+420 733 555 958
office@sedlakovalegal.com
www.sedlakovalegal.cz

RECHTSGUTACHTEN — SYSTEM PROOFSNAP ALS BEWEISMITTEL UND BEURTEILUNG SEINER BEWEISKRAFT

Mandant: **Software Innovations Group LLC**
Sitz: Sharjah Media City (SHAMS), Al Messaned, Al Bataeh, Sharjah, Vereinigte Arabische Emirate

(im Folgenden auch „Mandant")

Verfasserin: **SEDLAKOVA LEGAL s.r.o.**
IČO (Identifikationsnummer): 056 69 871
Sitz: Purkyňova 648/125, Medlánky, 612 00 Brno
eingetragen im Handelsregister, geführt vom Regionalgericht Brno
Abteilung C, Einlage 97278

(im Folgenden auch „Verfasserin")

Erstellungsdatum: 21.04.2026

I. Auftrag

In der vorliegenden Angelegenheit wurde die Anwaltskanzlei SEDLAKOVA LEGAL s.r.o. von Herrn Radim Motyčka, der die Gesellschaft Software Innovations Group LLC vertritt, mit der Erstellung eines Rechtsgutachtens (einer Analyse) zum System „ProofSnap" beauftragt, das diese Gesellschaft betreibt (im Folgenden auch „ProofSnap" oder „Dienst"). Gegenstand des Dienstes ist die Möglichkeit, jegliche elektronische Darstellung (z. B. Websites, Kommunikation in sozialen Netzwerken usw.) mittels einer digitalen Aufzeichnung zu einem bestimmten Zeitpunkt zu erfassen, um anschließend die Integrität und Authentizität der erfassten Darstellung überprüfen zu können.

ProofSnap erfasst und speichert den aufgenommenen Inhalt zusammen mit relevanten technischen Daten (z. B. Aufnahmezeitpunkt, Quellenidentifikation, Dateikennungen und weitere Metadaten) und sichert diesen gleichzeitig durch kryptographische Mechanismen gegen nachträgliche Veränderungen ab, wodurch eine unabhängige Überprüfung ermöglicht wird, dass seit dem Aufnahmezeitpunkt keine Manipulation der Aufzeichnung stattgefunden hat.

Das Ergebnis des Dienstes ist ein „Beweispaket", das folgende Dateien enthält:

1. screenshot.jpeg — Bild, das eine visuelle Aufnahme der Website (der elektronischen Darstellung) erfasst.
2. metadata.json — enthält kontextbezogene Informationen über den Beweis, wie Zeitstempel, URL und Browserinformationen.
3. manifest.json — Liste aller Beweisdateien und ihrer Hashes zur Überprüfung der Integrität des Pakets.

+420 733 555 958
office@sedlakovalegal.com
www.sedlakovalegal.cz

4. manifest.sig — digitale Signatur des Manifests, gewährleistet Echtheit und Integrität.
5. manifest.json.ots — OpenTimestamps-Nachweis für die Datei manifest.json.
6. manifest.json.tsr — qualifizierter elektronischer Zeitstempel im Sinne von Art. 42 eIDAS, ausgestellt von Disig, a.s. (RFC 3161 ASN.1 TimeStampToken-Format).
7. eidas_validation.json — Validierungsmetadaten für den qualifizierten eIDAS-Zeitstempel (Disig).
8. publickey.pem — öffentlicher Schlüssel zur Überprüfung der digitalen Signatur des Manifests.
9. evidence.pdf — PDF-Dokument, das alle Beweisdateien zur einfachen Weitergabe und Überprüfung enthält.
10. domtextcontent.txt — aus dem DOM der Website extrahierter Textinhalt.
11. forensic_log.json — forensisches Protokoll gemäß ISO/IEC 27037 mit einer Hash-Kette, die jeden Erfassungsvorgang aufzeichnet.
12. chain_of_custody.json — Dokument der Beweismittelkette (Chain of Custody) mit Geräteintegrität, NTP-Zeitverifikation und Beweisverknüpfung.
13. page.html — vollständiger HTML-Inhalt der erfassten Website (der elektronischen Darstellung).
14. provenance_certificate.pdf — eigenständiges PDF-Dokument — Herkunftszertifikat, das die Herkunfts- und Integritätskette des Beweises in benutzerfreundlicher Form zusammenfasst. Das Dokument enthält die Identifikation des Beweises, den über NTP synchronisierten Aufnahmezeitpunkt, den kryptographischen Hash des Inhalts, Informationen zur Erfassungsumgebung sowie die Ergebnisse aller durchgeführten forensischen Prüfungen (Automationserkennung, DNS-Verifikation, TLS-Zertifikatsvalidierung, Status der Zeitstempel usw.).
15. capture_video.webm (optionales Ergebnis) — Videoaufzeichnung des gesamten Erfassungsprozesses, die der Nutzer nach eigenem Ermessen aktivieren kann. Das Ergebnis dokumentiert den Erfassungsverlauf in Echtzeit und dient als ergänzender Beweis für die Existenz des Inhalts auf der jeweiligen Seite zum Zeitpunkt der Erfassung (besonders geeignet in Fällen, in denen der Dienst in sozialen Netzwerken verwendet wird).

