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

LEGAL OPINION — THE PROOFSNAP SYSTEM AS A MEANS OF EVIDENCE AND ASSESSMENT OF ITS EVIDENTIARY VALUE

Client: **Software Innovations Group LLC**
registered office: Sharjah Media City (SHAMS), Al Messaned, Al Bataeh, Sharjah, United Arab Emirates

(hereinafter also the "Client")

Author:SEDLAKOVA LEGAL s.r.o.
Company ID (IČO): 056 69 871
registered office: Purkyňova 648/125, Medlánky, 612 00 Brno, Czech Republic
registered in the Commercial Register kept by the Regional Court in Brno,
Section C, File No. 97278

(hereinafter also the "Author")

Date of issue: 21 April 2026

I. Mandate

SEDLAKOVA LEGAL s.r.o. was approached by Mr Radim Motyčka, acting on behalf of Software Innovations Group LLC, with a request to prepare a legal opinion (analysis) on the "ProofSnap" system operated by that company (hereinafter also "ProofSnap" or the "Service"). The Service captures any electronic display (e.g. a website, social-media communication, etc.) by means of a digital recording at a specific moment in time, so that the integrity and authenticity of the captured display can subsequently be verified.

ProofSnap acquires and stores the captured content together with the relevant technical data (e.g. the time of capture, identification of the source, file identifiers and other metadata) and at the same time secures it against subsequent changes by means of cryptographic mechanisms, thereby allowing independent verification that the recording has not been tampered with since the moment of capture.

The output of the Service is an "evidence package" containing the following files:

1. screenshot.jpeg — an image of the visual snapshot of the website (electronic display).
2. metadata.json — contextual information about the evidence (timestamp, URL and browser information).
3. manifest.json — a list of all evidence files and their hashes for verifying the integrity of the package.
4. manifest.sig — a digital signature of the manifest, ensuring authenticity and integrity.
5. manifest.json.ots — an OpenTimestamps proof for the manifest.json file.

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

6. manifest.json.tsr — a qualified electronic timestamp within the meaning of Article 42 of the eIDAS Regulation, issued by Disig, a.s. (RFC 3161 ASN.1 TimeStampToken format).
7. eidas_validation.json — validation metadata for the qualified eIDAS timestamp (Disig).
8. publickey.pem — the public key for verifying the digital signature of the manifest.
9. evidence.pdf — a PDF document containing all evidence files for ease of sharing and review.
10. domtextcontent.txt — the textual content extracted from the DOM of the web page.
11. forensic_log.json — a forensic log compliant with ISO/IEC 27037 with a hash chain recording every capture operation.
12. chain_of_custody.json — a chain-of-custody document including device integrity, NTP time verification and evidence binding.
13. page.html — the complete HTML content of the captured website (electronic display).
14. provenance_certificate.pdf — a stand-alone PDF certificate that summarises the chain of origin and the integrity of the evidence in a user-friendly form. It contains identification of the evidence, the time of capture synchronised via NTP, the cryptographic hash of the content, information about the capture environment and the results of all forensic checks performed (automation detection, DNS verification, TLS certificate validation, timestamp status, etc.).
15. capture_video.webm (optional output) — a video recording of the entire evidence-capture process, which the user may activate at will. The output captures the course of acquisition in real time and serves as supplementary evidence of the existence of the content on the given page at the moment of capture (particularly suitable when the Service is used for social-media content).

The subject of this legal opinion is the admissibility of evidence acquired through ProofSnap before courts and administrative authorities, and an assessment of the evidentiary value of such evidence. The opinion is drafted from the perspective of EU law and not from the perspective of the law of individual Member States.

II. Materials

In connection with this mandate, the Author received from the Client access credentials to the ProofSnap system. The Author was therefore able to use the Service without any limitation. The Client further referred the Author to its website — getproofsnap.com.

No documentary or other materials were provided by the Client for the purpose of preparing this opinion.

III. Opinion

Assessing the evidentiary value of ProofSnap is not entirely straightforward. First, it is necessary to consider which specific output of the Service is relevant for judicial or administrative proceedings. For basic evidentiary purposes the most important output is undoubtedly the “evidence.pdf” document. This is documentary evidence which, thanks to its format, is easily readable even by non-IT specialists — that is, by judges, judicial assistants, officers of administrative authorities and similar persons.

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

The presentation of evidence — the “evidence.pdf” document — should not pose any difficulty for the relevant authorities. Factually it is a document that displays an electronic record together with further verification data of the Service, e.g. metadata, the date of capture, the URL of the source, etc. In legal practice it is entirely common for an electronic record (e.g. the state of a website) to be ascertained (proven) by way of an ordinary screenshot, and courts and administrative authorities generally accept such evidence.

