Dr. René Sasse
RECHTSANWALT

Dr. René Sasse
Rechtsanwalt

Chemnitzer Str. 126
44139 Dortmund

Telefon 02 31.130 90 33
Mobil 01 76.21 05 22 46
Telefax 02 31.799 23 15

E-Mail info@rechtsanwalt-sasse.de
info@sasse-heilpraktikerrecht.de

Internet www.rechtsanwalt-sasse.de
www.sasse-heilpraktikerrecht.de

RA Dr. René Sasse ● Chemnitzer Straße 126 ● 44139 Dortmund

pgt technology scouting GmbH
Ruschgraben 51
76139 Karlsruhe

Cloud-basierte Datenverarbeitungssysteme und die 2-Faktor-Authentifizierung – Auswirkungen auf die Praxisverwaltungssoftware Lemniscus

Begriff der 2-Faktor-Authentifizierung

Webanwendungen – wie z.B. eine cloud-basierte Praxisverwaltungssoftware – sind durch ihre Online-Anbindung bequem zugänglich. Erforderlich sind lediglich eine Internetverbindung und ein entsprechendes Endgerät. Sodann reichen die Eingabe des Benutzernamens und eines Passwortes aus, um Zugriff auf die jeweiligen Inhalte zu erlangen. Zwar kann die Browserfreigabe diesen Prozess erschweren, allerdings ist sie nicht sicher. Dieser leichte Zugang führt zu dem Risiko, dass unbefugte Dritte Zugriff auf die Daten erhalten können. Dies gilt insbesondere für in diesen Fällen:

- Ausnutzen von fehlerhaftem Nutzerverhalten, z.B. Nutzung ungeeigneter Passwörter, Wiederholter Einsatz von Passwörtern,
- Speicherung von Passwörtern im Browser, so dass andere Nutzer des Gerätes Zugriff erhalten,
- Hackerangriffe, Cyberangriffe, Social Engineering (z.B. Phishing), Datendiebstahl.

Dieser Gefahr beugt die sogenannte 2-Faktor-Authentifizierung vor, indem sie den Zugang zum System durch einen zusätzlichen Faktor absichert. Hierbei kann es sich beispielsweise um die Zusendung eines Codes per SMS/E-Mail, einen generierten Zahlencode einer Authenticator-App oder einen Hardwarestick (z.B. Fido-Stick) handeln. Es reicht nicht (mehr) aus, ausschließlich das Passwort einzugeben; erst wenn anschließend auch der zusätzliche Faktor korrekt verwendet wurde, erhält der Anmelder Zugriff auf die Daten. Diese Methode reduziert erheblich das Risiko eines unbefugten Zugriffs. Sofern der Dritte keinen Zugriff auf den zweiten Faktor hat, nutzt ihm

allein die Kenntnis des Benutzernamens und des Passwortes nichts. Deshalb liegt bei aktiver 2-Faktor-Authentifizierung bei Verlust des Passwortes noch keine meldepflichtige Datenpanne im Sinne der DSGVO vor. Bei einem unberechtigten Login-Versuch der zweite Faktor nicht korrekt eingegeben wird, sollte der Nutzer vom Anbieter über den nicht identifizierbaren Anmeldeversuch benachrichtigt werden. Er kann dann weitere Maßnahmen, wie z.B. eine Passwortänderung vornehmen. Mangels Verletzung des Schutzes personenbezogener Daten, muss die verantwortliche Stelle **nicht** gemäß Art. 33 der DS-GVO unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung eine Meldung an die Aufsichtsbehörden abgeben.