Gegenstand dieses Rechtsgutachtens ist die Anerkennung der mittels ProofSnap erlangten Beweise durch Gerichte und Verwaltungsbehörden sowie die Beurteilung der Beweiskraft solcher Beweise. Das Rechtsgutachten wird aus der Perspektive des EU-Rechts unter Bezugnahme auf das tschechische Prozessrecht erstellt.

II. Grundlagen

Im Zusammenhang mit dem gegenständlichen Auftrag erhielt die Verfasserin vom Mandanten Zugangsdaten zum System ProofSnap. Der Verfasserin wurde somit die uneingeschränkte Nutzung des Dienstes ermöglicht. Zudem wurde die Verfasserin vom Mandanten auf dessen Website (getproofsnap.com) verwiesen.

Vom Mandanten wurden keine weiteren schriftlichen oder sonstigen Unterlagen zur Erstellung dieses Gutachtens übermittelt.

III. Gutachten

+420 733 555 958
office@sedlakovalegal.com
www.sedlakovalegal.cz

Für die Beurteilung der Beweiskraft von ProofSnap ist die Sache nicht ganz einfach. Zunächst ist nämlich zu bewerten, welches konkrete Ergebnis des Dienstes für das gerichtliche oder verwaltungsbehördliche Verfahren relevant ist. Für Zwecke der grundlegenden Beweisführung ist zweifellos primär das Ergebnis in Form des Dokuments „evidence.pdf" wichtig. Es handelt sich um einen Urkundenbeweis (vgl. § 416 ZPO), der dank seines Formats auch für IT-Laien — also für Richter, Richterassistenten, Sachbearbeiter von Verwaltungsbehörden und andere vergleichbare Personen — leicht lesbar ist.

Die Beweiserhebung in Bezug auf das Dokument „evidence.pdf" kann für die zuständigen Behörden in keiner Weise problematisch sein. Faktisch handelt es sich um eine Urkunde, in der eine elektronische Aufzeichnung zusammen mit weiteren Verifizierungsdaten des Dienstes — also z. B. Metadaten, Aufnahmedatum, Quell-URL usw. — wiedergegeben ist. In der Rechtspraxis ist es üblich, dass eine elektronische Aufzeichnung (z. B. der Stand einer Website) mittels eines „einfachen" Screenshots ermittelt (nachgewiesen) wird. Sowohl Gerichte als auch Verwaltungsbehörden akzeptieren solche Beweise in der Regel.

Hat eine Prozesspartei Bedenken hinsichtlich des Beweises mittels Screenshot, kann sie diesen Beweis durch einen Antrag auf Inaugenscheinnahme der Website (als Beweismittel gemäß § 371 ZPO) oder durch eine notarielle Tatsachenfeststellung gemäß § 20 Abs. 1 BNotO i. V. m. §§ 36 ff. BeurkG, in welcher der Notar den Zustand der Website (oder eines anderen Mediums) festhält, zusätzlich untermauern.

