FAQ ZUM THEMA DSGVO

(LETZTE AKTUALISIERUNG AM 17.09.2019: FINGERSCANNER)

Diese FAQ sind als Tipps von Seiten Dampsoft und nicht als Rechtsbelehrung zu verstehen. Im Zweifel wenden Sie sich bitte an Ihren Rechtsbeistand.

Ist die Nutzung des Fingerscanners im Zusammenhang mit dem DS-Win DSGVO-konform?
Die technischen Voraussetzungen erfüllen die Anforderungen an technischen Maßnahmen zum Schutz personenbezogener Daten, die von der DSGVO gefordert sind.
Die in Dateien umgewandelten Fingerabdrücke werden verschlüsselt im DS-Win gespeichert. Die Ver- und Entschlüsselung findet mit Funktionen aus der DLL des Herstellers *Digital Persona* statt. Es ist an großer Sicherheit grenzender Wahrscheinlichkeit davon auszugehen, dass eine Entschlüsselung durch Dritte unmöglich ist. Sollte dieser höchst unwahrscheinliche Fall doch eintreten, so erhält man damit immer noch kein Abbild des gescannten Fingers, sondern einen Zahlenwert, der den Fingerabdruck repräsentiert. Aus dem Zahlenwert kann nicht auf das Abbild des Fingerabdrucks rückgeschlossen werden. Auch Dampsoft hat keinen Zugriff auf die verschlüsselten Dateien! Die Fingerabdrücke selbst können somit weder von der Praxis selbst noch von Dampsoft digital angezeigt weiterverarbeitet werden.
Der Mitarbeiter, der Supervisor-Rechte hat, kann jeden einzelnen Fingerabdruck eines Mitarbeiters jeder Zeit aus dem DS-Win löschen (ohne Dateizugriff zu haben - lediglich durch eine visuelle Darstellung einer Hand in der Mitarbeiterverwaltung, an der dann die Kontrollkästchen zu den dort hinterlegten Fingerabdrücken entfernt werden können). Dies hat keine Auswirkungen auf die Zeiten des jeweiligen Mitarbeiters.
Bei der Verarbeitung von biometrischen Daten (z. B. zur Zeiterfassung mit Hilfe eines Fingerabdrucks) ist gem. Art. 9 (2) a) DSGVO die Einwilligung der Mitarbeiter einzuholen, wenn nicht andere Gründe gem. Art. 9 (2) gegeben sind.

Benötigen Zahnarztpraxen eine schriftliche Einwilligung des Patienten, bevor Sie den Patienten behandeln dürfen?
Es kommt darauf an. Grundsätzlich ist der Behandlungsvertrag die Rechtsgrundlage für die Datenverarbeitung und somit ausreichend. Eine Einwilligung wäre nur für weitere, nicht zum Vertrag gehörende Verarbeitungen nötig, z.B. für einen Recall-Service. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein ULD hat zu diesen und anderen wichtigen Fragen Stellung bezogen: https://www.datenschutzzentrum.de/uploads/medizin/Heilberufe2018-05-25.pdf.

Was ist beim Online Terminmanagement und beim SMS-Versand zu beachten?
Auf der Registrierungsseite für das Online Terminmanagement muss der Kunde der Datenschutzerklärung zum Online-Terminmanagement zustimmen, bevor seine Daten zur Registrierung an Dampsoft übermittelt werden können. Dampsoft hat seine Unterauftragnehmer (Art. 28 DSGVO) gem. § 203 StGB zur Verschwiegenheit von Berufsgeheimnissen verpflichtet und mit Ihnen einen Vertrag zur Auftragsverarbeitung gemäß den Anforderungen der DSGVO abgeschlossen. Der Patient muss über ein Opt-in-Feld seine Zustimmung zur Datenweitergabe geben, möchte der Patient einen Reminder per SMS erhalten. Sowohl das Online Terminmanagement als auch der SMS-Versand sind DSGVO-konform!