Verpflichtung zur Integration und Nutzung der 2-Faktor-Authentifizierung

Aufgrund der erheblich höheren Sicherheit ist die 2-Faktor-Authentifizierung aus tatsächlichen Gründen eine ratsame Entscheidung. Es fragt sich jedoch, ob die DSGVO diese Maßnahme (datenschutz-)rechtlich erfordert und ob bei unberechtigtem Zugriff andernfalls Schadensersatzansprüche der Betroffenen drohen. Diese Frage richtet sich sowohl an die Nutzer solcher Webanwendungen als auch an die Anbieter dieser Programme. Während letztere eine Funktion zur 2-Faktor-Authentifizierung möglicherweise anbieten müssen, ist es die Aufgabe der Anwender, diese auch zu aktivieren bzw. zu nutzen. Es ist zu berücksichtigen, dass Verantwortlicher und Auftragsverarbeiter als Gesamtschuldner für einen durch die Datenverarbeitung entstandenen Schaden haften (Art. 82 DSGVO).

Die DSGVO gibt keine konkreten technischen Maßnahmen vor, sie setzt lediglich den Rahmen.

Nach Art. 32 DSGVO gilt:

> *(1) **Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten**; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:*
>
> *a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;*
> *b) die Fähigkeit, die **Vertraulichkeit**, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung **auf Dauer sicherzustellen**;*

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
(…)
(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere ***die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind,*** *insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.*

Zudem gibt Art. 25 DSGVO folgendes vor:

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung ***geeignete technische und organisatorische Maßnahmen*** *– wie z.B. Pseudonymisierung –, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.*

Gemäß Art. 28 Abs. 1 DSGVO darf eine Auftragsverarbeitung ausschließlich mit einem Anbieter erfolgen, der hinreichend Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Zudem können die Anforderungen bzw. Vorgaben für einen ordnungsgemäßen und sicheren Umgang mit den Daten aus Artikel 5 Abs. 1 lit. f DSGVO (Grundsätze für die Verarbeitung personenbezogener Daten), aus den Erwägungsgründen 39 und 78 Verordnung (EU) 2016/679 S. 12 sowie der Anlage zu § 9 BDSG 2003 entnommen werden. Daten müssen durch geeignete technische und organisatorische Maßnahmen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Erwägungsgrund 39 nennt als geforderte Maßnahmen, dass gewährleistet ist, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.

Bei Verstößen drohen empfindliche Bußgelder. Zudem sind Datenschutzverletzungen innerhalb von 72 Stunden zu melden.

Ob eine 2-Faktor-Authentifizierung erforderlich ist, ist demnach eine Frage der Abwägung. Hierbei sprechen insbesondere folgende Punkte für eine Pflicht zur 2-Faktor-Authentifizierung:

- Die DSGVO schützt Gesundheitsdaten in besonderem Maße, Art. 9 DSGVO. Eine unbefugte Einsichtnahme in diese sensiblen Daten kann mit scherwiegenden Nachteilen für den Patienten verbunden sein.
- Für die Anbieter als Auftragsverarbeiter sind die Implementierungskosten gering, für den Nutzer entstehen in der Regel keine oder nur sehr geringe Kosten durch die Einführung einer 2-Faktor-Authentifizierung.
- Der Mehraufwand bei der Anmeldung ist gering.
- Es handelt sich um eine effektive Schutzmaßnahme.
- Insbesondere bei Mobilgeräten bestehe eine erhöhte Gefahr von Diebstahl oder Verlust.

Gegen eine solche Pflicht könnten folgende Argumente sprechen:

- Höhere Ausfallrisiko bei Verlust des zweiten Faktors. Kein Zugang zur Webanwendung möglich. Dieses Risiko ist jedoch vermeidbar durch das Anlernen weiterer Faktoren.

Bei der Speicherung von Gesundheitsdaten in der Cloud sprechen die überwiegenden Gründe somit dafür, einen Zugang durch einen zweiten Faktor abzusichern. Neben der Gefahr von Bußgeldern droht bei „Datenpannen“ zudem das Risiko, dass Betroffene gemäß Art. 82 Abs. 1 DSGVO wegen Verstoßes gegen Art. 32 DSGVO immateriellen Schadensersatz vom Therapeuten fordern, weil dieser keine geeigneten technischen und organisatorischen Maßnahmen getroffen hat, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. (Art. 82 Abs. 1 DSGVO)