Der Nachteil dieser zusätzlichen Beweisformen besteht jedoch darin, dass der Beweis mit Verzögerung erhoben wird. Die Inaugenscheinnahme der Website erfolgt in der Regel erst in der mündlichen Verhandlung. Eine notarielle Tatsachenfeststellung kann nach den zeitlichen Möglichkeiten des jeweiligen Notars erfolgen (also mit einer Wartezeit von einigen Stunden bis zu mehreren Tagen). In keinem dieser Fälle kann der Beweis sofort erhoben werden, was in manchen Fällen zu fatalen Konsequenzen im Rechtsstreit in Form der Beweisfälligkeit führen kann. Der Grund liegt darin, dass der Inhalt der betreffenden Website in der Zwischenzeit geändert oder entfernt werden kann (ebenso kann elektronische Kommunikation in sozialen Netzwerken gelöscht werden usw.).

Im Falle der Beweisführung mittels notarieller Tatsachenfeststellung besteht ein weiterer Nachteil darin, dass die notarielle Tatsachenfeststellung ein relativ kostspieliges Mittel ist. Sie wird daher tatsächlich nur in Situationen genutzt, in denen das Ergebnis des gesamten Verfahrens vom Nachweis der elektronischen Aufzeichnung abhängt. Insbesondere bei umfangreichen Websites mit vielen Reitern, Abschnitten usw. kann die notarielle Tatsachenfeststellung bei deren Erfassung auf technische Beschränkungen stoßen und mitunter auch zur Unübersichtlichkeit des Endergebnisses führen.

Die Beweisführung mittels des Ergebnisses des Dienstes ProofSnap erscheint somit als geeignete und wirtschaftliche Alternative zum Nachweis einer elektronischen Aufzeichnung, die den Beweis durch Screenshot ergänzen oder ersetzen kann. In der Regel wird dabei das Dokument „evidence.pdf" vorgelegt.

+420 733 555 958
office@sedlakovalegal.com
www.sedlakovalegal.cz

In diesem Zusammenhang ist jedoch hervorzuheben, dass die Ergebnisse von ProofSnap im Vergleich zu notariellen Tatsachenfeststellungen hinsichtlich der Beweiskraft stets im Nachteil sein werden. Die notarielle Tatsachenfeststellung ist nämlich in der Regel eine öffentliche Urkunde (§§ 415, 437 ZPO), was bedeutet, dass bei ihr die Echtheit und Richtigkeit vermutet werden. Mit anderen Worten: Solange das Gegenteil nicht bewiesen ist, gilt die in der notariellen Tatsachenfeststellung festgehaltene Aufzeichnung als echt. Beweisrechtlich handelt es sich zudem um einen sogenannten Vollbeweis (§ 415 ZPO), was bedeutet, dass zum Nachweis einer Tatsache, für die eine gesetzliche Vermutung besteht, kein anderer Beweis als die öffentliche Urkunde, in der sie festgehalten ist, erforderlich ist.

Auch wenn Einwände gegen Echtheit und Richtigkeit beim Nachweis einer elektronischen Aufzeichnung kein besonders häufiges prozessuales Vorgehen der Verfahrensbeteiligten darstellen (zumindest nach der eigenen Praxis der Verfasserin), kann ein solcher Verlauf eines streitigen Verfahrens nie ausgeschlossen werden. Wird ein solcher Einwand gegen das primäre Dokument — „evidence.pdf" — erhoben, ist es erforderlich, dass die übrigen Ergebnisse des Dienstes die Echtheit und Richtigkeit des primären Dokuments zuverlässig nachweisen. Der Nutzer sollte daher darauf hingewiesen werden, dass er sämtliche Ergebnisse des Dienstes aufbewahren sollte und nicht nur dasjenige, mit dem er ursprünglich eine Tatsache bezeugt bzw. nachweist.

Die Beurteilung dieser übrigen Ergebnisse ist eine rein technische Angelegenheit (keine rechtliche), weshalb eine Beweisführung durch ein Sachverständigengutachten oder eine sachverständige Stellungnahme (durch einen Sachverständigen für Informations- und Kommunikationstechnologie oder Cybersicherheit) erforderlich sein wird.