Hat Dampsoft über das DS-Win Zugriff auf meine Patienten- und Mitarbeiterdaten?
Nein, da sich die Daten auf einem eigenen Server der Praxis befinden. Ein Zugriff kann aber durch die Praxis, z. B. über ein Remote-Service, gewährt werden. Für diese und andere Fälle haben Bestandskunden von uns am 30.04.2018 eine Verpflichtung auf das Datengeheimnis nach DSGVO erhalten. Alle Neukunden erhalten die Geheimhaltungsvereinbarung zusammen mit dem Softwarenutzungs- und -wartungsvertrag.

FAQ ZUM THEMA DSGVO

(LETZTE AKTUALISIERUNG AM 17.09.2019: FINGERSCANNER)

Wie verpflichte ich Dampsoft und ihre Mitarbeiter sowie andere mitwirkende Personen zur Geheimhaltung?
Dampsoft wird Ihnen eine von uns unterschriebene Geheimhaltungsvereinbarung für Ihre Unterlagen zur Verfügung stellen, in der wir Ihnen bestätigen, dass Sie uns und Dampsoft ihre Mitarbeiter zur Verschwiegenheit verpflichten haben bzw. hat.
Dampsoft wird Ihnen zudem eine Vorlage zur Geheimhaltungsvereinbarung zur Verfügung stellen, die Sie für alle mitwirkende Personen (z. B. externe Reinigungskräfte, externe Sicherheitsdienste oder externe IT-Dienstleister) verwenden können.

Was ist in puncto Wartung oder Remote-Services zu beachten?
Bei einem Remote-Zugriff ist darauf zu achten, dass der Remote-Zugriff von Seiten der Praxis zu protokollieren und ein Praxisteammitglied während der Remote-Sitzung anwesend ist. Über das Kamera-Symbol im Teamviewer kann die Praxis die Sitzung aufzeichnen und die Datei abspeichern. Auch wenn es noch keine Rechtsprechung diesbezüglich gibt, führen wir einen Remoteservice nur bei vorliegendem unterschriebenem AV-Vertrag durch. Dies dient der Absicherung aller Beteiligten.
Ein weiterer Schritt zu mehr Sicherheit ist es, von dauerhaften Remote-Sitzungen, z. B. zu Technikern, abzusehen und eigene Benutzernamen und Passwörter für Remote-Zugänge vertraulich zu behandeln.

Wann wird ein Vertrag zur Auftragsverarbeitung benötigt und wie ist dieser abzuschließen?
Ein AV-Vertrag wird benötigt, wenn Sie einen Dritten beauftragen, in Ihrem Namen personenbezogene Daten weiterzuverarbeiten, also z. B. dann, wenn Sie Dampsoft per Remote auf Ihre IT-Umgebung Zugang gewähren oder, aufgrund eines nicht unter üblichen Supportwegen zu behebenden technischen Problems, eine Datensicherung zusenden müssen.
Wir werden allen Kunden proaktiv einen von uns unterschrieben AV-Vertrag zur Verfügung stellen. Bitte unterschreiben Sie diesen handschriftlich und senden Sie diesen einmalig an uns zurück (per E-Mail, Fax oder Brief). Wir empfehlen Ihnen, eine Kopie für Ihre Unterlagen anzufertigen.

Wann und wie versende ich eine Datensicherung an Dampsoft?
Ein Verlust von Patientendaten ist der „Worst Case“ einer jeden Zahnarztpraxis. Der Versand einer Datensicherung an uns sollte nur in Absprache mit einem unserer Mitarbeiter erfolgen.
Sollte es notwendig sein, eine Datensicherung zu versenden, dann treffen Sie bitte mindestens folgende Sicherheitsvorkehrungen:
Auch wenn die programmeigene Datensicherung durch ein proprietäres Format für andere Programme schwer lesbar ist, empfehlen wir, bei der Erstellung der Datensicherung ein Passwort einzugeben.
Sollte der gesamte Ordner „TDAMP“ übermittelt werden müssen, sollte dieser z. B. mit dem Programm 7Zip gepackt und dabei auf jeden Fall ein Passwort festgelegt werden, damit das erstellte Archiv verschlüsselt ist. Für die Übermittlung des Passworts an uns sollte immer ein anderer Weg als für die Datensicherung an sich gewählt werden. Auch können Sie den Versand per Upload über unseren Webserver unter https://www.dampsoft.de/service/ verschlüsselt vornehmen.
Zusätzlich ist eine Anonymisierung der Datensicherung möglich. Diesbezüglich finden Sie weiter unten zusätzliche Informationen.

