

Was tun vor dem Wieder-Start des beA?

Rechtsanwältin Dr. Tanja Nitschke, Mag. rer. publ., BRAK, Berlin

Der weitere Fahrplan

Noch ist das beA nicht wieder am Netz. Die Sicherheitstests der von der BRAK beauftragten Firma secunet laufen derzeit. Der Prüfauftrag ist allerdings noch nicht vollständig abgearbeitet. Vorläufig lässt sich sagen, dass in einzelnen Bereichen Maßnahmen umgesetzt werden sollten, um die IT Sicherheit weiter zu erhöhen; Atos ist bereits mit der Umsetzung betraut worden. Sobald das abschließende Gutachten von secunet vorliegt und im Grundsatz grünes Licht gibt, entscheidet die BRAK-Präsidentenkonferenz darüber, wann das beA wieder in Betrieb geht.

Die Vorlaufphase

Die BRAK wird das System nach dem Beschluss der Präsidentenkonferenz nicht sofort wieder scharf schalten. Vielmehr soll eine Vorlaufphase der Anwaltschaft Zeit geben, die (Neu-)Installation von beA durchzuführen; diejenigen, die ihren Einstieg in die Arbeit mit dem beA für die Zeit des Jahreswechsels geplant hatten, sollen sich am beA-System erstregistrieren und es testen können. Die alte beA Client Security – deren Sicherheitslücken die BRAK veranlassten, das beA vom Netz zu nehmen – sollte in jedem Fall (sofern noch nicht erfolgt) deinstalliert werden.

Die BRAK nimmt mit der Vorlaufphase Rücksicht darauf, dass manche Kolleginnen und Kollegen hierzu die Hilfe von IT-Dienstleistern benötigen oder ihre IT-Abteilung einbinden müssen. Hier bestehen sehr unterschiedlichen Anforderungen; deren ist die BRAK sich bewusst und wird versuchen, sie so weit wie möglich zu berücksichtigen.

Die sinnvollen Vorbereitungen

Was sollten Anwältinnen und Anwälte tun, um für den Wieder-Start des beA gewappnet zu sein? Juristentypisch lautet die Antwort: Es kommt darauf an.

Wenig zu tun hat, wer bisher schon mit dem beA gearbeitet hat: Nach aktuellem Stand ist lediglich die beA Client Security herunterzuladen und erneut zu installieren. Wann sie bereitsteht, wird die BRAK rechtzeitig bekanntgeben.

Wer in einer Kanzlei oder in einem Unternehmen mit eigenen IT-Sicherheitsrichtlinien tätig ist, sollte dann baldmöglichst die IT-Abteilung bzw. seinen

IT-Dienstleister kontaktieren, um die richtlinienkonforme Implementierung der neuen Client Security sicherzustellen (dazu *Hermesmeier*, BRAK-Magazin 5/2017, 12).

Der Einstieg für beA-Neulinge

Neu-Einsteiger in die Arbeit mit dem beA sollten zunächst einmal sicherstellen, dass die notwendige bzw. sinnvolle technische Ausrüstung – insbesondere ein Kartenlesegerät (oder mehrere, falls mehrere Personen in der Kanzlei mit dem beA arbeiten sollen) bzw. ein Scanner – zur Verfügung stehen oder jedenfalls kurzfristig beschafft werden können.

Wer noch keine beA-Karte (und ggf. zusätzliche beA-Karten für Mitarbeiter) hat, sollte sich beizeiten um die Bestellung (unter <https://bea.bnotk.de>) kümmern. Das mag etwas merkwürdig klingen, solange das beA nicht nutzbar ist. Jedoch sollte auch die Lieferzeit der Bundesnotarkammer mit bedacht werden, welche die beA-Karten im Auftrag der BRAK ausstellt. Sobald der Wieder-Start des beA angekündigt ist, könnte es dort wegen geballter Nachfrage zu Wartezeiten kommen. Sinnvoll ist es, vorher den eigenen Eintrag im bundesweiten amtlichen Anwaltsverzeichnis (www.rechtsanwaltsregister.org) zu prüfen und die für die Bestellung nötige SAFE-ID nachzusehen.

Zudem muss die beA Client Security heruntergeladen und auf allen Rechnerarbeitsplätzen der Kanzlei installiert werden, die mit dem beA arbeiten sollen. Sodann ist die Erstregistrierung durchzuführen. Auch hier sollte man nach Bekanntgabe des Wieder-Starts möglichst rasch handeln und bedenken, dass es auch beim Support zu Wartezeiten kommen kann. Sofern vorhanden, sollten auch hier IT-Abteilungen bzw. IT-Dienstleister rechtzeitig eingebunden werden.

Das beA ermöglicht es, z.B. dem Kanzleipersonal oder einem Urlaubsvertreter abgestufte Zugriffsrechte auf das eigene beA-Postfach einzuräumen und so die Aufgabenteilung der Kanzlei auch für das beA abzubilden. Auch hierüber sollte man sich vorab Gedanken machen. Und schließlich kann die Zeit bis zum Wieder-Start auch genutzt werden, um sich in einer Schulung mit dem beA vertraut zu machen.