In dieser Hinsicht ist die Eignung der Nutzung von OpenTimestamps, das eine unabhängige zeitliche Verankerung des Hashes über die Bitcoin-Blockchain ermöglicht, zweifellos zu begrüßen. Die auf der Blockchain und externer Verankerung basierende Architektur wirkt aus Sicht der Datenintegrität durchdacht; gleichwohl ist hier eine anschließende Bestätigung durch einen Sachverständigen auf diesem Gebiet bzw. einen anderen qualifizierten Fachmann erforderlich, der die Gegebenheiten bestätigen kann. Die Verfasserin ist der Auffassung, dass aus technischer Sicht eine Bestätigung erforderlich sein wird, dass das Tool OpenTimestamps ordnungsgemäß ausgeführt und in die Blockchain verankert wurde. Die bloße Existenz der Datei manifest.json.ots bedeutet nämlich für sich allein noch nicht zwingend eine endgültige Blockchain-Bestätigung. Wichtig wird auch die Robustheit und Größe der gewählten Blockchain-Lösung sein und somit auch die (Un-)Wahrscheinlichkeit einer möglichen Veränderung der in der Blockchain gespeicherten Daten sowie der technische Fortschritt und neue Technologien (z. B. Quantenprozessoren und deren Leistungsbedrohung für Blockchain-Technologien). Dies sind jedoch eher theoretisch-technische Überlegungen der Verfasserin. Für die rechtliche Praxis ist hervorzuheben, dass die nachträgliche Vorlage der Dateien screenshot.jpeg, metadata.json, manifest.json, manifest.sig, manifest.json.ots usw. beim Gericht bzw. bei der Verwaltungsbehörde aus beweisrechtlicher Sicht nichts bringt (auch wenn dies ein notwendiger Schritt sein wird), da der zuständige Richter bzw. Sachbearbeiter solche Dateien nicht entschlüsseln und auf deren Grundlage keine qualifizierte Schlussfolgerung treffen kann. Gerade aus diesem Grund wird die Beteiligung eines Sachverständigen stets erforderlich sein.

+420 733 555 958
office@sedlakovalegal.com
www.sedlakovalegal.cz

Ein Sachverständiger kann im Rahmen seiner fachlichen Tätigkeit überprüfen, ob das Beweispaket ProofSnap die ursprünglich vorgelegte Aufzeichnung bestätigt (auch hinsichtlich des Erfassungszeitpunkts) und somit, ob die Darstellung im Dokument evidence.pdf zutreffend ist. Ein Sachverständigengutachten stellt jedoch in der Regel eine erhebliche Kostensteigerung dar.

Eine gewisse Alternative kann daher die im Rahmen des Dienstpakets erstellte Videoaufzeichnung darstellen, wobei deren Möglichkeiten in gewisser Weise begrenzt sind. Die Videoaufzeichnung selbst kann dem Richter bzw. Sachbearbeiter naturgemäß nicht bei der qualitativen Auswertung technischer Dateien helfen.

Wenn der Nutzer des Dienstes beispielsweise eine Konversation in einem sozialen Netzwerk aufzeichnen möchte, wird sich eine solche Aufzeichnung kaum von anderen Aufzeichnungen (außerhalb des Dienstes) unterscheiden, mit denen bestimmte Tatsachen seit langem zu Beweiszwecken festgehalten werden. Es handelt sich zwar nicht um eine besonders häufige Methode in der Praxis, doch wird sie in Einzelfällen genutzt. De facto handelt es sich um die Aufzeichnung des Bildschirms mittels einer Kamera, die den Verlauf auf dem Bildschirm bei gleichzeitiger Anzeige der aktuellen Titelseite einer Online-Tageszeitung (z. B. tagesschau.de) zwecks zeitlicher Verankerung filmt.

