignaturen wird die vorherige Einholung anwaltlicher Beratung empfohlen.

IV. Vor- und Nachteile der eSignatur

1. Vorteile

Vorteil der eSignaturen ist unbestreitbar die Beschleunigung des "Workflows", da es keiner Medienunterbrechung mehr bedarf. Insbesondere pandemische Situationen, in der Kontakte eingeschränkt und übersandte Schriftstücke virale Träger sein können, führen die Vorteile elektronischer Vertragsschlüsse deutlich vor Augen. Die Papierlosigkeit der elektronischen Vertragsunterzeichnung ist ein weiterer Pluspunkt, der dem aktuellen Trend zur umweltschonenderen Unternehmensgestaltung entgegenkommt. Damit einher geht die Entbehrlichkeit physischer Archive, die Platz wegnehmen und Kosten verursachen.

2. Nachteile

Die oben angesprochene Beschleunigung des „Workflows“ kann selbstredend erst dann gewährleistet werden, wenn die entsprechenden organisatorischen Vorkehrungen für eSignaturen geschaffen wurden. Insbesondere die fortgeschrittene und qualifizierte eSignatur kann einen nicht unerheblichen Zeit- und Kostenaufwand mit sich bringen, weil entsprechende Hard- und Software zunächst angeschafft und Mitarbeiter geschult werden müssen. Die Möglichkeit des Rückgriffs auf Vertrauensdienstanbieter mag diesen Malus teilweise relativieren, dennoch bleiben die Kosten für diese Dienstleistung, die bei der eigenhändigen Signatur nicht anfallen würden. Zudem ist die eSignatur nicht vor dem Risiko eines Hackerangriffs gefeit, wenngleich Manipulationsrisiken auch bei der handschriftlichen Unterzeichnung bestehen.

V. Umsetzung und Fazit

Es zeigt sich, dass die Nutzung von eSignaturen große Potentiale hinsichtlich der Effizienzsteigerung bei der Abgabe und der (sicheren) Dokumentation von Erklärungen hat. Gleichzeitig erfordert ihre Implementierung in die Unternehmenspraxis eine sorgfältige technische, rechtliche und organisatorische Planung und Umsetzung. Nur so kann sichergestellt werden, dass ein "Wildwuchs" vermieden wird (etwa

durch unternehmensinterne Richtlinien zur Verwendung von eSignaturen) und dass rechtliche Risiken reduziert werden (insbesondere auch in datenschutzrechtlicher Hinsicht) sowie, dass die technische Sicherheit, insbesondere soweit sie für eine Wirksamkeit der eSignaturen erforderlich ist.

Diese Mandanteninformation beinhaltet lediglich eine unverbindliche Übersicht über das in ihr adressierte Themengebiet. Sie ersetzt keine rechtliche Beratung. Als Ansprechpartner zu dieser Mandanteninformation und zu Ihrer Beratung stehen gerne zur Verfügung:

DR. THOMAS NÄGELE,
PARTNER
T +49 621 4257-222
F +49 621 4257-286
Thomas.Naegele@sza.de
www.sza.de

DR. SIMON APEL,
ASSOCIATE
T +49 621 4257-386
T +49 621 4257-286
Simon.Apel@sza.de
www.sza.de