Where a party to proceedings has concerns about proof by means of a screenshot, that evidence may be further supported by a motion for judicial inspection of the website (as a means of evidence) or by a notarial deed in which the notary records the state of the website (or other medium). (In Czech law, a notarial deed is a public document with a statutory presumption of authenticity and accuracy.)

The disadvantage of these additional methods is, however, that the evidence is taken with a delay. A judicial inspection of a website is usually carried out only at the oral hearing. A notarial deed can only be drawn up subject to the notary's availability (typically several hours to several days). In none of these cases is it possible to take the evidence immediately, which in some cases can lead to fatal consequences in the form of a failure to discharge the burden of proof. The reason is that during the intervening period the content of the website concerned may be altered or removed (electronic communications on social media may likewise be deleted, etc.).

When proving facts by means of a notarial deed, an additional disadvantage is that it is a relatively expensive instrument. It is therefore generally only used in situations where the outcome of the entire proceedings depends on demonstrating the electronic record. Particularly in the case of large websites with multiple tabs, sections, etc., the notarial deed may also encounter technical limitations on capture and at times lacks clarity in its final form.

Proving facts by means of a ProofSnap output therefore appears to be a suitable and economical alternative for demonstrating an electronic record, which complements or replaces a screenshot. As a rule, the document submitted will be the “evidence.pdf” file.

In this context, however, it must be emphasised that ProofSnap outputs will always be at a disadvantage compared to notarial deeds in terms of evidentiary value. A notarial deed is generally a public document, which means that its authenticity and accuracy are presumed. In other words, until the contrary is proved, the record contained in a notarial deed is regarded as authentic. Moreover, from an evidentiary perspective it constitutes so-called “full evidence”, meaning that to prove a fact for which a presumption of existence is laid down, no further evidence is needed beyond the public document recording it.

Although objections to authenticity and accuracy in cases of proving an electronic record are not a particularly frequent procedural step taken by parties (at least in the Author's own practice), such procedural posture cannot, however, be ruled out. If, therefore, such an objection is raised against the primary document — “evidence.pdf” — it is essential that the other outputs of the Service reliably demonstrate the authenticity and accuracy of that primary document. The user should therefore be

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

advised to retain all outputs of the Service and not only the one by which they originally certified or proved a particular fact.

The assessment of these other outputs is, however, a purely technical (not legal) matter, and it will therefore be necessary to proceed by means of an expert report or expert statement (provided by an expert in information and communication technology or cybersecurity).

In this respect, the use of OpenTimestamps — which allows independent temporal anchoring of a hash via the Bitcoin blockchain — can undoubtedly be welcomed. The blockchain-based architecture and external anchoring appears well thought through from a data-integrity perspective; what is necessary, however, is subsequent confirmation by an expert in the given field, or by another qualified specialist who can confirm the relevant facts. The Author is of the view that, from a technical standpoint, it will be necessary to confirm that the OpenTimestamps tool was duly executed and anchored to the blockchain. The mere existence of the manifest.json.ots file does not in itself necessarily entail final blockchain confirmation. The robustness and size of the chosen blockchain solution will also matter — and therefore the likelihood (or unlikelihood) of altering data stored on the blockchain — as will technical progress and new technologies (e.g. quantum processors and the cryptanalytic threat they pose to current blockchain technologies). These are, however, theoretical and technical considerations on the part of the Author. For legal practice itself, it is essential to emphasise that the subsequent submission to the court or administrative authority of the screenshot.jpeg, metadata.json, manifest.json, manifest.sig, manifest.json.ots and similar files will, from an evidentiary perspective, add nothing on its own (although it will be a necessary step), as the relevant judge or officer will not be able to decrypt those files and draw a qualified conclusion from them. For that very reason the involvement of an expert will always be necessary.

In the course of their professional activity, an expert can verify that the ProofSnap evidence package corresponds to the originally submitted record (including with regard to the time of capture) and therefore that the display in the evidence.pdf document is truthful. An expert report, however, generally entails a significant increase in costs.

An alternative may therefore be the video recording produced as part of the Service package, although its capabilities are in some respects limited. The video itself (by its very nature) cannot help a judge or administrative officer with the qualitative evaluation of technical files.

If a user of the Service intends to record, for example, a conversation on social networks, such a recording will not differ much from other (non-Service) recording methods that have been used to capture certain facts for evidentiary purposes for some time. While not a particularly frequent method in practice, it is used in isolated cases. In essence, it amounts to filming the screen with a camera that captures what is happening on screen while simultaneously displaying the current front page of an online news website (e.g. seznam.cz) to anchor the recording in time.