Andererseits bedeutet dies nicht, dass das Ergebnis aus capture_video.webm keine Berechtigung hätte und sich nicht praktisch durchsetzen könnte. Die Verfasserin sieht dessen Vorteil in seinem überzeugenden Potenzial. Sollte die Gegenseite aus irgendeinem Grund tatsächlich die Echtheit der Datei evidence.pdf bestreiten, kann die betreffende Aufzeichnung ein ausreichender Anreiz sein, von einer sachverständigen Untersuchung abzusehen (und so die Kosten nicht unnötig zu erhöhen), da offensichtlich wäre, dass ein solches Vorgehen unwirtschaftlich und sinnlos ist. Bei fehlender Videoaufzeichnung ist demgegenüber zu erwarten, dass Einwände der Gegenseite gegen die Echtheit des Dokuments häufiger auftreten. Das Ergebnis aus capture_video.webm minimiert somit den Raum für Einwände, die sich auf die Frage richten, ob der erfasste Inhalt zum jeweiligen Zeitpunkt tatsächlich so dargestellt wurde, wie im Dokument evidence.pdf wiedergegeben.

Dieses Werkzeug eignet sich zugleich zweifellos besonders bei dynamischen Inhalten (insbesondere in sozialen Netzwerken, bei interaktiven Elementen von Websites, animierten Inhalten oder bei der Wiedergabe von Videos), bei denen ein statischer Screenshot das Wesen des dargestellten Inhalts nicht vollständig erfasst. Aus prozessualer Sicht handelt es sich um einen ergänzenden Augenscheinsbeweis (§ 371 ZPO). Er erhöht für sich allein nicht den Beweiswert der Datei evidence.pdf, sondern deren Glaubwürdigkeit.

In diesem Zusammenhang hat auch das Herkunftszertifikat (die Datei provenance_certificate.pdf), das Bestandteil des Beweispakets ist, praktische Bedeutung. Im Unterschied zu technischen Dateien, deren Inhalt für eine Laienbewertung durch Gericht oder Verwaltungsbehörde nicht unmittelbar verwertbar ist, fasst das Herkunftszertifikat die Ergebnisse aller durchgeführten forensischen Prüfungen in einer benutzerfreundlichen Form zusammen. Auch wenn bei konfliktreicheren Streitigkeiten zur autoritativen Bestätigung technischer Aspekte weiterhin in der Regel eine sachverständige Stellungnahme oder ein Sachverständigengutachten erforderlich sein wird, ermöglicht das

+420 733 555 958
office@sedlakovalegal.com
www.sedlakovalegal.cz

Herkunftszertifikat der im Verfahren entscheidenden Stelle eine grundlegende Orientierung in den Ergebnissen der technischen Prüfungen, ohne sofort einen Sachverständigen hinzuziehen zu müssen, und liefert zugleich eine konsistente strukturierte Grundlage, von der ein Sachverständiger anschließend ausgehen kann.

In der vorliegenden Angelegenheit spielt die Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (sog. „eIDAS") eine bedeutende Rolle, die einen rechtlichen Rahmen für die Anforderungen an qualifizierte elektronische Signaturen, Zeitstempel, elektronische Siegel und weitere Vertrauensdienste schafft, welche die rechtliche Anerkennung elektronischer Dokumente und Transaktionen sicherstellen.

Aus Sicht der rechtlichen Relevanz ist es erforderlich, dass der im Rahmen des Dienstes verwendete Zeitstempel die in der eIDAS-Verordnung festgelegten Anforderungen erfüllt, das heißt, dass er:

- Datum und Uhrzeit derart mit den Daten verbindet, dass die Möglichkeit einer unbemerkten Veränderung der Daten nach vernünftigem Ermessen ausgeschlossen ist,
- auf einer korrekten, mit der koordinierten Weltzeit verbundenen Zeitquelle beruht und
- von einem qualifizierten Vertrauensdiensteanbieter gewährleistet wird.

Im Übrigen sieht Art. 41 eIDAS ausdrücklich vor: „Einem elektronischen Zeitstempel darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil er in elektronischer Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Zeitstempel erfüllt."

Wird ein Zeitstempel im Einklang mit den eIDAS-Vorschriften ausgestellt, gewährt er eine starke Rechtssicherheit in gerichtlichen oder verwaltungsbehördlichen Verfahren.