Auch das Bayerische Landesamt für Datenschutzaufsicht hält eine 2-Faktor-Authentifizierung für medizinische Einrichtungen für erforderlich. So weist das Amt in der Veröffentlichung „Cybersicherheit für medizinische Einrichtungen“ darauf hin, dass sicherheitskritische Bereiche längst im Fokus von Angreifern lägen. Neben klassischen Passwörtern seien daher weitere Zugangsfaktoren erforderlich, um diese besonders schützenswerten Zugänge angemessen

abzusichern. Bei der Veröffentlichung handelt sich ausdrücklich um eine Hilfestellung zur schnellen Überprüfung der Sicherheit hinsichtlich der Verfügbarkeit der eigenen Datenverarbeitung im Sinne von Art. 32 DSGVO. Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt hat sich dieser Sichtweise angeschlossen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät ebenfalls dazu eine 2-Faktor-Authentifizierung bei schützenswerten Konten zu verwenden.

Die Kassenärztliche Bundesvereinigung fordert in ihrer Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit eine „strikte Absicherung" der Zugänge zu Internetanwendungen. Der Begriff „strikt" deutet darauf hin, dass eine „normale" Passwortabsicherung nicht als ausreichend erachtet wird, sondern weitergehende Maßnahmen - wie eine 2 Faktor-Authentifizierung - erforderlich sind.

Aus technischer Sicht wird darauf hingewiesen, dass klassische Passwörter keinen ausreichenden Datenschutz (mehr) bieten. Um Online-Zugänge zuverlässig zu schützen, wird deshalb eine Zwei-Faktor-Authentifizierung empfohlen. (Rügheimer, H. Zwei Faktoren für mehr Sicherheit. Schmerzmed. 35, 53 (2019).)

Eine interessante Entscheidung hierzu betrifft ein Amsterdamer Krankenhaus. Die niederländische Datenschutzbehörde hat ein Bußgeld in Höhe von 440.000 Euro gegen das Krankenhaus OLVG verhängt, weil keine ausreichenden technischen und organisatorischen Maßnahmen ergriffen worden seien, um den Zugriff auf Krankenakten durch unbefugtes Personal zu verhindern. Hier war es Mitarbeitern möglich, Patientenakten einzusehen, die neben den Krankengeschichten der Patienten auch die Sozialversicherungsnummern sowie Kontakt- und Adressdaten enthielten. Außerhalb des Krankenhauses konnten die Mitarbeiter mithilfe einer 2-Faktor-Authentifizierung die Akte einsehen, innerhalb des Krankenhauses reichte jedoch ein einfacher Login aus. Zudem wurden die Zugriffe auf die Patientenakten nicht auf unautorisierte Zugriffe hin überprüft.

Konsequenzen für die Praxissoftware Lemniscus

Verantwortliche und Auftragsverarbeiter müssen in Anbetracht hochdynamischer digitaler Prozesse ihre gesetzlichen Verpflichtungen nach Art. 32 DSGVO uneingeschränkt erfüllen.

Ein DSGVO-konformes Schutzniveau für den Zugriff auf Patientendaten in der Cloud erfordert somit eine 2-Faktor-Authentifizierung. Im Hinblick auf mögliche Schadensersatzansprüche von Patienten und dem Risiko von Bußgeldern empfehle ich deshalb, bei Ihrer Praxisverwaltungssoftware eine solches Authentifizierungsverfahren verpflichtend zu integrieren. Andernfalls bestehen für Sie als

Anbieter der Praxissoftware und für Ihre Kunden erhebliche Haftungsrisiken. Damit Lemniscus „definitiv“ DSGVO-konform bleibt, ist eine verbindliche 2 Faktor Authentifizierung erforderlich.

Zwar wäre es denkbar, eine 2 Faktor-Authentifizierung nur optional anzubieten; dies würde jedoch das Risiko hervorrufen, dass Therapeuten diese nicht einrichten oder bewusst deaktivieren. Im Hinblick auf das Mithaftungsrisiko als Auftragsverarbeiter aus Art. 82 DSGVO sollte dieses Risiko ausgeschlossen werden.

Dr. René Sasse
(Rechtsanwalt)