On the other hand, this does not mean that the capture_video.webm output is without merit and could not be used in practice. The Author sees its advantage in its persuasive potential. Should the opposing party genuinely dispute the authenticity, for any reason, of the evidence.pdf file, the recording may be

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

sufficient motivation not to commission an expert examination (and unnecessarily increase costs), as it would be apparent that such a course is uneconomic and pointless. In the absence of a video recording, objections to the authenticity of the document can be expected to be more frequent. The capture_video.webm output therefore minimises the scope for objections regarding whether the captured content was actually displayed at the given moment in the way presented in the evidence.pdf document.

This tool is also undoubtedly suitable in particular for dynamic content (especially on social networks, with interactive web-page elements, animated content or video playback), where a static screenshot does not fully capture the substance of the displayed content. Procedurally, this is a supplementary form of real evidence. It does not, by itself, increase the evidentiary weight of the evidence.pdf file, but rather its credibility.

In this context, the provenance certificate (the provenance_certificate.pdf file) included in the evidence package also has practical significance. Unlike the technical files, whose contents are not directly usable for non-expert assessment by a court or administrative authority, the provenance certificate summarises the results of all forensic checks performed in a user-friendly form. Although in more contentious disputes an expert statement or expert report will, as a rule, still be required for authoritative confirmation of technical aspects, the provenance certificate enables the deciding authority to gain a basic understanding of the results of the technical checks without the immediate need to involve an expert, and at the same time provides a consistent, structured basis on which an expert can subsequently rely.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (the so-called eIDAS Regulation) plays a central role in this matter, ensuring the legal recognition of electronic documents and transactions.

From a legal standpoint, the timestamp used within the Service must satisfy the requirements laid down by the eIDAS Regulation, namely:

- it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;
- it is based on an accurate time source linked to Coordinated Universal Time (UTC); and
- it is guaranteed by a qualified trust service provider.

Article 41 of the eIDAS Regulation expressly provides: “An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp.”

Where a timestamp is issued in accordance with the rules of the eIDAS Regulation, it provides strong legal certainty in judicial and administrative proceedings.

Furthermore, the eIDAS Regulation distinguishes between an “ordinary” electronic timestamp and a qualified electronic timestamp. Whereas a non-qualified timestamp must not be denied legal effect

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

solely because it is electronic, a qualified electronic timestamp enjoys an enhanced level of legal protection because it carries a presumption of accuracy of the date and time it indicates and of the integrity of the data to which the date and time are linked. In practical terms, this means that if ProofSnap can in a particular case demonstrate the involvement of a qualified trust service (e.g. a qualified timestamp issued by a qualified trust service provider), this significantly strengthens the procedural position of the party submitting the evidence, because it will be more difficult for the opposing party to successfully challenge the moment of capture and the immutability of the content.

From the materials provided by the Client it can be inferred that the Service uses two complementary mechanisms for the temporal anchoring of the record:
(i) a qualified electronic timestamp within the meaning of Article 42 of the eIDAS Regulation (the manifest.json.tsr file), issued by the Slovak company Disig, a.s., which is, as of the date hereof, listed as a qualified trust service provider in the EU Trusted List. The statutory presumption of accuracy of the date and time, as well as of the integrity of the data linked to the date and time under Article 41(2) of the eIDAS Regulation, applies directly to this timestamp; this presumption operates directly in all 27 EU Member States;
(ii) anchoring through OpenTimestamps on the Bitcoin blockchain (the manifest.json.ots file), which provides a decentralised, provider-independent verifiable proof of authenticity as regards the moment the record was made. This anchoring does not by itself satisfy all the formal requirements for a qualified electronic timestamp within the meaning of Article 42 of the eIDAS Regulation, since no qualified trust service provider participates in it and the Bitcoin blockchain is not directly connected to a certified accurate time source linked to UTC; within the framework of free evaluation of evidence, however, it can serve as a significant supplementary proof of authenticity.
The combination of both mechanisms provides the evidence package with both the statutory presumption afforded by the eIDAS Regulation and a provider-independent, blockchain-verifiable check (see below).

At the same time, however, it must be pointed out that even a technically robust solution (hashing, signatures, log chaining, OpenTimestamps and the like) does not in itself address all types of objection that may be raised in proceedings. Typical challenges may concern (i) the identity of the source and the context of the captured display (e.g. whether it was publicly available content or, on the contrary, content of a private nature), (ii) the lawfulness of the manner in which the recording was obtained (e.g. interference with the rights of third parties, breach of trade secret or unauthorised access), or (iii) the substantive truthfulness of the captured content. ProofSnap primarily strengthens the proof of the existence and form of the content over time (the integrity and authenticity of the record), and not necessarily the proof of the material truth of statements contained in the captured display; this distinction should be emphasised in the proceedings.