FAQ ZUM THEMA DSGVO

(LETZTE AKTUALISIERUNG AM 17.09.2019: FINGERSCANNER)

Wie oft sollte eine Datensicherung durchgeführt werden?
Wir empfehlen eine tägliche Datensicherung durchzuführen. Darüber hinaus sollten mindestens zwei verschiedene externe Datenträger verwendet werden, z. B. einer für montags, mittwochs und freitags und einer für dienstags und donnerstags. Die Datenträger sollten für Dritte unzugänglich, passwortgeschützt und vor Brand, Nässe und Witterung geschützt aufbewahrt werden – im besten Fall voneinander und vom Server räumlich getrennt.

Von wem sollte eine Datensicherung durchgeführt werden?
Im Sinne der Datensicherheit empfehlen wir den Kreis derjenigen Personen, die eine Datensicherung durchführen dürfen, möglichst klein zu halten. Welche Personen Datensicherungen über das DS-Win vornehmen dürfen, können Sie in der Mitarbeiterverwaltung des DS-Win über das Berechtigungssystem steuern. Zudem empfehlen wir Ihnen für die Datensicherung ein Passwort zu vergeben. Mit dem nächsten Update wird zukünftig eine Passwortabfrage voreingestellt sein.

Welche Anforderungen sollte ich grundsätzlich an Passwörter stellen?
Passwörter sollten mindestens 8 Zeichen enthalten und sich aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen zusammensetzen. Außerdem empfehlen wir, das Passwort regelmäßig zu ändern.

Muss ich mit jeder einzelnen mitwirkenden Person eines Dienstleisters eine separate Geheimhaltungsvereinbarung schließen?
Nein, es reicht, wenn der Arzt seinen Dienstleister verpflichtet, seinerseits sich, seine Mitarbeiter und etwaige Dienstleister zu verpflichten, diese Aufgabe also an seinen Dienstleister delegiert. Wir von Dampsoft haben Ihnen bereits eine Bestätigung zur Verpflichtung auf das Datengeheimnis nach DSGVO zur Verfügung gestellt.

Wie kann ich einen unmittelbaren Zugriff auf Datenbankdateien vermeiden?
Um den unmittelbaren Zugriff auf Datenbankdateien vermeiden zu können, schlagen wir folgende Lösungsansätze vor:
1. Haben Sie bereits Remotedesktopdienste im Einsatz, schlagen wir die Konfiguration einer Remote-App für das DS-Win-Plus vor. Nähere Details erfragen Sie bitte bei Ihrem Systembetreuer.
2. Stellen Sie zusammen mit Ihren Systembetreuer sicher, dass nur autorisierte Personen auf die Praxis-PCs und die Server zugreifen sowie über entsprechende Maßnahmen keine Daten auf externe Datenträger kopiert oder von diesem eingespielt werden können.
Onlinezugänge zur Fernwartung sollten keinen unbeaufsichtigten Zugriff erlauben.
Der/die Server sollte/n in einem abgeschlossenem Bereich stehen und auf den Praxis-PCs keine Daten oder Daten-Kopie abgelegt sein.

Wie kann ich sensible Dokumente auf Dateiordnerebene schützen?
Mit der Vergabe von Windows-Berechtigungen können Sie Zugriffe auf Dateiordnern verhindern. Zudem empfehlen wir, sensible Dokumente vor unberechtigte Zugriffe mit einem Passwort zu schützen.

Wie kann ich den Druck von sensiblen Dokumenten einschränken?
Die Berechtigungen zum Druck von sensiblen Daten/Listen können in der Mitarbeiterverwaltung im DS-Win über das Berechtigungssystem vergeben werden.