Über das Vorgenannte hinaus ist zu ergänzen, dass eIDAS zwischen einem „gewöhnlichen" elektronischen Zeitstempel und einem qualifizierten elektronischen Zeitstempel unterscheidet. Während auch ein nicht qualifizierter Zeitstempel nicht allein deshalb zurückgewiesen werden darf, weil er elektronisch ist, genießt der qualifizierte Zeitstempel ein höheres Maß an Rechtsschutz, da mit ihm die Vermutung der Richtigkeit des angegebenen Datums und der Uhrzeit sowie der Integrität der bezogenen Daten verbunden ist. Praktisch bedeutet dies, dass ProofSnap, sofern es im konkreten Fall den Zusammenhang mit einem qualifizierten Vertrauensdienst (z. B. einem qualifizierten Zeitstempel, der von einem qualifizierten Vertrauensdiensteanbieter ausgestellt wurde) nachweisen kann, die prozessuale Position des Beweisführers erheblich stärkt, da es für die Gegenseite schwieriger sein wird, den Aufnahmezeitpunkt und die Unveränderlichkeit des Inhalts erfolgreich anzuzweifeln.

Aus den Unterlagen des Mandanten ist abzuleiten, dass der Dienst zwei einander ergänzende Mechanismen zur zeitlichen Verankerung der Aufzeichnung einsetzt:
(i) einen qualifizierten elektronischen Zeitstempel im Sinne von Art. 42 eIDAS (Datei manifest.json.tsr), ausgestellt von der slowakischen Gesellschaft Disig, a.s., die Stand heute als qualifizierter Vertrauensdiensteanbieter in der EU Trusted List eingetragen ist. Für diesen Zeitstempel gilt nach Art. 41 Abs. 2 eIDAS unmittelbar die gesetzliche Vermutung der Richtigkeit des Datums und der Uhrzeit sowie der Integrität der mit Datum und Uhrzeit verbundenen Daten; diese Vermutung wirkt

+420 733 555 958
office@sedlakovalegal.com
www.sedlakovalegal.cz

unmittelbar in allen 27 EU-Mitgliedstaaten;
(ii) eine OpenTimestamps-Verankerung über die Bitcoin-Blockchain (Datei manifest.json.ots), die einen dezentralen und vom Anbieter unabhängig überprüfbaren Echtheitsnachweis hinsichtlich des Erfassungszeitpunkts liefert. Diese Verankerung erfüllt für sich allein nicht alle formalen Anforderungen an einen qualifizierten elektronischen Zeitstempel im Sinne von Art. 42 eIDAS, da kein qualifizierter Vertrauensdiensteanbieter beteiligt ist und die Bitcoin-Blockchain nicht direkt mit einer zertifizierten, an die koordinierte Weltzeit angebundenen Zeitquelle verknüpft ist; sie kann gleichwohl im Rahmen der freien Beweiswürdigung (§ 286 ZPO) als gewichtiger ergänzender Echtheitsbeweis dienen.
Die Kombination beider Mechanismen verleiht dem Beweispaket sowohl die durch eIDAS gewährte gesetzliche Vermutung als auch eine vom Anbieter unabhängige, blockchainbasierte Verifizierbarkeit (siehe unten).

Zugleich ist jedoch darauf hinzuweisen, dass auch eine technisch robuste Lösung (Hashing, Signaturen, Verkettung von Logs, OpenTimestamps usw.) für sich allein nicht alle Arten von Einwänden ausräumt, die im Verfahren erhoben werden können. Typischerweise kann (i) die Identität der Quelle und der Kontext der erfassten Darstellung in Frage gestellt werden (z. B. ob es sich um öffentlich zugänglichen Inhalt handelte oder ob der Inhalt im Gegenteil privater Natur war), (ii) die Berechtigung zur Erlangung der Aufzeichnung (z. B. Eingriff in Rechte Dritter, Verletzung von Betriebsgeheimnissen oder unbefugter Zugriff) oder (iii) die inhaltliche Richtigkeit des erfassten Inhalts. ProofSnap stärkt primär den Nachweis der Existenz und Gestalt eines Inhalts zu einem bestimmten Zeitpunkt (Integrität und Authentizität der Aufzeichnung), nicht notwendigerweise den Nachweis der materiellen Wahrheit der in der erfassten Darstellung enthaltenen Aussagen; auf diese Unterscheidung sollte im Verfahren hingewiesen werden.