The outputs of the Service therefore enjoy the presumption of accuracy of the date, time and integrity of data under Article 41(2) of the eIDAS Regulation, which undoubtedly strengthens their evidentiary value in demonstrating the moment of capture and the immutability of the captured content, and at the same time reduces the need to involve an expert solely to confirm the temporal anchoring of the evidence. It must, however, be noted that this is a relatively new type of means of evidence to which no settled case law of the Czech courts has yet developed. How decision-making practice will evolve

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

thus remains an open question, and it cannot be ruled out that, in an individual case, a court (particularly in light of the nature of the specific dispute and any objections raised by the opposing party) will require additional evidence beyond the statutory presumption under Article 41(2) of the eIDAS Regulation.

Conclusion

From the foregoing it follows that the outputs of the ProofSnap service are, from the perspective of Czech procedural law and the EU legal framework, generally usable as means of evidence in any type of proceedings. The most readily usable output will, as a rule, be the evidence.pdf document, which is intelligible to courts and administrative authorities and procedurally easy to present as documentary evidence. After all, in everyday practice, proving the state of a website or of electronic communications by means of "screenshots" is commonly accepted.

From the perspective of evidentiary value, however, it must be emphasised that evidence.pdf is a private document, in respect of which the burden of proof rests on the submitting party in the event of an objection to its authenticity or accuracy. ProofSnap provides significant added value in this regard: it allows the captured content to be preserved together with technical metadata and cryptographic elements (hashing, signature, log chains and temporal anchoring) which can — particularly with the involvement of an expert — serve to demonstrate the integrity, authenticity and temporal placement of the record. Compared to a notarial deed, however, ProofSnap will always be in a weaker position, because a notarial deed is a public document for which authenticity is presumed. It is therefore necessary to expect that, in more contentious disputes, an expert statement or expert report may be required to confirm technical aspects.

At the same time, even a technically robust ProofSnap solution primarily strengthens proof of the existence and form of content at a given time (the integrity and authenticity of the record), and not, without further evidence, the substantive truthfulness of statements contained in the captured display or the question of whether the recording was lawfully obtained. The assessment of the context of the captured content (e.g. public vs. private, identity of the source) and of the lawfulness of obtaining the recording from the perspective of third-party rights may therefore continue to be relevant in the proceedings.

It is reasonable to assume that, with the rise of generative AI — which is constantly improving — proof by means of website "screenshots" will no longer be sufficient, and that cases in which the authenticity of such documents is challenged will increase. Without the use of the Service, the party submitting such evidence will be able to demonstrate authenticity only by way of judicial inspection or a notarial deed. Such an approach, however, places that party in a procedural disadvantage, because the objecting party will, as a rule, raise the objection only once it has assured itself that those additional means of evidence will be of no avail to the submitting party (e.g. due to modification of the website, deletion of the conversation, etc.).

It is also worth adding that, when assessing evidentiary value, the procedural strategy and the manner of presenting the evidence will also matter. As a practical matter, the following appears effective: (i) submitting evidence.pdf as the primary document; (ii) at the same time making the

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

complete evidence package available to the court (e.g. on an electronic data carrier); and (iii) proposing that evidence be taken in the form of an expert report or expert statement that will explain the principles of hashes, signatures and temporal anchoring in an intelligible manner and verify the specific package. This approach minimises the risk that the relevant facts would not be sufficiently demonstrated by the Service.

ProofSnap can be regarded as a practically usable and economically efficient tool for securing and preserving electronic evidence — procedurally usable across types of proceedings, and capable (provided that the complete package is properly preserved and the procedural approach is suitably chosen) of significantly strengthening the evidentiary value of commonly submitted electronic records. In situations where a dispute about authenticity or integrity can be expected, however, it must be borne in mind that, in practice, the full evidentiary value will, as a rule, require expert technical verification (by an expert or other qualified specialist).

By way of conclusion, the Author may state that, in some cases, the Service has already been used within the Author's legal practice; as of the date hereof, however, the Author has no feedback available from the relevant authorities (in the given case the court and the bailiff's office) that could be communicated to the Client. In view of the absence of settled case law on this type of means of evidence, it is not possible to predict in advance how a particular authority will evaluate the outputs of the Service. The starting procedural position of the submitting party is, nevertheless, significantly strengthened by the statutory presumption of accuracy of the date, time and integrity of data under the eIDAS Regulation, which, in light of the use of a qualified electronic timestamp, applies to the outputs of the Service directly by operation of law. It can therefore reasonably be expected that, with the growing adoption of similar tools, acceptance of this type of evidence by courts and administrative authorities will gradually strengthen.

IV. Disclaimer

The conclusions set out above express the legal opinion of the Author. They are not legally binding and are not intended for transmission to third parties or for use in judicial or other proceedings.