FAQ ZUM THEMA DSGVO

(LETZTE AKTUALISIERUNG AM 17.09.2019: FINGERSCANNER)

Wo erhalte ich Hinweise zur Mitarbeiterverwaltung und zum Berechtigungssystem im DS-Win?
Im DS-Win-Handbuch unter den Kapiteln 22.1.2 bis 22.1.2.5 erhalten Sie Informationen zur Mitarbeiterverwaltung und zum Berechtigungssystem im DS-Win und können entsprechend dieser Ausführungen ihre Mitarbeiterverwaltung und die Berechtigungsvergabe umsetzen. Zusätzlich empfehlen wir Ihnen die Anleitung „Mitarbeiterverwaltung“, die Sie im Bereich „Service“ auf unserer Webseite finden. Dort finden Sie ebenfalls detaillierte Beschreibungen des Vorgehens.
Wir empfehlen Ihnen dringend, die Anleitung vor Einrichtung der Mitarbeiterverwaltung zu lesen, damit diese im Sinne Ihrer Praxis arbeitet.

Tipps zum Umgang mit dem DS-Win:

1.) Berechtigungsvergabe:
Wir empfehlen Ihnen, mit der Mitarbeiterverwaltung des DS-Win zu arbeiten. So haben Sie die Möglichkeit, für jeden Mitarbeiter spezielle Berechtigungen und Zugriffsmöglichkeiten zu definieren. Bitte beachten Sie bei der Einrichtung, dass einem Behandler oder Mitarbeiter in jedem Fall alle Berechtigungen zugewiesen werden (Administrator-Rolle).
Wir empfehlen dem Praxisinhaber die Rolle des Administrators einzunehmen, ein nicht leicht zu erratendes Passwort zu vergeben und dieses vor Dritten zu schützen.
Das Passwort können Sie im DS-Win unter folgendem Pfad verwalten:
Verwaltung -> Praxis -> Mitarbeiter -> Administrator als Mitarbeiter anlegen mit allen Berechtigungen
Zusätzlich finden Sie auf unserer Webseite eine Anleitung zur Unterstützung bei der Einrichtung der Mitarbeiterverwaltung. Klicken Sie einfach auf den folgenden Link:
https://www.dampsoft.de/wp-content/uploads/2018/04/Anleitung_Mitarbeiterverwaltung.pdf
Wir empfehlen Ihnen dringend, die Anleitung vor Einrichtung der Mitarbeiterverwaltung zu lesen, damit diese im Sinne Ihrer Praxis arbeitet.

2.) Anonymisierte Darstellung des Terminbuches:
Sollte der Nutzer gemeinsam mit dem Patienten in das Terminbuch schauen müssen, besteht die Möglichkeit der anonymen Darstellung in der Tagesansicht des Terminbuches. Betätigen Sie hierzu das rote Symbol mit der schwarzen Sonnenbrille oben rechts in der Symbolleiste.

3.) Datenportabilität:
Sollten Patienten die Aushändigung ihrer Karteikarte verlangen, können Sie dafür eine mit einem Kennwort geschützte PDF-Datei generieren. Dazu sind folgende Einstellungen einmalig im DS-Win vorzunehmen:
Einstellungen > Sonstige Einstellungen > Externe Programme > AzP-Export markieren (AzP-Schnittstelle – Schnittstelle zum Austausch zahnärztlicher Patientendaten) > Button >>eigene Schaltfläche<< anwählen > das Fenster mit >>OK<< verlassen > zur Kontrolle die Patientenauswahl neu öffnen und in der Patienteninfo kontrollieren > hier sollte nun auf der rechten Seite die neue Schaltfläche >>AzP-Export<< sichtbar sein.

Um die Kartei des Patienten als geschützte PDF-Datei zu erhalten und ihm diese per E-Mail zukommen zu lassen, sind folgende Schritte notwendig:

FAQ ZUM THEMA DSGVO

(LETZTE AKTUALISIERUNG AM 17.09.2019: FINGERSCANNER)

Patienten aufrufen > Reiter Pat.info anwählen > rechts die Schaltfläche >>AzP-Export<< betätigen > Kennwort eingeben / 4 Ziffern nach Wahl (dem Patienten muss dieses Kennwort mitgeteilt werden, sonst kann er später seine Kartei nicht öffnen) > Verzeichnis auswählen, in dem die Datei gespeichert werden soll > abschließend Schaltfläche >>Daten exportieren<< betätigen und das Fenster mit >>Ok<< verlassen.