Rechtsverkehr elektronisch – der rechtliche Rahmen

Rechtsanwältin Dr. Tanja Nitschke, Mag. rer. publ., BRAK, Berlin

Seit Anfang 2018 gelten neue Regelungen für den elektronischen Rechtsverkehr, und zwar unabhängig davon, ob das besondere elektronische Anwaltspostfach (beA) nutzbar ist. Natürlich betrifft das vor allem diejenigen, die, solange das beA offline ist, elektronische Dokumente per EGVP (oder per DE-Mail) bei Gericht einreichen; aber alle anderen sollten bereits jetzt einen Überblick haben, was auf sie zukommt.

Zulässige Übermittlungswege

Vorbereitende Schriftsätze und deren Anlagen können elektronisch bei Gericht eingereicht werden (§ 130a I ZPO). Aus dem „kann“ wird ab dem 1.1.2022 ein „muss“ (§ 130d ZPO in der dann geltenden Fassung). Die Länder können die verpflichtende Nutzung des elektronischen Rechtsverkehrs auf 2020 bzw. 2021 vorziehen.

Senden darf man elektronische Dokumente nur auf den in § 4 I ERVV genannten Wegen: über einen „sicheren Übermittlungsweg“ oder über das EGVP des Gerichts – also nicht etwa per E-Mail. „Sichere Übermittlungswege“ definiert § 130a IV ZPO: z.B. DE-Mail, das beA oder das besondere elektronische Notarpostfach (beN). Scheitert die Übermittlung z.B. an der maximalen Dateigröße, kann gem. § 3 ERVV ersatzweise nach den allgemeinen Vorschriften (möglichst mit den Dateien auf einem Datenträger) eingereicht kann.

Anforderungen an vorbereitende Schriftsätze

Neben den Anforderungen des § 130 ZPO (Bezeichnung von Parteien, Anträgen etc.) sind spezielle Vorgaben für elektronische Dokumente zu beachten. Formal müssen die Dokumente gem. § 130 II ZPO „für die Bearbeitung durch das Gericht geeignet“ sein. Der technische Rahmen dafür ist in der Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs (ERVV) fixiert. Sie gilt für Verfahren vor Zivilgerichten (und weitere in § 1 ERVV genannte) und für Strafverfahren (vgl. §§ 10, 11 ERVV). Nicht „geeignet“ sind z.B. durch Schadsoftware kontaminierte Dateien; dafür sieht § 130a VI ZPO ein Auffang-Verfahren vor. In anderen Fällen, in denen ein Dokument nicht „geeignet“ ist (z.B. Textdatei statt pdf, fehlende Signatur o.ä.) dürfte die allgemeine gerichtliche Hinweispflicht greifen (z.B. § 139 ZPO).

Wichtig sind v.a. die Vorgaben zum Dateiformat in § 2 I ERVV: Zulässig sind pdf und tiff; Konkretes regeln § 4 I ERVV und die aufgrund von § 5 ERVV erlassene Verordnung. Ferner verlangt § 2 II ERVV Dateinamen, die den Inhalt des Dokuments umschreiben, also z.B. „Klageschrift“ oder „Anlage 1“. Beizufügen ist auch ein sog. Strukturdatensatz (§ 4 III ERVV), der – ähnlich wie § 130 ZPO – u.a. Parteien, Gericht und Aktenzeichen enthält und automatisch vom IT-System des Gerichts ausgelesen werden kann (dazu Brosch, BRAK-Magazin 6/2017, 11).

Schriftformersatz

Elektronische Dokumente müssen zuverlässig erkennen lassen, von wem sie stammen. Dies kann entweder durch eine qualifizierte elektronische Signatur des Ausstellers erfolgen (§ 130a III, 1. Alt. ZPO) – dann kann ein beliebiger Übermittlungsweg i.S.d. ERVV genutzt werden. Oder der Aussteller sendet das Dokument über einen sicheren Übermittlungsweg (z.B. als Anwalt: sein beA) – dann genügt eine einfache Signatur (Art. 3 Nr. 10 eIDAS-VO, z.B. Wiedergabe des Namens), um das prozessuale Formerfordernis zu erfüllen (§ 130a III, 2. Alt. ZPO). Materiell-rechtliche Schriftformerfordernisse sind so indes nicht erfüllbar, für sie gelten §§ 126 III, 126a BGB.

Containersignaturen, mit denen mehrere Dokumente zugleich signiert werden, sind nach § 4 II ERVV unzulässig. Dies sieht zwar das OLG Brandenburg (BRAK-Mitt. 2018, 116 Ls.) anders; das Gebot des sichersten Weges legt aber nahe, dem nicht zu folgen.

Vorschriften für Anlagen

Für Anlagen gilt die ERVV nur, soweit es Dokumente sind, für die die Schriftform nach § 130a ZPO elektronisch ersetzbar ist (§ 1 ERVV). Elektronische Beweismittel (z.B. Audio-/Videodateien) können auf einem (nach § 5 I ERVV zulässigen) Datenträger eingereicht werden.

Urkunden dürfen gem. § 131 I ZPO nur als Abschrift eingereicht werden – bei elektronischer Einreichung also: als Scan der Urkunde. Insoweit gelten die Vorgaben des § 2 ERVV. Die Beweisregeln (insb. §§ 371, 371a, 371b ZPO) berücksichtigen elektronische Beweismittel bereits.