Die Ergebnisse des Dienstes genießen somit die Vermutung der Richtigkeit von Datum, Uhrzeit und Datenintegrität gemäß Art. 41 Abs. 2 eIDAS, was zweifellos ihre Beweiskraft hinsichtlich des Nachweises des Aufnahmezeitpunkts und der Unveränderlichkeit des erfassten Inhalts stärkt und im Rahmen der freien Beweiswürdigung (§ 286 ZPO) durch das Gericht zu berücksichtigen ist; zugleich verringert sie die Notwendigkeit der Beteiligung eines Sachverständigen allein zur Bestätigung der zeitlichen Verankerung des Beweises. Es ist jedoch darauf hinzuweisen, dass es sich um einen relativ neuen Typ von Beweismittel handelt, zu dem bislang keine gefestigte Rechtsprechung tschechischer Gerichte besteht. Wie sich die Entscheidungspraxis entwickeln wird, bleibt eine offene Frage; es kann nicht ausgeschlossen werden, dass das Gericht im Einzelfall (insbesondere im Hinblick auf die Natur des konkreten Streits und etwaige Einwände der Gegenseite) eine ergänzende Beweisführung auch über die gesetzliche Vermutung nach Art. 41 Abs. 2 eIDAS hinaus verlangen wird.

Schlussfolgerung

Aus den vorstehenden Ausführungen ergibt sich, dass die Ergebnisse des Dienstes ProofSnap aus Sicht des tschechischen Prozessrechts und des EU-Rechtsrahmens allgemein als Beweismittel in jeder Art von Verfahren verwendbar sind. Das praktisch am besten verwertbare Ergebnis wird in der Regel das Dokument (die Datei) evidence.pdf sein, das für Gerichte und Verwaltungsbehörden verständlich und prozessual leicht als Urkundenbeweis erhoben werden kann. Im Übrigen ist es in

+420 733 555 958
office@sedlakovalegal.com
www.sedlakovalegal.cz

der gängigen Praxis allgemein akzeptiert, den Stand von Websites oder elektronischer Kommunikation mittels „Screenshots" nachzuweisen.

Hinsichtlich der Beweiskraft ist jedoch zu betonen, dass evidence.pdf eine Privaturkunde (§ 416 ZPO) ist, bei der im Falle eines Einwands gegen Echtheit oder Richtigkeit die Beweislast bei der vorlegenden Partei liegt. ProofSnap bietet in dieser Hinsicht einen erheblichen Mehrwert: Es ermöglicht, den erfassten Inhalt zusammen mit technischen Metadaten und kryptographischen Elementen (Hashing, Signatur, Log-Ketten und zeitliche Verankerung) aufzubewahren, die — insbesondere unter Beteiligung eines Sachverständigen — dem Nachweis der Integrität, Authentizität und zeitlichen Einordnung der Aufzeichnung dienen können. Im Vergleich zur notariellen Tatsachenfeststellung wird ProofSnap jedoch stets eine schwächere Position innehaben, da die notarielle Tatsachenfeststellung eine öffentliche Urkunde ist, bei der die Echtheit vermutet wird. Daher ist damit zu rechnen, dass bei konfliktreicheren Streitigkeiten zur Bestätigung der technischen Aspekte eine sachverständige Stellungnahme oder ein Sachverständigengutachten erforderlich sein kann.

Zugleich gilt, dass auch die technisch robuste Lösung ProofSnap primär den Nachweis der Existenz und Gestalt eines Inhalts zu einem bestimmten Zeitpunkt (Integrität und Authentizität der Aufzeichnung) stärkt, ohne dass damit ohne Weiteres die materielle Wahrheit der in der erfassten Darstellung enthaltenen Aussagen oder die Frage der Rechtmäßigkeit der Erfassung der Aufzeichnung nachgewiesen wäre. Im Verfahren kann daher weiterhin die Beurteilung des Kontexts des erfassten Inhalts (z. B. Öffentlichkeit/Privatheit, Identität der Quelle) sowie die Rechtmäßigkeit der Erlangung der Aufzeichnung aus Sicht der Rechte Dritter relevant sein.