In dem gewählten Speicherort finden Sie nun einen ZIP-Ordner. In diesem Ordner befindet sich zum einen die verschlüsselte PDF-Datei und zum anderen eine txt-Datei, mit der die Daten in ein anderes Programm exportiert werden können. Grundsätzlich kann der AzP-Export auch ausgedruckt dem Patienten mitgegeben werden.

4.) Datenverfügbarkeit (Backup):
Wir empfehlen Ihnen täglich eine passwortgeschützte Datensicherung zu erstellen. Die Datensicherung erstellen Sie über den folgenden Pfad:
Oben links das Dampsoft-Symbol anklicken > Datensicherung > Erstellen.

Möchten Sie an die Datensicherung erinnert werden, nehmen Sie bitte einmalig folgende Einstellung vor:
Einstellungen > Allgemeine Einstellungen > Checkbox: Datensicherung erfolgt über DS-Win-Plus.

5.) Erstellen einer anonymisierten Datensicherung Ihres DS-Win:
Sie haben die Möglichkeit, eine anonymisierte Datensicherung des DS-Win zu erstellen. Diese können Sie über den folgenden Pfad erstellen:
Oben links das Dampsoft-Symbol anklicken -> Datensicherung -> Erstellen -> Daten anonymisieren
Grundsätzlich ist eine Anonymisierung der Datensicherung nicht notwendig. Bei Datensicherungen zum Gebrauch in der Praxis z. B. zur Wiederherstellung des Programms sollte auf eine Anonymisierung verzichtet werden, damit alle relevanten Daten nachvollziehbar sind (Datenintegrität). Eine Anonymisierung kann u. U. bei Datensicherungen erfolgen, wenn diese Dampsoft zur Diagnose zugesendet werden. Bitte besprechen Sie das Vorgehen hier im Einzelfall mit unserem Kundenservice.

6.) Kommunikation mit Dritten:
Für eine schriftliche Kommunikation mit Dritten über einen Patienten (z. B. Laborbrief), stehen Ihnen zudem in unserem Textprogramm vielfältige Makros zur Verfügung, mit denen Sie auch ohne die Angabe des Patientennamens eine Zuordnung zum Patienten herstellen können, z. B. Patientennummer, XML-Nr. etc.

7.) E-Mails, z. B. mit Röntgenbildern, sicher versenden:
Dampsoft bietet eine mögliche Verschlüsselung mit Zertifikaten für den E-Mail-Verkehr an, die jedoch über andere Dienstleister bezogen werden müssen. Die Einrichtung ist dann von dem jeweiligen Systembetreuer unter folgendem Pfad durchzuführen:
Kommunikation > E-Mail > E-Mail > Einstellungen > Konten Einstellungen > Zertifikate verwalten.

FAQ ZUM THEMA DSGVO

(LETZTE AKTUALISIERUNG AM 17.09.2019: FINGERSCANNER)

Weitere Informationen finden Sie auch in Abschnitt 4 „E-Mail-Signatur und –Verschlüsselung mit Zertifikaten“ der Anleitung, die Sie im E-Mail-Client des DS-Win abrufen können. Folgen Sie hierzu einfach folgendem Pfad:
Kommunikation > E-Mail > E-Mail > Einstellungen > Allgemeine Einstellungen > Schaltfläche „i“ Anleitung.

Wem die zertifizierte Verschlüsselung für den E-Mail-Verkehr zu aufwändig ist, dem empfehlen wir (wo möglich) eine direkte Verschlüsselung über die jeweilige Software zum Endgerät (z. B. Röntgengerät) vorzunehmen und diese verschlüsselte Datei dann als Anhang einer E-Mail zu versenden. Zudem bieten manche KZVen einen sicheren Upload zum Datenaustausch an.