Es ist begründet anzunehmen, dass mit dem Aufkommen generativer KI, die sich ständig weiterentwickelt, die Beweisführung mittels „Screenshots" von Websites nicht mehr ausreichen wird und sich die Fälle häufen werden, in denen die Echtheit solcher Urkunden bestritten wird. Ohne Inanspruchnahme des Dienstes kann der Beweisführer die Echtheit der Urkunde dann nur noch durch Augenschein (§ 371 ZPO) oder eine notarielle Tatsachenfeststellung (§ 20 Abs. 1 BNotO i. V. m. §§ 36 ff. BeurkG) nachweisen. Ein solches Vorgehen versetzt ihn jedoch in eine prozessuale Nachteilssituation, da der Bestreitende den Einwand in der Regel erst dann erhebt, wenn er sich sicher ist, dass der Beweisführer mit diesen zusätzlichen Beweisen nichts erreichen wird (z. B. durch Änderung der Website, Löschung der Konversation usw.).

Ebenso ist zu ergänzen, dass bei der Beurteilung der Beweiskraft auch die Prozessstrategie selbst und die Art der Beweisvorlage Bedeutung haben werden. Als praktisch zweckdienlich erscheint es, (i) evidence.pdf als primäre Urkunde vorzulegen, (ii) zugleich das vollständige Beweispaket dem Gericht zur Verfügung zu stellen (z. B. auf einem elektronischen Datenträger) und (iii) die Erhebung eines Sachverständigengutachtens oder einer sachverständigen Stellungnahme zu beantragen, das bzw. die die Prinzipien der Hashes, Signaturen und der zeitlichen Verankerung verständlich erläutert und die Verifikation des konkreten Pakets vornimmt. Ein solches Vorgehen minimiert das Risiko, dass der jeweilige Sachverhalt durch den Dienst nicht hinreichend nachgewiesen werden könnte.

ProofSnap kann als praktisch verwertbares und wirtschaftlich effizientes Werkzeug für die Sicherung und Aufbewahrung elektronischer Beweise angesehen werden, das prozessual

+420 733 555 958
office@sedlakovalegal.com
www.sedlakovalegal.cz

verfahrensübergreifend einsetzbar ist und — bei ordnungsgemäßer Aufbewahrung des vollständigen Pakets und geeigneter prozessualer Vorgehensweise — den Beweiswert üblicherweise vorgelegter elektronischer Aufzeichnungen erheblich stärken kann. In Situationen, in denen mit einem Streit über Echtheit oder Integrität zu rechnen ist, ist jedoch davon auszugehen, dass die volle Beweiskraft in der Praxis in der Regel eine fachliche technische Verifikation (durch einen Sachverständigen oder qualifizierten Fachmann) erfordert.

Abschließend kann die Verfasserin feststellen, dass sie den Dienst in einigen Fällen bereits im Rahmen ihrer anwaltlichen Praxis genutzt hat, jedoch Stand heute noch keine Rückmeldung der zuständigen Stellen (in diesem Fall Gericht und Gerichtsvollzieheramt) vorliegt, die dem Mandanten mitgeteilt werden könnte. Angesichts des Fehlens einer gefestigten Entscheidungspraxis zu dieser Art von Beweismittel kann nicht vorab vorhergesagt werden, wie das jeweilige Organ die Ergebnisse des Dienstes bewerten wird. Die Ausgangsposition der vorlegenden Partei wird jedoch durch die gesetzliche Vermutung der Richtigkeit von Datum, Uhrzeit und Datenintegrität nach eIDAS erheblich gestärkt, die im Hinblick auf die Verwendung eines qualifizierten elektronischen Zeitstempels für die Ergebnisse des Dienstes unmittelbar kraft Gesetzes Anwendung findet. Es kann somit begründet erwartet werden, dass mit der zunehmenden Verbreitung vergleichbarer Werkzeuge die Akzeptanz dieser Art von Beweis seitens der Gerichte und Verwaltungsbehörden allmählich steigen wird.

IV. Vorbehalt

Die vorstehenden Schlussfolgerungen geben die Rechtsauffassung der Verfasserin wieder, sind nicht rechtsverbindlich und dienen weder der Weitergabe an Dritte noch der Verwendung in Gerichts- oder sonstigen Verfahren.