8.) Löschen von Patientendaten:
Das DS-Win ist so konfiguriert, dass Patientendatensätze frühestens 10 Jahre nach Beendigung der Behandlung gelöscht werden können. Wir empfehlen, nur die Informationen über den Patienten zu sammeln, die aufgrund rechtlicher Vorschriften benötigt werden.
Mit dem Generalupdate 02/2018 wird es möglich sein, dass das DS-Win Patientendaten nach Ablauf der Aufbewahrungsfrist für Sie zum Löschen auflistet und Sie somit die Möglichkeit haben, selbst zu entscheiden, ob Sie die Daten aufgrund zivilrechtlicher Risiken noch weiter verwalten oder sie unwiderruflich löschen möchten. Bitte beachten Sie, dass Sie als verantwortliche Person selbst entscheiden müssen, ob Sie und welche Datensätze Sie löschen möchten – die durch das DS-Win generierte Liste ist lediglich als Vorschlag zu verstehen. Im zugehörigen Update Aktuell 2/2018 finden Sie weitere Informationen.

9.) Wie kann ich datenschutzrelevante Formularvorlagen in das DS-Win integrieren?
Wir empfehlen zwei Vorgehensweisen:

1. Sie haben die Erweiterung DS-Win-View installiert:
Gehen Sie im Hauptmenü des DS-Win auf „Erweiterungen“ und wählen Sie hier „View“ aus. Entscheiden Sie, ob Sie das Dokument für einen Patienten („Patient“) oder als allgemeine Vorlage („allgemein“) hinterlegen möchten. Klicken Sie nun links unten auf die Schaltfläche >>Datei<< im DS-Win-View, wählen Sie im sich öffnenden Windows-Explorer den Speicherort der einzubindenden Vorlage aus und klicken Sie auf „öffnen“. Die Vorlage ist nun im View abgespeichert.

2. Sie arbeiten nicht mit dem DS-Win-View:
Kopieren Sie den Inhalt der Word-Vorlage in die Textverarbeitung des DS-Win, formatieren diesen Inhalt Ihren Wünschen entsprechend und speichern das Dokument ab. Um das Formular patientenbezogen zu nutzen, wählen Sie den gewünschten Patienten aus und rufen Sie die Textverarbeitung auf (Formular > Briefe > Patientenbrief von Vorlage). Über „Text“ und „Auswahl“ können Sie die gespeicherte Vorlage auswählen.

10.) Wie komme ich an datenschutzrelevante Vorlagen, die ich nutzen kann?
Eine Vorlage eines AV-Vertrags inkl. einer Vorlage technischer und organisatorischer Maßnahmen finden Sie auf der Homepage der GDD unter folgendem Pfad: https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo oder auf der Homepage des Bitkom unter

FAQ ZUM THEMA DSGVO

(LETZTE AKTUALISIERUNG AM 17.09.2019: FINGERSCANNER)

folgendem Pfad: https://www.bitkom.org/Bitkom/Publikationen/Mustervertragsanlage.html. ACHTUNG: Für die Zusammenarbeit zwischen Ihnen und Dampsoft stellt Dampsoft Ihnen einen vollständigen AV-Vertrag zur Verfügung.

Dampsoft stellt Ihnen und Ihrem Team folgende für den Datenschutz relevante Vorlagen auf unserer Homepage unter https://www.dampsoft.de/die-dsgvo-nuetzliche-hinweise-als-faq/ zur Verfügung:

- Verfahrensverzeichnisse für unsere Produkte (spätestens bis zum 25.05.2018)
- Patienteninformation zum Artikel 13 DSGVO: Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person.
- Vorlage zur Verpflichtung auf das Datengeheimnis
- Vorlage(n) für Schweigepflichtentbindungserklärungen
- Vorlage zur Einwilligungserklärung bei Auskunft an Angehörige
- Vorlagen zur Einwilligungserklärung bei Verrechnungsstellen (im DS-Win hinterlegt)
- Bestellungsurkunde für Datenschutzbeauftragte (notwendig bei Praxen mit mehr als 9 Mitarbeitern).

Bei anderen Vorlagen ist es ggf. sinnvoll, auf Ihren IT-Systembetreuer zuzugehen (z. B. Notfallhandlungskonzept) oder sich an andere Institutionen zu wenden.

Sie haben weitere Fragen zum Datenschutz? Senden Sie Ihre Anfrage bitte per E-Mail an:

datenschutz@dampsoft.de

Ihr Dampsoft-Team